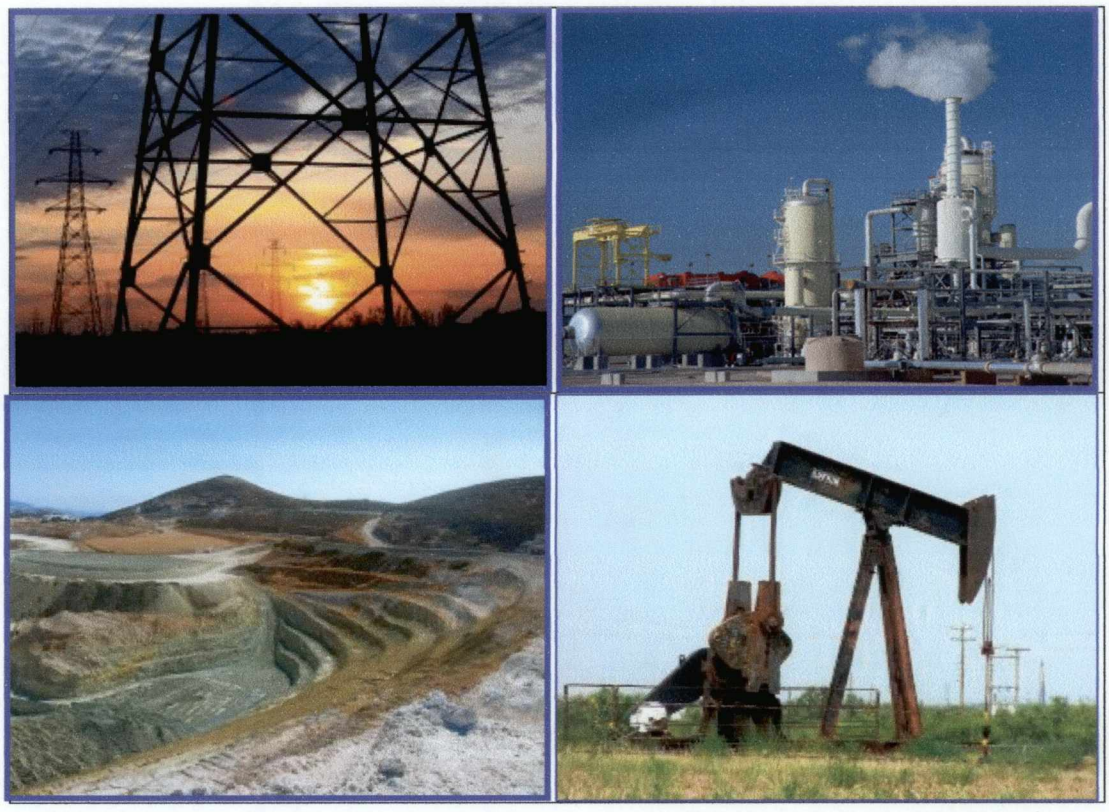
Osinergmin
ORGANISMO SUPERVISOR DE LA INVERSIÓN EN ENERGÍA Y MINERÍA

MANUAL DE GESTIÓN DE SEGURIDAD

SGS

OSINERGMIN



ENERO - 2010

TABLA DE CONTENIDO

Pág.

CAPÍTULO 1

PANORAMA GENERAL

1.1 GENERALIDADES

1.1.1 Este Manual tiene la intención de proveer a OSINERGMIN el desarrollo del marco regulador y el material de soporte para apoyar en la puesta en práctica de un Sistema de Gestión de Seguridad (SGS) en la organización.

1.2 OBJETIVOS

1.2.1 Los objetivos de este Manual son proporcionar conocimiento a OSINERGMIN:

- Sobre los conceptos de Gestión de Seguridad.
- Para estructurar un sistema de gestión de seguridad (SGS) para los procesos establecidos en el sistema integrado de gestión (SIG)
- Para identificar peligros y establecer riesgos y así poder generar un conocimiento dinámico y permanente de las amenazas que puedan afectar a la organización con el fin de diseñar los controles y estrategias para minimizarlos.
- Para desarrollar y/o mejorar el Programa de Seguridad Operacional dispuesto por OSINERGMIN a las empresas de su ámbito.
- Para certificar y supervisar la puesta en práctica de los componentes claves de un SGS en las empresas del ámbito de OSINERGMIN en los sub- sectores de energía y minas en cumplimiento con las disposiciones establecidas.

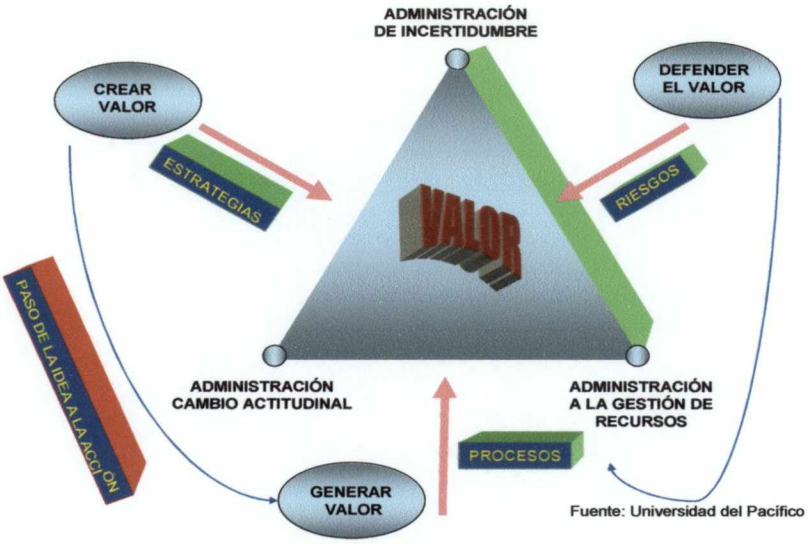
1.3 CONCEPTOS BASICOS DE SEGURIDAD Y RIESGO

1.3.1 Para entender los procedimientos usados en una gestión de seguridad, es necesario examinar exactamente cual es el significado de **"safety".** Si recurrimos a un diccionario, la traducción es "seguridad", si recurrimos también al diccionario para la palabra "**security**", la traducción también es "seguridad". Tanto "safety" como "security" tienen medidas de **prevención**.

1.3.2 Cuando nos hablan de seguridad tenemos el modelo mental a relacionarlo solo a seguridad física. Ejemplo: Observamos a una persona sospechosa y decimos, llamemos a seguridad.

1.3.3 Por otro lado, en el contexto de la industria, la seguridad, era conceptuada como la ausencia de accidentes. El incremento de las incertidumbres (peligros) en los mercados y la necesidad de convertirlas en riesgos para poder medirlas, permitió la evolución de una herramienta de gestión de riesgos que sea totalmente flexible que se pueda aplicar tanto en la parte estratégica para las variables del entorno, como para los procesos operativos y de apoyo.

1.3.4 En la actualidad hablamos de procesos de creación de valor (gestión estratégica), procesos de defensa del valor (gestión de riesgos) y procesos de generación del valor (procesos operativos)



Fuente: Universidad del Pacífico

Definición de seguridad

1.3.5 **Seguridad:** Es una condición en la cual el riesgo de daño ó perjuicio se limita aun nivel aceptable

Definición de gestión de seguridad

1.3.6 **Sistema de gestión de Seguridad:** es el estado en que los riesgos del entorno, de los procesos y de la información de la toma de decisiones se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos.

Definición de peligro

1.3.7 **Peligro**: Condición, objeto o actividad que potencialmente puede causar lesiones al personal, daños al ambiente, equipamiento o estructuras, pérdida de personal, o reducción de la habilidad de desempeñar una función determinada.

Definición de riesgo.

1.3.8 **Riesgo:** La posibilidad de pérdida o daño, medida en términos de severidad y probabilidad. La posibilidad que algo pueda ocurrir y sus consecuencias si ocurre.

Definición de gestión de riesgos

1.3.9 **Gestión de riesgos**. Identificación, análisis y eliminación (o mitigación a un nivel aceptable o tolerable) de los peligros, y los consiguientes riesgos, que amenazan la viabilidad de una organización.

1.3.10 La gestión de riesgos sirve para concentrar las actividades de seguridad operacional en aquellos peligros que presentan más riesgos.

1.4 EL SISTEMA DE GESTIÓN DE SEGURIDAD Y EL AMBITO DE OSINERGMIN

1.4.1 Los conceptos de gestión de seguridad como la forma de administrar las incertidumbres básicamente son universales, las metodología de identificación de

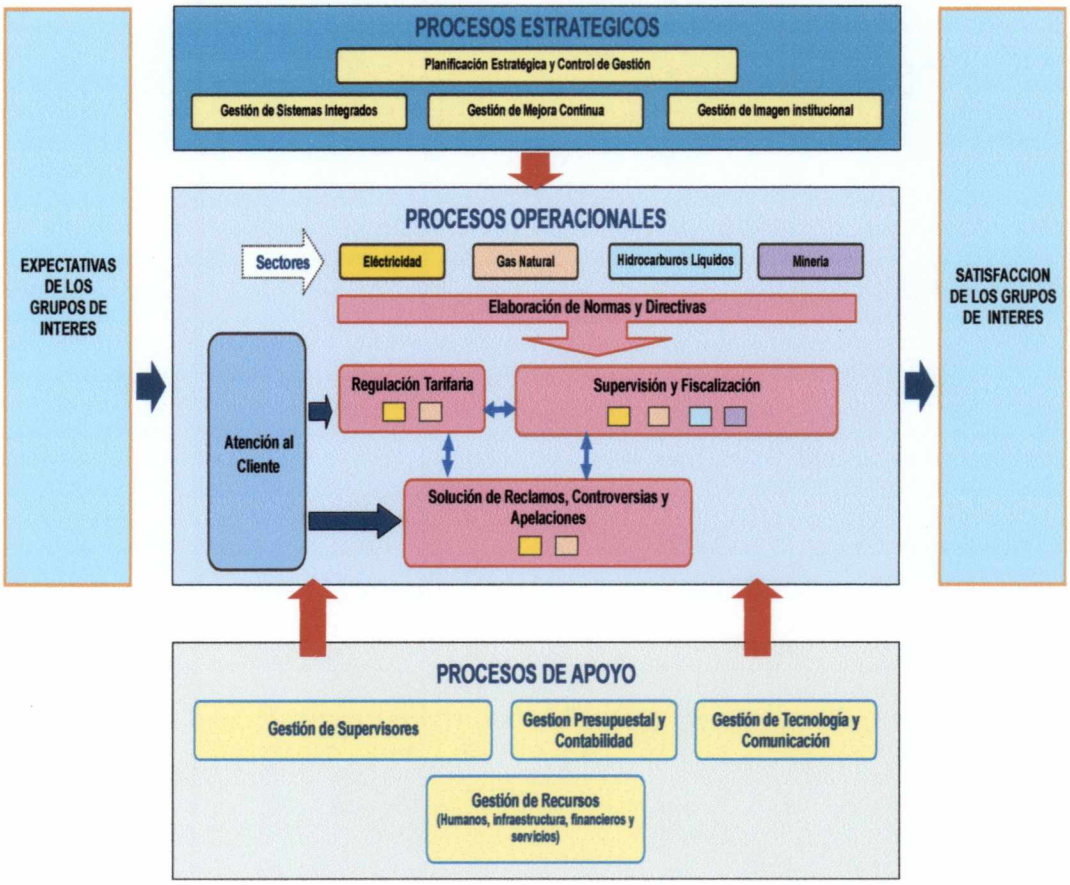
peligros, el análisis y la forma como realizan la gestión de riesgos las diferencian unas de otras.

Marco normativo

1.4.2 El Estado, por medio de los Ministerios Públicos, en su carácter de autoridad de reglamentación, establece entre otros aspectos, el marco normativo para que en el territorio nacional se realicen actividades seguras y eficientes

1.4.3 El Estado dispuso que OSINERGMIN sea el órgano competente, con las facultades necesarias para asegurar el cumplimiento de los reglamentos, disposiciones técnicas y legales referidas al medio ambiente y a la seguridad y los riesgos eléctricos en los subsectores de hidrocarburos, electricidad y minería.

1.4.4 OSINERGMIN dentro del desarrollo de sus procesos internos establece mecanismos para regular, supervisar y fiscalizar la seguridad de la inversión para asegurarse de que los explotadores y los proveedores de servicios mantienen un nivel aceptable de seguridad en sus actividades.



1.4.5 OSINERGMIN para el cumplimiento del marco normativo enunciado en los párrafos anteriores, desarrolla una estructura organizacional con procesos estratégicos (creadores de valor), procesos operacionales y de apoyo como (generadores de valor)

1.4.6 Defiende valor en sus procesos operacionales en la medida que cuenta con sistemas de gestión de seguridad OHSAS: 18001:2007 e ISO 14001:2004 y vela por el

cumplimiento de las reglamentaciones estipuladas. Pero el concepto de defender valor es un poco más amplio, el defender valor es tener una organización confiable que controle y mitigue las consecuencias de los probables peligros en la ejecución de las actividades de la cadena de valor de la organización, **mediante un sistema de gestión de seguridad y un programa de seguridad operacional.**

Se entiende como un programa de seguridad operacional al conjunto integrado de reglamentos y actividades encaminados a mejorar la seguridad

Una vista panorámica de los procesos internos de OSINERGMIN en relación a la gestión de seguridad

1.4.7 En los procesos estratégicos OSINERGMIN tendría incertidumbres (peligros) generadas por variables del entorno que están fuera de su control, que sería conveniente convertirlas a riesgos para poder medirlas y así establecer las estrategias de mitigación respectivas. Por ejemplo: El peligro de la interferencia política. Las alianzas de los grupos de interés.

1.4.8 Asimismo, los procesos estratégicos tendrían otros peligros que no son generadas por variables del entorno, si no por, peligros de información para la toma de decisiones tales como, análisis del entorno, medición del desempeño, arquitectura de las tecnologías de información, planificación estratégica etc.

1.4.9 Del mismo modo en los procesos operacionales, donde las incertidumbres (peligros) se centrarían en los siguientes aspectos:

a) Peligros de operación

1) Satisfacción de los grupos de interés.
2) Recursos actuales.
3) Desarrollo actual del producto ó servicio en relación al cumplimiento de la misión.
4) Eficacia
5) Eficiencia
6) Capacidades para el cumplimiento de la misión.
7) Cumplimiento
8) Defectos del desarrollo del producto ó servicio

b) Peligros de dirección.

1) Liderazgo
2) Disposición al cambio
3) Comunicaciones internas
4) Autoridad
5) Limites de los outsorcing

c) Peligros de la información y su procesamiento

Nota: Las variables de peligro descritas son las variables del modelo internacional de riesgos, que no necesariamente todas ellas sean peligros para OSINERGMIN. Variables que durante la implantación del Sistema de Gestión de Seguridad (SGS) se analizaran cuando se encuentren en la etapa de identificación de peligros

Desarrollo del sistema de gestión de seguridad de los procesos internos de OSINERGMIN

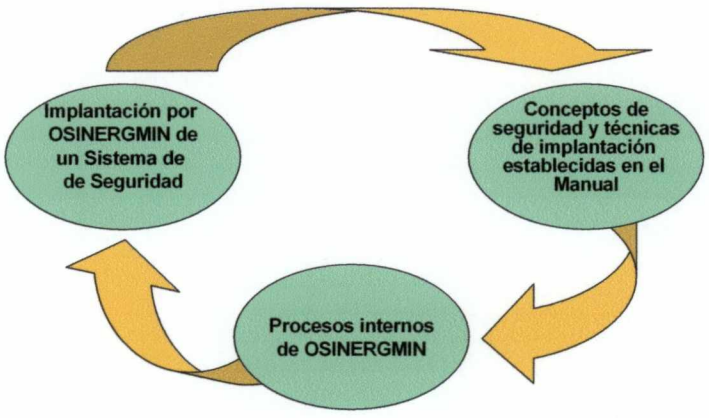
1.4.10 En el presente Manual se van a desarrollar los conceptos y la forma de cómo implantar un sistema de gestión de seguridad. Los procesos internos actuales tienen como ventaja que la mayor parte de los procesos se encuentran documentados y supervisados por auditorias internas y externas. Dicho de otro modo, al tener una gran parte certificada con un sistema de gestión de calidad en base a la norma ISO 9001:2008 y al modelo de excelencia en la gestión, las primeras barreras de defensas en el sistema de seguridad se encuentran implantadas. **Axioma de gestión**: No se puede tener seguridad sin previamente haber asegurado la calidad de los procesos.

1.4.11 La norma ISO 9001:2008 es una norma de gestión de calidad orientada a la satisfacción del cliente, dicho de otro modo, se concentra en o los productos o servicios de las operaciones. El sistema de gestión de seguridad se concentra en la seguridad, los aspectos humanos y organizacionales de las operaciones es decir, para satisfacer la seguridad. El sistema de gestión de OSINERGMIN es orientada a los grupos de interés donde el cliente es parte del grupo de interés. El modelo de excelencia en la gestión cumple con esta función integradora.

1.4.12 **Una parte del grupo de interés requiere la satisfacción de la seguridad,** tal como se evidencia en el establecimiento de la visión, misión de OSINERGMIN y a lo dispuesto en la ley Nº 26734 artículo 5, así también por la Contraloría General de la Republica dispuesta en su RC Nº 320-2006-CG Normas de Control Interno y en su RC Nº 458-2008-CG Guía para la Implementación del Sistema de Control Interno de las entidades del Estado.

1.4.13 El tener la certificación OHSAS: 18001:2007 e ISO 14001:2004 ayuda mucho en la implantación del sistema de gestión de seguridad, ya que estas y la correspondiente al peligro de la información y a su procesamiento son las más laboriosas.

1.4.14 En el siguiente gráfico se intenta resumir el concepto de desarrollo del sistema de seguridad de los procesos internos.



En relación al programa de seguridad operacional

1.4.15 El Reglamento de Organización y Funciones establece, entre otros, que OSINERGMIN debe **"velar por las mejores condiciones de calidad, seguridad, oportunidad y precio de las entidades de los subsectores de su ámbito,** verificando asimismo el cumplimiento de sus obligaciones técnicas, legales y las derivadas de los contratos de concesión, en la realización de dichas actividades, cautelando la adecuada conservación y protección del medio ambiente.

1.4.16 La misión del OSINERGMIN es regular, supervisar y fiscalizar, en el ámbito nacional, el cumplimiento de las disposiciones legales y técnicas relacionadas con las actividades de los subsectores de electricidad, hidrocarburos y minería, así como **el cumplimiento de las normas legales y técnicas referidas a la conservación y protección del medio ambiente** en el desarrollo de dichas actividades. (Artículo 2 de la Ley Nº 26734)

1.4.17 En el párrafo (e) (Artículo 5 de la Ley Nº 26734), son funciones de OSINERGMIN.... Fiscalizar y supervisar el cumplimiento de las disposiciones técnicas y legales del subsector electricidad, **referidas a la seguridad y riesgos eléctricos,** por parte de empresas de otros sectores, así como de toda persona natural o jurídica de derecho público o privado, informando al organismo o sector competente sobre las infracciones cometidas, las que le informarán de las sanciones impuestas

1.4.18 El conjunto integrado de disposiciones técnicas, legales referidas al medio ambiente, riesgos eléctricos **y actividades** encaminadas a mejorar la seguridad operacional de los explotadores se llama **"programa de seguridad operacional"** cuyo objetivo primario es la seguridad pública.

1.4.19 Un programa de seguridad operacional tiene un alcance amplio, e incluirá muchas actividades de seguridad dirigidas a alcanzar **los objetivos del programa.** El programa de seguridad operacional de OSINERGMIN debería comprender los reglamentos y las instrucciones para la realización de operaciones seguras por los explotadores y los que proveen servicios en los subsectores del ámbito de OSINERGMIN. El programa de seguridad operacional puede incluir disposiciones para diversas actividades, tales como notificación de incidentes, investigaciones de seguridad, auditorías de seguridad y promoción de la seguridad.
Poner en práctica las actividades conducentes a la seguridad de modo integrado exige un SGS coherente.

Estrategias para la consolidación del programa de seguridad operacional

1.4.20 OSINERGMIN tiene de ya un programa de seguridad operacional, programa que contiene actividades de regular supervisar y fiscalizar el cumplimiento de las disposiciones técnicas y legales establecidas en los subsectores de su ámbito. Pero, no se ha encontrado evidencia que se hayan planteado objetivos de calidad y/o seguridad a cada explotador o proveedor de servicios a fin de velar por las mejores condiciones de calidad, seguridad, oportunidad y precio tal como lo establece el Reglamento de Organización y Funciones.

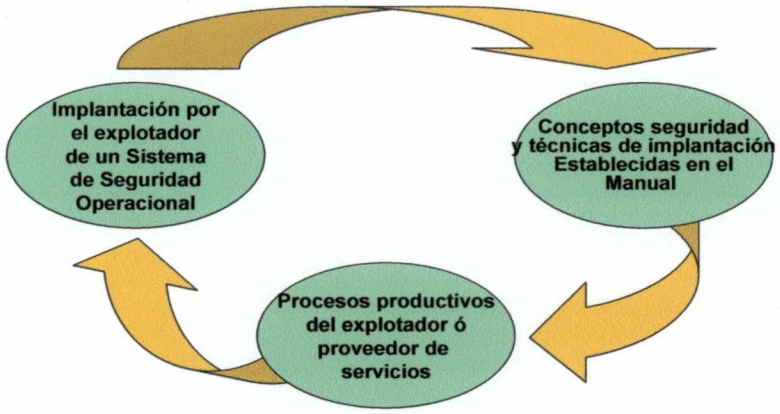
1.4.21 Por lo tanto, OSINERGMIN exigirá que cada explotador, proveedor de servicios ponga en práctica un SGS aprobado por el ente regulador, del mismo modo que la Contraloría General de la Republica lo dispone. Como mínimo, los SGS deberán:

a) Identificar los peligros para la seguridad operacional.

b) Asegurar que se aplican las medidas correctivas necesarias para mitigar los riesgos y peligros.

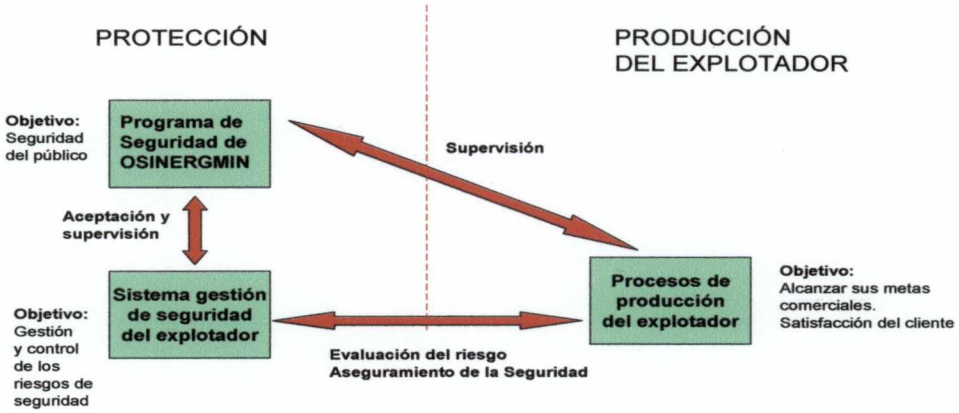
c) Prever una supervisión permanente y una evaluación periódica del nivel de seguridad operacional logrado.

1.4.22 El SGS de una organización aprobado por OSINERGMIN también deberá definir claramente las líneas de responsabilidad por la seguridad operacional, e incluirá una responsabilidad directa del personal administrativo superior con respecto a la seguridad operacional.



1.4.23 El objetivo final es tener un sistema integrado de seguridad alineado a la misión, tal como se muestra en el siguiente gráfico

Programa de Seguridad de OSINERGMIN + SGS del explotador + SGS de OSINERGMIN de los procesos internos = Sistema Integrado de Gestión de Seguridad de OSINERGMIN



1.5 CONTENIDO DEL MANUAL

Capítulo 1: Introducción. Aspectos Generales.
Capítulo 2: Conceptos básicos de seguridad.
Capítulo 3: Introducción a la Gestión de Seguridad.
Capítulo 4: Peligros.
Capítulo 5: Riesgos
Capítulo 6: Establecimiento de un sistema de Gestión de Seguridad Operacional.

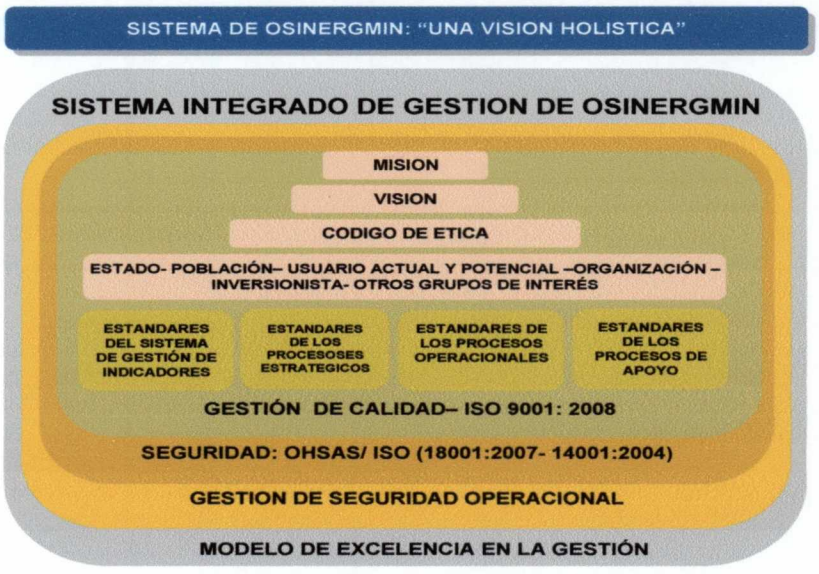
1.6 ESTRUCTURA DEL MANUAL

El presente Manual es diseñado bajo un enfoque modular. El capítulo 2 establece los fundamentos en base a conceptos contemporáneos de seguridad. El capitulo 3 nos muestra los conceptos básicos de gestión de seguridad poniendo énfasis porque la seguridad debe ser tratada como un sistema de gestión. Los capítulos 4 y 5 nos muestra el marco dogmático como base para una gestión de riesgos de seguridad y explicar sus dos (2) conceptos básicos: peligros y riesgos de seguridad. Finalmente, desde el capítulo 6 al 9 se presenta un enfoque del diseño, la puesta en práctica y el mantenimiento de procesos para gestionar la seguridad, proponiendo así un Programa de Seguridad Operacional (PSO) y un Sistema de Gestión de Seguridad (SGS) como sistemas de gestión para gestionar la seguridad dentro de las empresas del ámbito de OSINERGMIN así como la de propia organización respectivamente, y, la noción de gestión como una actividad sistemática.

1.7 MARCO LEGAL

1.7.1 Ley del Organismo Supervisor de Inversión en Energía – OSINERG LEY Nº 26734
1.7.2 Resolución de Contraloría General Nº 320-2006-CG
1.7.3 Resolución de Contraloría General Nº 458-2008-CG

1.8 MODELO ESTRUCTURAL DE GESTIÓN DE OSINERGMIN



CAPÍTULO 2

CONCEPTOS BÁSICOS DE SEGURIDAD

2.1 OBJETIVO Y CONTENIDO.

2.1.1 OBJETIVO

Este capítulo revisa las fortalezas y debilidades de enfoques metodológicos que se encuentran arraigados al tema de seguridad, y propone nuevas perspectivas y conceptos que son la base de un enfoque contemporáneo de seguridad.
Estas nuevas perspectivas y conceptos son actualmente las mejores prácticas de sistemas de gestión de seguridad en muchas organizaciones cuyo desarrollo se encuentran en la etapa de madurez, tales como los sectores nucleares y la aviación comercial internacional.

2.1.2 Este capítulo incluye lo siguiente:

- Concepto de seguridad.
- Evolución del concepto de seguridad.
- El concepto de causalidad de los actos no deseados – Modelo de Reason
- La "no conformidad" ó acto no deseado organizacional
- Errores y violaciones
- Cultura organizacional

2.2 CONCEPTO DE SEGURIDAD

2.2.1 Dependiendo de la perspectiva que se adopte, el concepto de seguridad en OSINERGMIN puede tener diferentes connotaciones, tales como:

a) ningún accidente (o incidente grave), opinión que sostiene ampliamente la Alta Dirección;

b) ausencia de peligro o riesgos, es decir, de aquellos factores que causan o que probablemente causen perjuicios;

c) actitud de los empleados con respecto a actos y condiciones inseguras (que reflejan una cultura "segura" de la organización);

d) grado en que los riesgos inherentes a las empresas del ámbito de OSINERGMIN son *"aceptables"*;

e) proceso de identificación de peligros y gestión de riesgos;

f) control de pérdida accidental (de personas y bienes, y daños al medio ambiente);

g) etc.

2.2.2 Independientemente de la connotación que uno podría escoger, todos ellos tienen la siguiente concordancia: la posibilidad del control absoluto. Cero actos no deseados, ausencia de peligros, etc, etc, nos permiten generar la idea que sería posible, según sea el diseño ó la intervención de OSINERGMIN para tener bajo control, tanto bajo el contexto operacional como el administrativo, todas las variables que puedan precipitar actos no deseados o resultados perjudiciales. Sin embargo, mientras la eliminación de actos no deseados, que pueden ser accidentes y/o incidentes serios,

el logro del control absoluto seguramente sería deseable, tales absolutos de control son objetivos inaccesibles en contextos abiertos y dinámicos operacionales.
En contextos abiertos tales como el entorno, OSINERGMIN tiene una serie de variables que están fuera de su control, tal como la injerencia política, la generación de nuevas regulaciones que dificultan el cumplimiento de la misión.
En contextos dinámicos operacionales las fallas y errores operacionales de las empresas que se encuentran en su ámbito, los peligros siempre van a existir a pesar de lo mejor y los esfuerzos más dotados para prevenirlos. Ninguna actividad humana o un sistema hecho por el hombre pueden garantizar la ausencia de peligros y errores operacionales.

2.2.3 La seguridad es por lo tanto un concepto que abarca aspectos más relativos que absolutos, por el cual los riesgos de seguridad surgen de las consecuencias de los peligros que en contextos operacionales debe ser aceptable en un sistema intrínsecamente seguro.
El problema clave todavía reside en el control, pero en el relativo más que en el control absoluto. Mientras los riesgos de seguridad y errores operacionales son considerados bajo un grado razonable de control, un sistema - abierto y dinámico, como la generación de energía- se considera como seguro. En otras palabras, los riesgos de seguridad y los errores operacionales que son controlados a un grado razonable son aceptables en un sistema intrínsecamente seguro.

2.2.4 La seguridad cada vez más es vista como el resultado de la gestión de ciertos procesos de la organización, que tienen el objetivo de mantener en control los riesgos de seguridad determinados por las consecuencias de los peligros en los contextos operacionales. De este modo, para el propósito de este manual, seguridad se considera, que tenga el siguiente significado:

Seguridad *es el estado en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos.*

2.3 EVOLUCIÓN DEL CONCEPTO DE SEGURIDAD

2.3.1 Dados los pronósticos de aumento continuo de las actividades mundiales de la industria, existe la preocupación de que los métodos tradicionales para reducir los riesgos a un nivel aceptable quizá no sean suficientes. Por consiguiente, están apareciendo nuevos métodos para comprender la seguridad y llevar a cabo su gestión.

2.3.2 La evolución de la gestión de la seguridad puede observarse desde dos puntos de vista diferentes: tradicional y moderno.

Enfoque tradicional.

2.3.3 Históricamente, la seguridad se concentraba en el cumplimiento de requisitos reglamentarios cada vez más complejos. Este enfoque funcionó bien hasta fines del decenio de 1970, cuando la tasa de actos no deseados acusó un aumento pronunciado. Los actos no deseados continuaban ocurriendo a pesar de todos los reglamentos.

2.3.4 Este enfoque respecto a la seguridad **reaccionaba** ante sucesos indeseables prescribiendo medidas para impedir que volvieran a ocurrir. En vez de definir mejores prácticas o los niveles deseados, ese enfoque procuraba asegurar que se respetaran los niveles mínimos.

2.3.5 Mientras este enfoque era bastante eficaz en la identificación **"que"** pasó, **"quien"** lo hizo, **"y cuando"** pasó, era considerablemente menos claro en la revelación **"por**

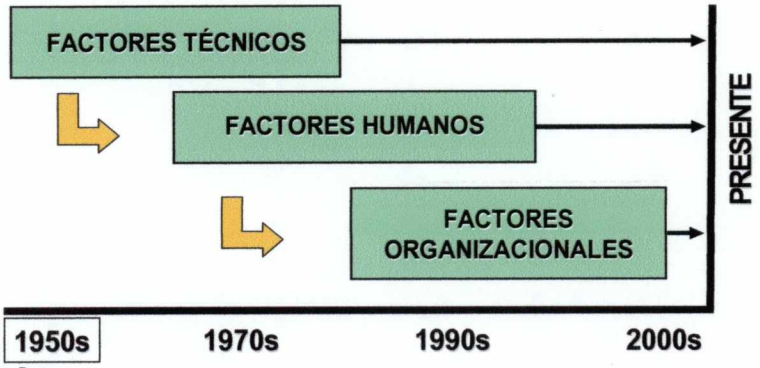
qué" "y como" pasó. Mientras en cierta época era importante entender "el que", "quien" "y cuando", cada vez más se hizo necesario de entender "el por qué" "y el como" para entender totalmente las interrupciones de un estado de seguridad aceptable. En años recientes, el progreso significativo ha sido hecho en el alcanzar este entendimiento.

Enfoque moderno.

2.3.6 Complementando un **marco sólido** de leyes y requisitos, las organizaciones, a fin de mantener los riesgos para la seguridad en un nivel aceptable con niveles de actividad más elevados, están aplicando prácticas modernas de gestión de la seguridad, dejando de actuar por **reacción** para actuar de un modo más **preventivo**.

2.3.7 Este nuevo modo, y la necesidad de saber el "porque" y "como paso" hizo evolucionar el pensamiento en aspectos de seguridad, donde el Doctor James Reason diseño un modelo de causalidad que se utiliza actualmente en los sistemas de seguridad más exigentes como las plantas nucleares y los sistemas de seguridad de aviación civil entre otros.

La evolución del pensamiento en materia de seguridad



Fuente: James Reason

2.4 EL CONCEPTO DE CAUSALIDAD DE LOS ACTOS NO DESEADOS. MODELO REASON

2.4.1 La aceptación a nivel de toda la industria y la necesidad de preveer actos no deseados (no conformidades) en la organización, fue hecha posible por un simple y poderoso modelo desarrollado por el Profesor James Reason. Modelo que tiene la ventaja de haberse diseñado gráficamente lo cual facilita su comprensión y aplicación. Este modelo proporciona el medio para entender como un sistema funciona satisfactoriamente o deriva con rumbo al fracaso.

Según este modelo, los actos no deseados requieren de la llegada en forma conjunta de un número de factores que por si solos no son suficientes para quebrar las defensas del sistema.

En un sistema de generación de energía, por ejemplo, generalmente los sistemas tienen varias capas de defensas, donde la falla de una defensa raramente tiene efectos consecuenciales.

Las fallas de grandes equipos o los errores del personal de operaciones raramente son la causa de que se quiebren las defensas en la seguridad, pero más bien son los gatillos. A menudo, estos trastornos son una consecuencia retrasada de decisiones hechas en los niveles más altos del sistema, que permanecen inactivos hasta que sus efectos o su no conformidad potencial sean activados por un conjunto específicos de circunstancias operacionales. En tales circunstancias específicas,

fracasos humanos o **fallas activas** en el nivel operacional actúan como los gatillos de **condiciones latentes** conducentes a facilitar la quiebra de las defensas inherentes a la seguridad del sistema. En el concepto del modelo de James Reason, los actos no deseados (no conformidades) incluyen una combinación tanto de condiciones activas como de latentes.

2.4.2 Las fallas activas son acciones o inacciones, incluyendo errores y violaciones que tienen un efecto inmediato adverso. Ellos generalmente son vistos - con la ventaja de la retrospección - **como actos inseguros.** Las fallas activas generalmente son asociadas con el personal de primera línea que podría causar un resultado no deseado (tales como los encargados directos en OSINERGMIN de regular, supervisar y fiscalizar, en el ámbito nacional, el cumplimiento de las disposiciones legales y técnicas relacionadas con las actividades de los subsectores de electricidad, hidrocarburos y minería, así como el cumplimiento de las normas legales y técnicas referidas a la conservación y protección del medio ambiente en el desarrollo de dichas actividades) En el caso de las empresas que OSINERGMIN supervisa, son el personal encargado de las operaciones.

Estos actos inseguros pueden penetrar las diversas defensas existentes para proteger la organización creadas por la administración de la organización, las autoridades de reglamentación, etc. y dar como resultado un acto no deseado.
Estos actos inseguros pueden ser el resultado de errores ordinarios o pueden ser el resultado de infracciones deliberadas de las prácticas y los procedimientos prescritos. El modelo reconoce que en el lugar de trabajo hay muchas condiciones que conducen al error o a generar infracciones y que pueden afectar al comportamiento individual o de equipo.

2.4.3 Estos actos inseguros se cometen en un contexto operacional que incluye ***condiciones inseguras latentes***. *Una condición latente es el resultado de una acción o decisión adoptada mucho antes de un acto no deseado (no conformidad).* Sus consecuencias pueden permanecer latentes durante mucho tiempo. Por si solas, estas condiciones latentes generalmente no son perjudiciales, puesto que, en primer lugar, no se perciben como fallas.

2.4.4 Las condiciones inseguras latentes sólo pueden llegar a ser evidentes una vez que se han quebrado las defensas del sistema. Estas condiciones puedan haber estado presentes en el sistema mucho antes de un acto no deseado (no conformidad) y generalmente las crean quienes toman decisiones o las autoridades de reglamentación y otras personas que están muy lejos, en tiempo y espacio, del acto no deseado. El personal que ejecuta las operaciones puede heredar defectos del sistema, tales como objetivos incompatibles (por ejemplo, calidad en el servicio o bien seguridad operacional); defectos de organización (por ejemplo, comunicaciones internas deficientes); o malas decisiones de la administración (por ejemplo, la postergación de una capacitación al personal de supervisores). La **perspectiva** que es la base de todo sistema de gestión se orienta en identificar y mitigar estas condiciones inseguras latentes en todo el sistema, en vez de realizar actividades localizadas para reducir a un mínimo los actos inseguros de los individuos. Esos actos inseguros sólo pueden ser síntomas de problemas de seguridad, no causas.

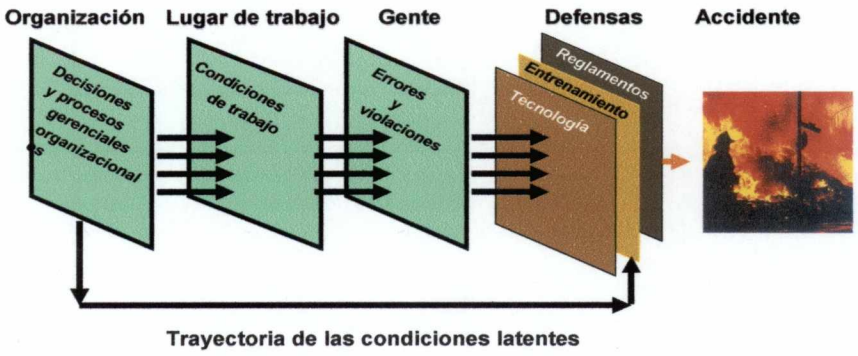
2.4.5 Aun en las organizaciones mejor dirigidas, la mayoría de las condiciones inseguras latentes comienzan en quienes toman las decisiones. Este personal directivo también está sujeto a limitaciones y predisposiciones humanas normales, así como también a limitaciones de tiempo, presupuestarias, políticas y de otro tipo muy reales. Dado que algunas de estas decisiones inseguras no pueden evitarse, deben adoptarse medidas para detectarlas y reducir sus consecuencias perjudiciales.

2.4.6 Las decisiones falibles de los encargados de la gestión de operaciones pueden traducirse en procedimientos inadecuados, programación deficiente o negligencia de los peligros reconocibles. Esas decisiones pueden conducir a pericias y conocimientos inadecuados o a procedimientos operacionales improcedentes. La

forma en que los encargados de la gestión de operaciones y la organización en su totalidad desempeñan sus funciones, establece las condiciones en que se produce un error o una violación. Las decisiones falibles adoptadas por la administración de la organización y las autoridades de reglamentación muy a menudo son la consecuencia de recursos inadecuados. Sin embargo, evitar los costos de reforzar la seguridad operacional del sistema puede facilitar actos no deseados que resultan tan caros como la bancarrota del explotador.

2.4.7 En la siguiente figura se muestra en forma gráfica el modelo de James Reason, de tal forma que nos ayude a entender la interacción de la organización y los factores de gestión en la causalidad de un acto no deseado ó no conformidad como lo expresaríamos en un sistema de gestión de calidad bajo una estructura de la norma ISO 9001:2008. Varias defensas en profundidad son construidas en un sistema para proteger las fluctuaciones en el desempeño humano o inconvenientes decisiones en todos los niveles del sistema (por ejemplo el lugar de trabajo, en los niveles de los encargados de las operaciones, de la Alta Dirección, entre otros). Las defensas son recursos proporcionados por el sistema para protegerse contra los riesgos de seguridad que las organizaciones que participan en actividades de producción generan y deben controlar. Este modelo muestra que mientras factores organizacionales, incluyendo decisiones de la dirección, pueden crear las condiciones latentes que podrían quebrar las defensas del sistema, ellos también contribuyen a la robustez de las defensas de la misma.

Modelo de causalidad de los actos no deseados (no conformidades)



Fuente: James Reason

2.5 LA NO CONFORMODIDAD Ó ACTO NO DESEADO ORGANIZACIONAL

2.5.1 La Organización de Aviación Civil Internacional (OACI) a través de un enfoque de bloques transmite en forma muy objetiva la noción de un acto no deseado ó no conformidad ó accidentes que es la base del modelo de James Reason. Esta noción, la OACI la caracteriza en cinco (5) bloques.

Fuente: OACI

2.5.2 El bloque superior representa los **procesos organizacionales.** Estas son **actividades sobre las cuales cualquier organización tiene un cierto grado razonable de control directo.** Los ejemplos típicos de tales procesos organizacionales incluyen: generación de políticas, planificación, comunicación, asignación de los recursos, supervisión etcétera, etcétera. Incuestionablemente, los dos procesos fundamentales de organización por lo que la seguridad está preocupada son la asignación de los recursos y la comunicación. Procesos que OSINERGMIN no tiene ningún problema, pero si es una incertidumbre en las empresas que supervisa.
Los inconvenientes o carencias de estos procesos organizacionales son el caldo de cultivo para un camino dual hacia el fracaso.

2.5.3 Otro camino es el camino de condiciones latentes. Los ejemplos de condiciones latentes pueden incluir: deficiencias en el diseño de los equipos, procedimientos estándar incompletos/incorrectos, deficiencias de entrenamiento, etcétera, etcétera. En términos genéricos, las condiciones latentes pueden ser agrupadas en dos grandes vertientes. Una vertiente es una **inadecuada identificación de peligros y gestión de riesgos de seguridad,** por el cual los riesgos de seguridad y las consecuencias de los peligros no son mantenidos bajo control, pero vagan libremente a lo largo del sistema para tarde o temprano hacerse activos por gatillos operacionales.

2.5.4 La segunda vertiente se conoce como la **normalización de la desviación,** una noción que, simplemente es indicativo de contextos operacionales donde la excepción se hace la regla. La asignación de los recursos en este caso contiene imperfecciones hasta el extremo. Como una consecuencia de la carencia de recursos, el único camino que el personal, quien es directamente responsable del desempeño real de las actividades de operación, puede alcanzar satisfactoriamente el logro de sus actividades es adoptando accesos rápidos que implican la violación constante de las reglas y procedimientos.

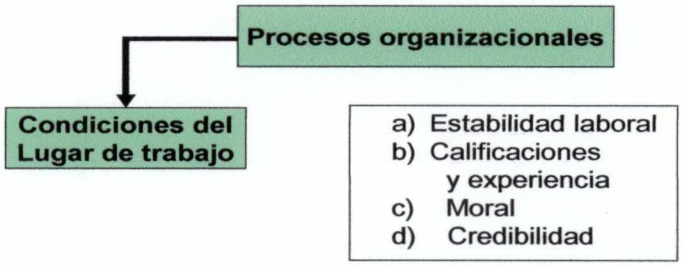
Condiciones presentes en el sistema antes del acto no deseado que se evidencian por factores desencadenantes.

2.5.5 Las condiciones latentes tienen todo el potencial para quebrar las defensas de un sistema. En las organizaciones, las defensas pueden ser agrupadas en tres (3) grandes grupos: tecnología, entrenamiento y reglamentaciones. Las defensas son por lo general la última red de seguridad para contener las condiciones latentes, así como las consecuencias de los lapsos en el desempeño humano. Es más, si no es todo, las estrategias de mitigación contra los riesgos de seguridad, determinados de las consecuencias de los peligros, están basados sobre el refuerzo de defensas existentes o el desarrollo de nuevas defensas.

Por ejemplo, una organización que OSINERGMIN supervisa. Esta organización tiene un sistema de gestión de seguridad y ante determinado riesgo tiene implantado como primera defensa un equipo de detección, como segunda defensa el entrenamiento que le ha brindado a su personal, como tercera defensa tiene sus procedimientos que son realizados en función de las disposiciones del ente regulador (OSINERGMIN), como cuarta defensa la supervisión por la organización y como quinta defensa la supervisión de OSINERGMIN. La cuarta y quinta defensa deben ser orientadas a buscar condiciones latentes y/o huecos que pueden tener las defensas implantadas, como por ejemplo, procedimientos mal confeccionados ó el personal no los usa, el entrenamiento no es el más adecuado etc. La pregunta es ¿Las empresas tienen identificados sus peligros? ¿Tienen defensas implantadas? ¿OSINERGMIN tiene identificadas las defensas de las empresas que supervisa?

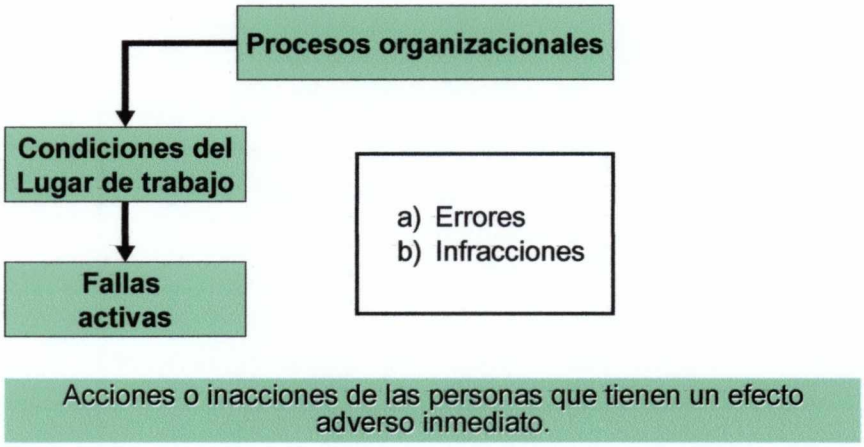
Recursos para protegerse de los riesgos que las organizaciones que realizan actividades productivas deben enfrentar.

2.5.6 Otro bloque que proviene de los procesos organizacionales son las condiciones del lugar de trabajo. Las condiciones del lugar de trabajo son factores que directamente influyen en la eficacia de las personas. Las condiciones de lugar de trabajo son en gran parte intuitivas, e incluyen condiciones como: estabilidad de trabajo, calificaciones y experiencia, moral, credibilidad de la dirección, factores de ergonomía tradicionales como iluminación, calefacción, refrigeración, etcétera, etcétera.

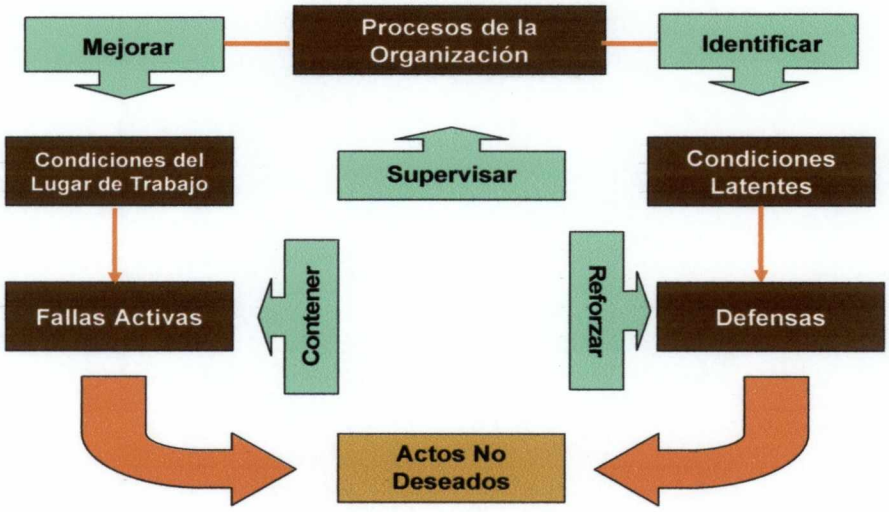


Factores que influencian directamente la eficacia de las personas en los lugares de trabajo de las empresas.

2.5.7 Las fallas activas son originadas por el personal de operaciones en su lugar de trabajo. Las fallas activas pueden ser consideradas como errores o como infracciones. La diferencia entre error e infracción es el componente de motivación: una persona que trata de hacer todo lo posible de lograr una tarea, siguiendo las reglas y procedimientos según el entrenamiento recibido, pero falla comete un error. Una persona que a sabiendas se desvía de las reglas, procedimientos o del entrenamiento recibido para lograr una tarea comete una infracción. Así, la diferencia básica entre error e infracción es la intención



2.5.8 Desde la perspectiva de la no conformidad ó acto no deseado organizacional, los esfuerzos de seguridad deberían ser la de **supervisar** el proceso organizacional para **identificar** condiciones latentes y así **reforzar** las defensas.
Los esfuerzos de seguridad también deberían **mejorar** condiciones de lugar de trabajo para **contener** fallas activas, porque la concatenación de todos estos factores produce interrupciones de seguridad



Fuente: OACI

2.6 ERRORES E INFRACCIONES

En los párrafos anteriores hemos mencionado error e infracción, para este concepto de seguridad también recurrimos a la Organización Internacional de Aviación Civil, por haber desarrollado muy bien el concepto, valga la redundancia, de error e infracción. Aspectos que son importantes y valederos en la gestión de OSINERGMIN. Tenemos que tener en claro que una infracción es un acto deliberado, mientras que un error no lo es.

Factores Humanos.

2.6.1 Los orígenes de algunos problemas que causan o contribuyen actos no deseados apuntan a un diseño deficiente del equipo o a los procedimientos, o a una formación o instrucciones para la utilización inadecuadas. Cualquiera sea el origen, es fundamental comprender las capacidades y las limitaciones de la actuación humana normal y el comportamiento en un contexto operacional para comprender la gestión de seguridad. Un enfoque intuitivo para los factores humanos ya no es apropiado.

2.6.2 El elemento humano es la parte más flexible y adaptable de los sistemas en los sectores de electricidad, hidrocarburos y minería, pero es también el más vulnerable a las influencias que pueden perjudicar su actuación. Dado que la mayoría de los actos no deseados resultan de una actuación humana que no llega a ser óptima, ha habido una tendencia a atribuirlos simplemente al error humano. Sin embargo, la expresión **"error humano"** no es muy útil para la gestión de seguridad. Si bien puede indicar **dónde** ocurrió la falla en el sistema, no proporciona orientación en cuanto a **por qué** ocurrió.

2.6.3 Un error atribuido a personas puede haber sido inducido por el diseño, o estimulado por una instrucción o un equipo inadecuado, procedimientos mal diseñados, o una presentación deficiente de las listas de verificación o de los manuales. Además, la expresión "error humano" permite ocultar los factores subyacentes que se deben sacar a la luz para evitar los actos no deseados. En el concepto moderno de seguridad, **el error humano es el comienzo en vez del final.** Las iniciativas de gestión de seguridad procuran encontrar formas de prevenir los errores humanos que pueden poner en peligro la seguridad y de reducir al mínimo las consecuencias perjudiciales de los errores que inevitablemente ocurrirán. Esto exige la comprensión del contexto en que se desarrollan las operaciones y en que las personas cometen errores (es decir, comprender los factores y condiciones que afectan a la actuación humana en el lugar de trabajo).

Tipos de error.

2.6.4 Los errores pueden producirse en la etapa de planificación o durante la ejecución del plan. Los, **errores de planificación** conducen a **equivocaciones**; sea que la persona sigue un procedimiento improcedente para tratar un problema ordinario, sea que construye un plan de medidas improcedentes para hacer frente a una nueva situación. Aun cuando la medida prevista sea apropiada, en la ejecución del plan pueden ocurrir errores. Los textos sobre factores humanos que tratan de esos errores de ejecución generalmente establecen una distinción entre descuidos y lapsus. Un **descuido** es una acción que no se llevó a cabo como estaba planeada y, por lo tanto, siempre se podrá observar. Un **lapsus** es una falla de la memoria y puede no ser necesariamente evidente para quien no sea la persona que la experimentó.

Errores de planificación (equivocaciones)

2.6.5 A la hora de resolver problemas intuitivamente buscamos un conjunto de reglas que son conocidas y han sido empleadas antes y que serán apropiadas para el problema de que se trata. Las equivocaciones pueden ocurrir de dos formas: la aplicación de

una regla que no es apropiada para la situación o la aplicación correcta de una regla imperfecta.

2.6.6 **Aplicación incorrecta de reglas buenas.** Esto ocurre generalmente cuando se está frente a una situación que presenta muchas características comunes con las circunstancias para las cuales se creó la regla, pero con algunas diferencias importantes. Si no se reconoce la importancia de las diferencias, podría aplicarse una regla que no es apropiada.

2.6.7 **Aplicación de reglas malas.** Esto ocurre cuando se usan procedimientos que en experiencias pasadas han demostrado funcionar, pero que contienen imperfecciones que no son conocidas. Si esa solución funciona en las circunstancias en que se usó por primera vez, puede llegar a ser parte del enfoque acostumbrado del individuo para resolver ese tipo de problemas.

2.6.8 Cuando una persona no tiene una solución basada en la experiencia previa o en la instrucción, esa persona acude a su conocimiento y experiencia personal. Desarrollar una solución para un problema empleando este método inevitablemente tomará más tiempo que aplicar una solución basada en una regla, puesto que requiere un razonamiento basado en el conocimiento de principios básicos. Las equivocaciones pueden ocurrir por la falta de conocimiento o por un razonamiento equivocado. La aplicación del razonamiento basado en el conocimiento a un problema será particularmente difícil en circunstancias en que el individuo está ocupado, o cuando su atención probablemente se desvíe del proceso de razonamiento para tratar otros problemas. La probabilidad de que ocurra una equivocación es mucho mayor en esas circunstancias.

Errores de ejecución (descuidos y lapsus)

2.6.9 Las acciones de personal experimentado y competente tienden a ser habituales y de mucha práctica; se realizan de un modo bastante automático, excepto para las verificaciones ocasionales del desarrollo de la tarea. Los descuidos y los lapsus pueden ocurrir como resultado de:

- **Descuidos de atención.** Estos ocurren como resultado de no seguir el desarrollo de una acción habitual en algún punto crítico. Esto es particularmente probable cuando el plan de acción es similar, pero no idéntico, a un procedimiento usado habitualmente. Si se permite que la atención se desvíe o que ocurra una distracción en el punto critico cuando la acción difiere del procedimiento habitual, puede resultar que la persona siga el procedimiento habitual en vez del que estaba previsto para el caso.
- **Lapsus de memoria.** Estos ocurren cuando olvidamos lo que habíamos planeado hacer omitimos algo en una secuencia de acciones previstas.
- **Errores de percepción.** Estos son errores de reconocimiento, que ocurren cuando creemos que vimos u oímos algo que es diferente de la información que se nos presentó en la realidad.

Errores e infracciones.

2.6.10 Los errores (que son normales en la actividad humana) son muy distintos de las infracciones. Ambos pueden conducir a una falla del sistema. Ambos pueden resultar en una situación peligrosa. La diferencia reside en la intención.

2.6.11 Una infracción es un acto deliberado, mientras que un error no lo es. Algunas infracciones son el resultado de procedimientos deficientes o poco realistas, cuando se han elaborado "soluciones" para evitar las dificultades de una tarea. En esos casos, es muy importante notificarlas tan pronto como se identifiquen a fin de que se puedan corregir los procedimientos. En todo caso, no deberían tolerarse las

infracciones. Ha habido actos no deseados ó no conformidades en que una cultura de empresa que toleraba o que, en algunos casos, alentaba que se tomaran atajos en vez de seguir los procedimientos publicados, había sido una causa que había contribuido para que ocurriera el acto no deseado ó no conformidad.

Control del error

2.6.12 Afortunadamente, pocos errores conducen a consecuencias perjudiciales, si descontamos los accidentes. Típicamente, los errores se detectan y corrigen sin que se produzcan resultados indeseables

2.6.13 Generalmente en la industria tienen tres (3) estrategias para manejar errores que son:

- **Estrategia de reducción de errores:** tienen por finalidad intervenir directamente en la fuente del error reduciendo o eliminando los factores que contribuyen a que ocurran errores. Ejemplo: Si los procesos organizacionales de OSINERGMIN, tales como una inadecuada comunicación en los niveles jerárquicos, procedimientos ambiguos, recursos insuficientes, presupuestos no adecuados etc, son caldo de cultivo para los errores operacionales.

- **Estrategia de captura de errores:** Capturar el error supone que se ha cometido un error. Se trata pues de *"capturar"* el error antes de que este produzca consecuencias perjudiciales. La captura de errores se diferencia de la reducción de errores en que no reduce o elimina directamente el error. Ejemplo: OSINERGMIN tomo una buena decisión de generar **escenarios, la complejidad y prospectiva del gas natural al 2030** con la finalidad analizar la industria de gas natural propiamente dicha, su interacción con industrias como la eléctrica, el contexto mundial y regional del desarrollo de fuentes de energía y dentro de ellas la de gas natural, y principales variables que afectarán su desempeño y accionar futuro, para prever los principales cambios en esta industria y plantear estrategias. De esos escenarios, estructurados entre el eje económico y el eje político, han debido llegar a la conclusión del escenario posible. Los otros escenarios deben ser controlados mediante una gestión de riesgos con estrategias claras de mitigación. El no tenerlas es un error

- **Estrategia de tolerancia:** La tolerancia de errores se refiere a la capacidad de un sistema para aceptar un error sin que ocurran consecuencias graves. Son ejemplos de medidas para aumentar la tolerancia de errores la incorporación de sistemas como el de gestión de calidad, riesgos, excelencia en los niveles estratégicos y operativos de la organización para que haya redundancia ó un programa de auditoría interna que prevea varias oportunidades para detectar no conformidades ó actos no deseados antes de que el error ó los factores que contribuyen a que ocurran errores, llegue a tener una dimensión critica.

2.7 CULTURA DE SEGURIDAD DE LA ORGANIZACIÓN.

2.7.1 Muchos factores crean el contexto para el comportamiento humano en el lugar de trabajo. La cultura de la organización o de la empresa establece los límites del comportamiento humano aceptable en el lugar de trabajo, estableciendo las normas de conducta y los límites. De este modo, la cultura de la organización o de la empresa constituye una piedra angular para la toma de decisiones de la administración y de los empleados: *"Así es como hacemos aquí las cosas"*.

2.7.2 La cultura de seguridad es un subproducto natural de la cultura de la empresa. La actitud de la empresa hacia la seguridad influye en el enfoque colectivo de los empleados al respecto. La cultura de seguridad operacional consiste en creencias, prácticas y actitudes compartidas. El tono de la cultura de seguridad operacional lo

establecen y alimentan las palabras y acciones del personal directivo de alto nivel. Así, la cultura de seguridad operacional de la empresa es la atmósfera que crea la administración y que da forma a las actitudes de los trabajadores respecto a la seguridad.

2.7.3 La cultura de seguridad resulta afectada por factores tales como:

a) medidas y prioridades de la administración;
b) políticas y procedimientos;
c) prácticas de supervisión;
d) planificación y objetivos de seguridad;
e) medidas en respuesta a comportamientos inseguros;
f) instrucción y motivación del personal; y
g) participación o adhesión de los empleados.

2.7.4 La responsabilidad final por la seguridad corresponde a la Alta Dirección y al personal directivo de la organización — que sea una planta generadora de energía, un proveedor de servicios etc. Las características de seguridad de una organización las establece desde el principio la medida en que la administración superior acepta la responsabilidad de operaciones seguras y la gestión de riesgos.

2.7.5 El modo en que los encargados de las operaciones de OSINERGMIN enfrentan las actividades cotidianas es fundamental para una buena cultura de seguridad. ¿Se sacan las conclusiones correctas de las experiencias de trabajo reales y se adoptan las medidas apropiadas? ¿Participan constructivamente los miembros del personal en este proceso o sienten que son víctimas de medidas unilaterales de los gerentes encargados de las operaciones?

2.7.6 La relación que tiene OSINERGMIN con los encargados de las operaciones de los explotadores que supervisa también indica si existe una cultura de seguridad sana o no. Esta relación debería distinguirse por la cortesía profesional, pero con suficiente distancia como para no comprometer la rendición de cuentas. La apertura, más que el estricto cumplimiento de los reglamentos, conducirá a una mejor comunicación en materia de seguridad. El primer enfoque alienta el diálogo constructivo, mientras que el segundo incita a ocultar o a ignorar los verdaderos problemas de seguridad.

Cultura de Seguridad Positiva.

2.7.7 Aunque el cumplimiento de los reglamentos de seguridad es fundamental para la seguridad de las operaciones, el pensamiento contemporáneo es que se necesita mucho más que eso. Las organizaciones que cumplen simplemente con las normas mínimas establecidas por los reglamentos no están en una buena posición para identificar los problemas de seguridad operacional que surgen.

2.7.8 Un modo eficaz de promover una actividad segura es que tanto OSINERGMIN como el explotador desarrolle una cultura de seguridad positiva. Dicho simplemente, todo el personal debe ser responsable y tener en cuenta las repercusiones de la seguridad en todo lo que hace. Esta manera de pensar debe estar tan arraigada que verdaderamente llegue a ser una *"cultura"*. Todas las decisiones, sean de la Alta Dirección, de los responsables de la planificación de la organización o de los funcionarios encargados de las operaciones, deben tomarse teniendo en cuenta las repercusiones sobre la seguridad.

2.7.9 Una cultura de seguridad positiva debe tener su origen en los niveles superiores y descansa en un elevado grado de confianza y respeto entre los trabajadores y la administración. Los trabajadores deben creer y sentir que tendrán apoyo en cualquier decisión que tomen en favor de la seguridad. También deben entender que las infracciones deliberadas de la seguridad que ponen en peligro las operaciones no serán toleradas.

2.7.10 Existe también un alto grado de interdependencia entre la cultura de seguridad y otros aspectos de un Sistema de Gestión de Seguridad. Una cultura de seguridad positiva es indispensable para el funcionamiento eficaz de un Sistema de Gestión de Seguridad. Sin embargo, la cultura de una organización también está determinada por la existencia de un Sistema de Gestión de Seguridad formal. Por lo tanto, una organización no debería esperar hasta que se haya logrado una cultura de seguridad operacional ideal para implantar un Sistema de Gestión de Seguridad. La cultura se irá desarrollando a medida que aumente el conocimiento y la experiencia respecto a la gestión de la seguridad operacional.

Señales de una cultura de seguridad positiva

2.7.11 Una cultura de seguridad positiva presenta los atributos que siguen:

a) La Alta Dirección pone mucho énfasis en la seguridad como parte de la estrategia de control de riesgos (es decir, reducir al mínimo las incertidumbres).

b) El personal directivo, de apoyo y el personal de operaciones tienen una opinión realista de los riesgos a corto y a largo plazo que presentan las actividades de la organización.

c) Quienes ocupan cargos altos:

1) Fomentan un clima en que hay una actitud positiva hacia las críticas, los comentarios y la información que se recibe de los niveles inferiores de la organización sobre asuntos de seguridad de las operaciones.

2) No emplean su influencia para imponer sus opiniones en los subordinados.

3) Aplican medidas para contener las consecuencias de las deficiencias de seguridad de las operaciones identificadas.

d) La Alta Dirección promueve un ambiente de trabajo que no es punitivo. Algunas organizaciones emplean la expresión "cultura justa" en vez de "no punitiva".

e) Existe en todos los niveles de la organización la conciencia y la importancia de comunicar información pertinente sobre la seguridad de las operaciones (tanto dentro como fuera de OSINERGMIN).

f) La existencia de procedimientos prácticos en relación a los tratamientos de los riesgos, la seguridad de las operaciones y las posibles fuentes de daños.

g) La incidencia de conductas arriesgadas es baja y la ética de seguridad desalienta ese comportamiento

Efectividad en el reporte de seguridad.

2.7.12 Uno de los aspectos más influyentes de una cultura de organización en términos de gestión de seguridad son los procedimientos y prácticas por el personal integrante de la organización. **La identificación de peligros es una actividad fundamental** que es la base de la gestión de seguridad. *Nadie está en una mejor posición para reportar la existencia de peligros, así como la realización de los procesos que el personal que los realiza, quienes tienen que vivir con y afrontar los peligros diariamente.* El reporte eficaz de peligros por el personal es por lo tanto **la piedra angular de la gestión de seguridad.** Por lo tanto, generar un ambiente de seguridad en el cual el personal ha sido entrenado a reportar los peligros, es el requisito previo para tener un sistema de reporte eficaz de seguridad.

2.7.13 El reporte eficaz de seguridad se construye sobre ciertos atributos básicos, como:

a) La Alta Dirección debe poner bastante énfasis sobre la identificación de peligros como parte de la estrategia para desarrollar una sólida gestión de seguridad, y como consecuencia de esa estrategia se debe generar la conciencia de la importancia de informar los peligros y asimismo, se comuniquen a todos los niveles de la organización.

b) La Alta Dirección y el personal de la organización tienen una visión compartida y realista de los peligros que están expuestas las actividades de la organización y, como una consecuencia, hay reglas y/o procedimientos realistas que se relacionan con esos peligros y con las fuentes potenciales de daño.

c) La Alta Dirección debe definir las exigencias que permita apoyar activamente el reporte de los peligros, primero, asegurando que los reportes de peligro son correctamente protegidos, segundo, demostrando una actitud receptiva al reporte de peligros por el personal y tercero, poniendo en práctica medidas para mitigar las consecuencias de los peligros.

d) En relación a la salvaguarda de los reportes de peligro, la Alta Dirección, debe promover un sistema de protección y verificación de modo que los reportes de peligros sean tratados en forma confidencial, que el reporte de peligro sea visto como una información proactiva y que será utilizado para el fin por la cual fue puesto en práctica (la gestión de seguridad).

e) El personal es entrenado para reconocer, reportar peligros y entender la incidencia y las consecuencias de los peligros en las actividades de la organización.

Efectividad en el reporte de seguridad: Cinco (5) rasgos básicos.

2.7.14 La observación de los resultados de sistemas avanzados de gestión de seguridad nos permite recoger cinco (5) rasgos comunes:

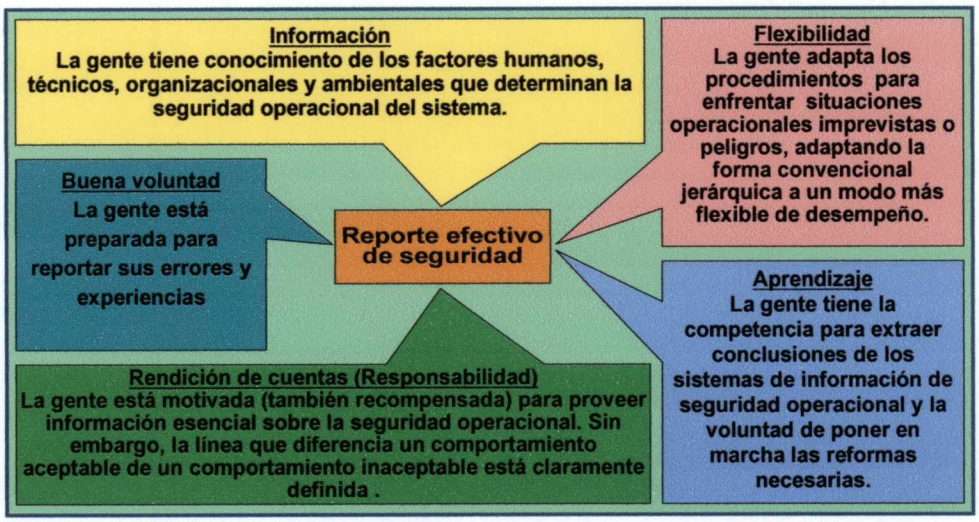
a) **Buena voluntad.** Como una consecuencia de los esfuerzos deliberados por la Alta Dirección de haber definido las exigencias necesarias para apoyar el reporte activo de peligros y asegure la salvaguarda de las mismas, lograremos que el personal de la organización esté dispuesto a reportar peligros, los errores operacionales que podrían generar peligros.

b) **Información.** Como una consecuencia del entrenamiento para reconocer, reportar peligros y entender la incidencia y las consecuencias de los peligros en las actividades que se desarrollan en la organización, el personal estará bien informado de los factores humanos, técnicos, organizacionales y ambientales que determinan la seguridad operacional del sistema.

c) **Flexibilidad.** Como una consecuencia de tener una visión compartida y realista de los peligros que están expuestas las actividades de la organización con reglas y/o procedimientos realistas que se relacionan con esos peligros y con las fuentes potenciales de daño, el personal puede adaptar los procedimientos para enfrentar situaciones operacionales imprevistas o peligros, adaptando la forma convencional jerárquica a un modo más flexible de desempeño.

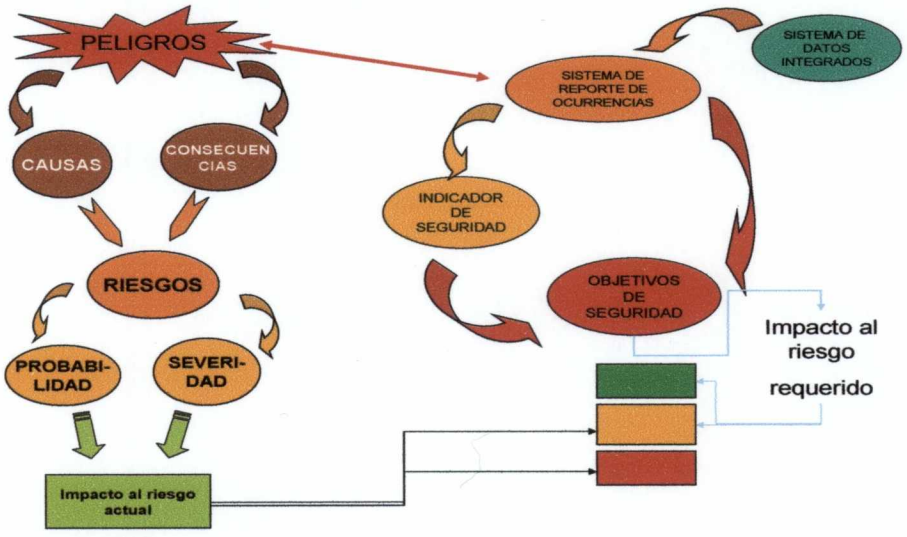
d) **Aprendizaje**. Como una consecuencia de la toma de conciencia de la importancia de información del peligro a todos los niveles de la organización, el personal tendrá la competencia para extraer conclusiones de los sistemas de información de seguridad y la voluntad de poner en marcha las reformas necesarias.

e) **Rendición de cuentas.** Como una consecuencia de que la Alta Dirección, promueve un sistema de protección y verificación de modo que los reportes de



peligros sean tratados en forma confidencial, así como el reporte de peligro es visto como una información proactiva y es utilizado para el fin por la cual fue puesto en práctica, motiva al personal para proveer información esencial sobre la seguridad operacional. Sin embargo, la línea que diferencia un comportamiento aceptable de un comportamiento inaceptable está claramente definida.

2.7.15 El reporte eficaz de seguridad es la piedra angular de la gestión de seguridad. Una vez reportado, la información sobre peligros es convertido en datos de seguridad. El reporte eficaz de seguridad es por lo tanto la puerta para la adquisición de datos de seguridad. Una vez los datos adquiridos, se debe realizar la gestión de seguridad. La gestión de datos de seguridad se construye sobre tres pasos claramente definidos. En los dos primeros, intervienen la gestión de datos de seguridad, que es la colección de datos de seguridad sobre peligros, y, el análisis de datos de seguridad, que se convierten en datos de información. El tercero, y el paso a menudo pasado por alto, son la mitigación o las actividades de respuesta de la organización a los peligros como una consecuencia de la información de seguridad desarrollada. La respuesta de una organización a la información de seguridad sobre peligros puede variar de la mitigación activa a la indiferencia ostensible.



Fuente: David Díaz

2.7.16 La literatura sobre aspectos organizacionales proponen tres (3) características de organización, dependiendo del grado de respuesta a la información de peligros y la información del sistema de gestión de seguridad:

- **Patológica** – Esconde la información
- **Burocrática** – Restringe la información
- **Generativas** – Valoriza la información

2.7.17 El siguiente cuadro se presenta una matriz que se explica por si sola, entre los aspectos más importantes de una gestión de información de seguridad y las características de las organizaciones descritas en el párrafo anterior.

Fuente: Ron Westrum

	Patológicas	**Burocráticas**	**Generativas**
Información	Escondida	Ignorada	Buscada
Mensajeros	Eliminados	Tolerados	Entrenados
Responsabilidades	Disimuladas	Encapsuladas	Compartidas
Reportes	Evitados	Permitidos	Recompensados
Fallas	Encubiertas	Disculpadas	Analizadas
Ideas nuevas	Restringidas	Problemáticas	Bienvenidas
Organización resultante	**Organización conflictiva**	**Organización burocrática**	**Organización confiable**

CAPÍTULO 3

GESTIÓN DE SEGURIDAD

Introducción

3.1 OBJETIVO Y CONTENIDO.

3.1.1 OBJETIVO

Este capítulo analiza la necesidad de estrategias y define las características importantes de la gestión de seguridad. El capítulo también establece las diferencias entre la gestión de seguridad como un proceso organizacional y la prevención de accidentes como una actividad remediadora.

3.1.2 Este capítulo incluye lo siguiente:

- Evolución del Sistema de Gestión de Seguridad en la industria.
- Conceptos de Gestión de Seguridad.
- Estrategias de Gestión de Seguridad
- Actividades claves para la Gestión de Seguridad
- Responsabilidades por la Gestión de Seguridad
- Proceso de Gestión de Seguridad.
- Vigilancia Operacional.

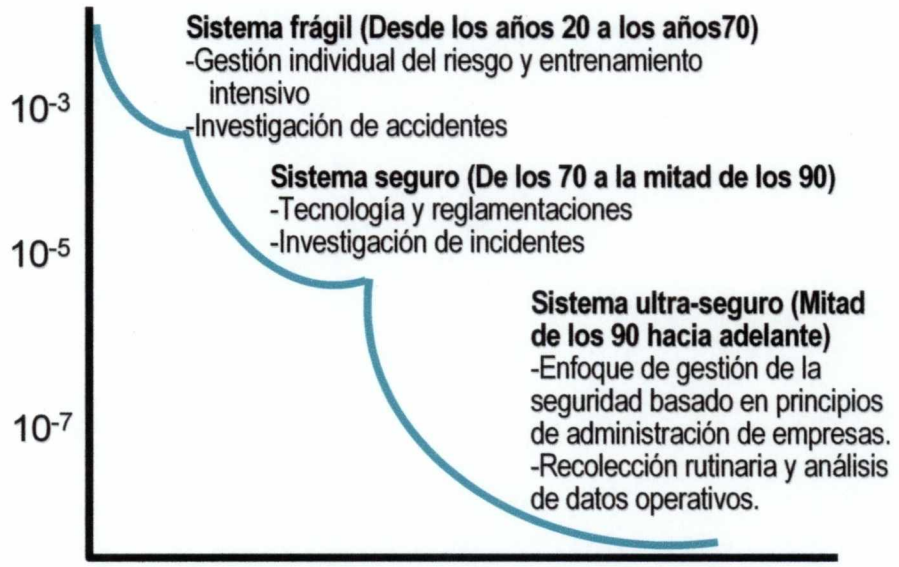
3.2 EVOLUCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INDUSTRIA.

3.2.1 Tradicionalmente, la necesidad de una gestión de seguridad ha sido justificada basada en un predicho crecimiento de la industria y el potencial aumento de accidentes como una consecuencia de tal crecimiento.
En retrospectiva, la historia del progreso de seguridad en las industrias puede ser dividida - justo como la evolución de los conceptos seguridad analizados en el Capítulo 2 - en tres eras distintas, cada uno con atributos fundamentalmente diferentes.

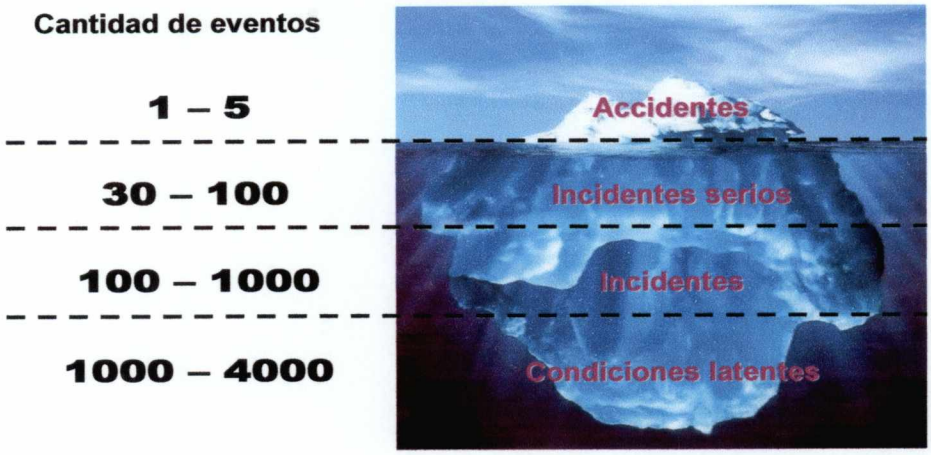
3.2.2 En la primera era, que los contamos a principios de los años de 1900 hasta aproximadamente finales de los años sesenta (los conceptos técnicos de seguridad analizada en el Capítulo 2), podría ser caracterizado en la industria en general como un sistema frágil bajo el punto de vista de confiabilidad en los sistemas de seguridad. Brechas de seguridad, aunque con ocurrencias no diarias, no eran infrecuentes. Era entonces lógico que solo el entendimiento de la seguridad y las estrategias de prevención fueran sacados principalmente de la investigación del accidente. No había realmente ningún sistema para hablar de, más bien la industria funcionó porque los individuos literalmente lo lanzaron sobre sus hombros y lo avanzaron. El enfoque de seguridad estaba sobre individuos y la gestión individual de riesgos de seguridad.

3.2.3 Es durante la segunda era, desde principios de los setenta hasta mediados de los noventa ciertas industrias no solo eran sistemas estructurados sino sistemas seguros. Las brechas de seguridad disminuyeron considerablemente y aún más una comprensión más realista de aspectos de seguridad, que pasaron de un enfoque más individualista a ir desarrollando progresivamente sistemas de seguridad. Naturalmente esta situación, partió de las lecciones aprendidas *de la investigación de accidentes y poniendo* ***mucho más énfasis en la investigación de incidentes***

3.2.4 Desde mediados de los años noventa hasta la actualidad (la época de la organización), ciertas industrias entraron en su tercera época de seguridad o de protección, convirtiéndose en sistemas ultra-seguros, (es decir, sistemas que tienen como experiencias de tener menos de una brecha de seguridad catastróficas por cada millón de ciclos de producción). Desde una perspectiva global, los accidentes se convirtieron en infrecuentes. Incidentes graves también se convirtieron en menos y muy espaciados. *En consonancia con* ***esta reducción de las ocurrencias,*** *el cambio hacia una amplia perspectiva sistémica de la seguridad que había comenzado a emerger durante la época anterior empieza a consolidarse.* Un aspecto fundamental en esta consolidación fue la adopción de un enfoque de negocios en la gestión de la seguridad, basado en la recopilación y análisis de rutina de los datos operativos que se realizan diariamente. Este enfoque de gestión de tipo empresarial a la seguridad es la base lógica del sistema de gestión de seguridad (SGS). En términos simples, el SGS es la aplicación de prácticas de gestión empresarial para la gestión de la seguridad.



En los párrafos 3.2.2, 3.2.3, y 3.2.4 hemos mencionado la palabra accidente, incidente y en Capitulo 2 condiciones latentes, en el siguiente gráfico nos muestra una estadística mundial que detrás de un accidente hay de 30 a 100 incidentes serios, de 100 a 1000 incidentes y de 1000 a 4000 condiciones latentes que ocurrieron previamente al accidente.



3.3 CONCEPTOS DE GESTIÓN DE SEGURIDAD.

3.3.1 En los términos más simples, la gestión de la seguridad supone la detección de peligros y cerrar todas las brechas en las defensas del sistema. La gestión eficaz de la seguridad es multidisciplinaria: requiere la aplicación sistemática de diversas técnicas y actividades en todo el espectro de las operaciones de OSINERGMIN. Una gestión eficaz de la seguridad se funda en los tres conceptos básicos que siguen:

a) Un **enfoque de OSINERGMIN** para la seguridad. Esto da el tono para la gestión de la seguridad. El enfoque de OSINERGMIN se debe fundar en su cultura de seguridad y este debe también comprender las políticas, los objetivos y metas establecidas y, lo que es más importante, el compromiso de la Alta Dirección respecto a la seguridad.

b) **Instrumentos de organización** eficaces para mantener niveles de seguridad. Se necesitan instrumentos de organización eficaces para llevar a cabo las actividades y procesos necesarios para fomentar la seguridad. Esto incluye la forma en que OSINERGMIN se organiza para llevar a la práctica sus políticas, objetivos y metas de seguridad y asigna recursos, etc. Los principales puntos de atención son los peligros y sus posibles efectos en las actividades críticas para la seguridad.

c) Un sistema formal de **vigilancia de la seguridad operacional**. Esto es necesario para confirmar el continuo cumplimiento por las organizaciones de las políticas, objetivos, metas y normas de seguridad establecidas por OSINERGMIN. La expresión vigilancia de la seguridad se refiere específicamente a las actividades de OSINERGMIN como parte de su programa de seguridad en las empresas que supervisa. Para un explotador o un proveedor de servicios, se emplea la expresión supervisión de la eficacia de la seguridad operacional para abarcar estas actividades en el marco de su sistema de gestión de seguridad (SGS).

En el apéndice de este capítulo se especifican estos conceptos

3.4 ESTRATEGIAS DE GESTIÓN DE SEGURIDAD.

3.4.1 La estrategia que OSINERGMIN adopte para su SGS reflejará su cultura de seguridad y puede situarse en una gama que va desde la pura reacción, respondiendo únicamente a los accidentes, hasta estrategias que son muy activas en su búsqueda para detectar problemas de seguridad. En el proceso tradicional, o de reacción, predominan las reparaciones retrospectivas (es decir, cerrar la puerta después que se escapó el gato). Con un enfoque más moderno o preventivo, la reforma futura tiene el papel más importante (es decir, hacer que la puerta no pueda quedar abierta o que el gato no quiera escaparse). Dependiendo de la estrategia adoptada, deben emplearse diferentes métodos y herramientas.

Estrategia de seguridad por reacción: investigar accidentes y notificar incidentes

3.4.2 Esta estrategia es útil para las situaciones en que se trata de fallas de la tecnología o de sucesos poco comunes. La utilidad del enfoque de reacción para la gestión de la seguridad depende de la medida en que la investigación va más allá de las causas determinantes, para incluir un examen de todos los factores que intervinieron. El enfoque de reacción tiende a presentar las características que siguen:

a) La atención respecto a la seguridad se concentra en el cumplimiento de los requisitos mínimos.

b) La medición de la seguridad se basa en los accidentes e incidentes que deben notificarse, con valores limitados tales como:

1) Todo análisis se limita a examinar las fallas ocurridas.

2) Los datos disponibles son insuficientes para determinar con precisión las tendencias, especialmente las atribuibles al error humano.

3) Se tiene poco conocimiento de las *"causas profundas"* y las condiciones inseguras latentes, que facilitan el error humano.

c) Es necesaria una "actualización" constante para igualar la inventiva humana respecto a nuevos tipos de errores.

Estrategia de seguridad preventiva: buscar activamente información proveniente de diversas fuentes que puede indicar la gestación de problemas de seguridad.

3.4.3 Si OSINERGMIN sigue una estrategia preventiva para la gestión de la seguridad debe estimar que el riesgo de accidentes pueda reducirse al mínimo, detectando los puntos vulnerables antes de que fallen y adoptando las medidas necesarias para reducir esos riesgos. Por lo tanto, buscan activamente las condiciones sistémicas inseguras empleando instrumentos tales como:

a) Sistemas de notificación de peligros e incidentes que promueven la identificación de condiciones inseguras latentes.

b) Encuestas de seguridad para obtener información del personal de operaciones respecto a áreas de insatisfacción o condiciones insatisfactorias que pueden encerrar posibilidades de accidentes.

c) Inspecciones o auditorías de todos los aspectos de las operaciones para identificar puntos vulnerables antes que accidentes, incidentes o sucesos de menor importancia confirmen que existe un problema respecto a la seguridad.

Estrategia de seguridad predictiva: documenta el desempeño espontáneo del personal y lo que realmente ocurre en las operaciones diarias

3.4.4 El método predictivo tiene:

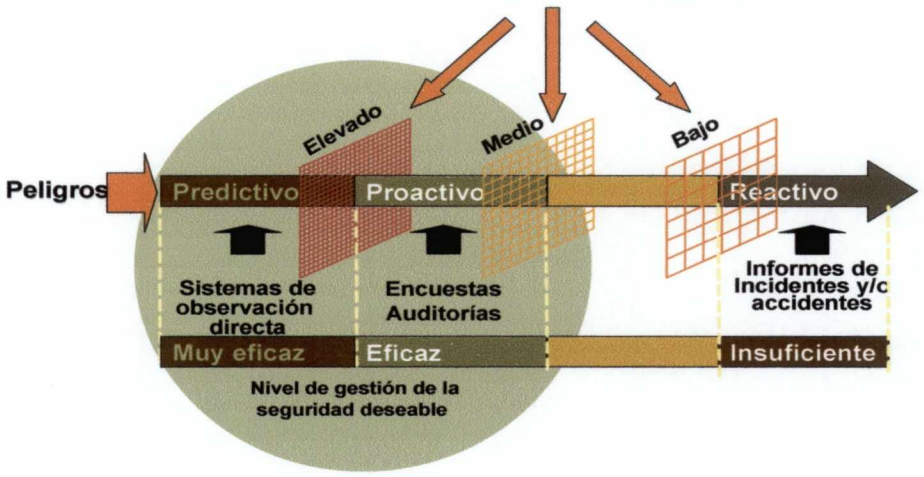
a) Sistemas de reporte confidenciales, análisis de los datos de y vigilancia de operaciones normales.

b) Se basa en la noción que la gestión de la seguridad se optimiza saliendo a buscar los problemas y no esperando que se produzcan.

c) Una búsqueda agresiva de la información de diferentes fuentes que puede revelar riesgos emergentes a la seguridad.

Método reactivo	Método proactivo	Método predictivo
El método reactivo responde a los acontecimientos que ya ocurrieron tales como incidentes y los accidentes	*El método proactivo busca activamente identificar riesgos potenciales a través del análisis de las actividades diarias de la organización*	*El método predictivo documenta el desempeño espontáneo del personal y lo que realmente ocurre en las operaciones diarias*

Nivel de las fuentes de identificación seguridad



Fuente: OACI

3.5 ACTIVIDADES CLAVES PARA LA GESTIÓN DE SEGURIDAD

3.5.1 Las actividades claves para la gestión de seguridad son:

a) **Organización.** Organizarse para establecer una cultura de seguridad y reducir sus pérdidas por actos no deseados. Estas organizaciones normalmente tendrán un SGS formal.

b) **Evaluaciones de la seguridad**. Analizar sistemáticamente los cambios propuestos para el equipo o los procedimientos a fin de detectar y mitigar los puntos débiles antes de implantar cambios.

c) **Notificación de sucesos.** Establecer procedimientos formales para notificar los sucesos relacionados con la seguridad y otras condiciones inseguras.

d) **Mecanismos de detección de peligros.** Emplear mecanismos de reacción, proactivos y preventivos para detectar los peligros relacionados con la seguridad en toda la organización, tales como notificación voluntaria de incidentes, encuestas y evaluaciones de seguridad.

e) **Investigación y análisis.** Hacer el seguimiento de los sucesos notificados y de las condiciones inseguras y, si es necesario, iniciar las investigaciones y análisis competentes de la seguridad.

f) **Supervisión de la eficacia.** Procurar activamente el retorno de información necesario para cerrar el ciclo del proceso de gestión de la seguridad empleando técnicas tales como observación de tendencias y auditorías internas de la seguridad.

g) **Promoción de la seguridad operacional.** Difundir activamente los resultados de las investigaciones y los análisis de seguridad, compartiendo la experiencia adquirida en la materia tanto dentro de la organización como fuera de ella, si se justifica.

h) **Vigilancia de la seguridad operacional.** Tanto OSINERGMIN (que reglamenta) como la organización objeto de reglamentación tienen sistemas para supervisar y evaluar la eficacia de la seguridad.

3.6 RESPONSABILIDADES POR LA GESTIÓN DE SEGURIDAD

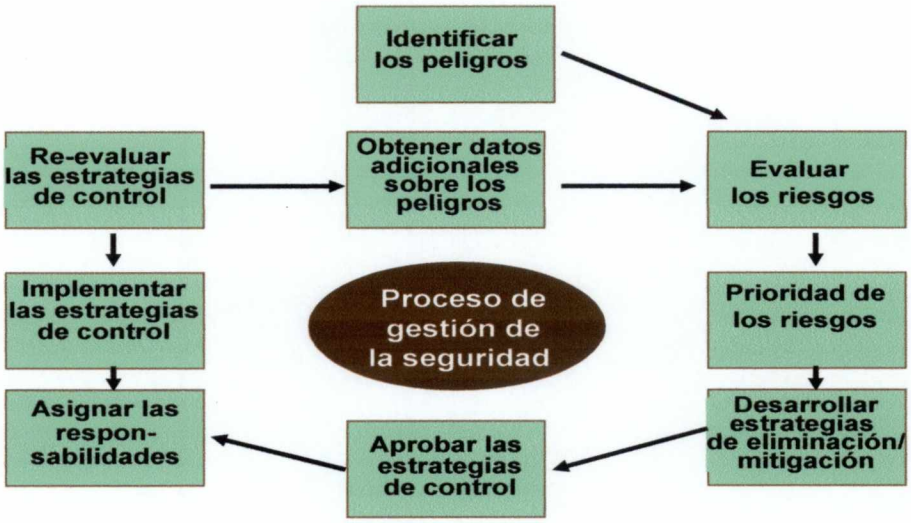
Estas responsabilidades están distribuidas en cuatro áreas básicas:

a) Definición de las políticas y procedimientos relacionados con la seguridad.
b) Asignación de los recursos para las actividades de gestión de la seguridad.
c) Incorporación de las mejores prácticas de la industria.
d) Desarrollo e implantación de la reglamentación necesaria que gobiernan la seguridad de las organizaciones objetos de la reglamentación.

3.7 PROCESO DE GESTIÓN DE SEGURIDAD

3.7.1 Conceptualmente el proceso de gestión de seguridad es un ciclo continuo.

3.7.2 La gestión de la seguridad se basa en pruebas, porque requiere el análisis de datos para detectar peligros. Empleando técnicas de evaluación de riesgos, se establecen prioridades para reducir las posibles consecuencias de los peligros. Una vez identificadas, se elaboran estrategias para reducir o eliminar los peligros y se aplican con responsabilidades claramente establecidas. La situación se reevalúa continuamente y se aplican medidas adicionales cuando es necesario.



a) **Recolección de datos.** El primer paso en el proceso de gestión de la seguridad es adquirir los datos de seguridad pertinentes — las pruebas necesarias para determinar la eficacia de la seguridad o detectar condiciones inseguras latentes (peligros para la seguridad). Los datos pueden obtenerse de cualquier parte del sistema: el equipo empleado, las personas que participan en la operación, los procedimientos de trabajo, las interacciones entre el elemento humano, el equipo y los procedimientos, etc.

b) **Análisis de datos.** Los peligros para la seguridad pueden detectarse analizando toda la información pertinente. Pueden determinarse las condiciones en que los peligros presentan riesgos reales, sus posibles consecuencias y la probabilidad de que ocurran; en otras palabras, ***¿qué puede ocurrir? ¿Cómo? ¿Cuándo?*** Este análisis puede ser cualitativo y también cuantitativo.

c) **Prioridad de las condiciones inseguras.** Un proceso de evaluación de riesgos determina la gravedad de los peligros. Aquellos que presentan los riesgos más grandes se consideran para medidas de seguridad. Esto puede exigir un análisis de costo-beneficio.

d) **Elaboración de estrategias.** Comenzando por los riesgos de mayor prioridad, pueden considerarse varias opciones de mitigación gestión de riesgos, cuyo desarrollo se hará en forma explicita en el Capitulo 5.

e) **Aprobación de estrategias.** Una vez analizados los riesgos y habiéndose decidido cuál es el plan de acción apropiado, se necesita la aprobación de la Dirección. En este paso el reto es la formulación de un argumento convincente (y quizá caro) para efectuar cambios.

f) **Asignación de responsabilidades y aplicación de estrategias.** Una vez adoptada la decisión de proceder, se deben estudiar los detalles de la aplicación. Esto incluye asignación de recursos y de responsabilidades, orden cronológico, revisiones de los procedimientos operacionales, etc

g) **Reevaluación de la situación.** La ejecución raramente tiene tanto éxito como se prevé inicialmente. Es necesario el retorno de información para cerrar el ciclo. ¿Qué nuevos problemas se han creado? ¿Responde la nueva estrategia de reducción de riesgos a las expectativas de eficacia? ¿Qué modificaciones al sistema o al proceso podrían ser necesarias?

h) **Recolección de datos adicionales.** Dependiendo de la etapa de reevaluación, podría ser necesario obtener nueva información y repetir el ciclo para perfeccionar la medida de seguridad.

3.7.3 La gestión de la seguridad exige capacidad analítica que quizá la Dirección no ponga habitualmente en práctica en aspectos de seguridad. Cuanto más complejo el análisis, más importante es la necesidad de aplicar los instrumentos analíticos más apropiados. El proceso de cerrar el ciclo de gestión de la seguridad también requiere el retorno de información para que la Dirección pueda comprobar la validez de sus decisiones y evaluar la eficacia de su aplicación.

3.8 VIGILANCIA DE SEGURIDAD OPERACIONAL.

3.8.1 La expresión vigilancia de la seguridad operacional se refiere a las actividades de OSINERGMIN en el marco de su programa de seguridad operacional, mientras que la supervisión de la eficacia de la seguridad operacional se refiere a las actividades de un explotador o proveedor de servicios en el marco de su SGS.

3.8.2 La vigilancia de la seguridad operacional o las actividades de supervisión de la eficacia de la seguridad operacional son un componente esencial de la estrategia de gestión de la seguridad de OSINERGMIN. La vigilancia de la seguridad operacional ofrece los medios por los que OSINERGMIN puede verificar en qué grado las organizaciones que supervisa alcanza sus objetivos de seguridad operacional.

3.8.3 Algunos de los requisitos de un sistema de control de la eficacia de la seguridad operacional ya existen en OSINERGMIN Por ejemplo, la notificación obligatoria de accidentes e incidentes.

3.8.4 Identificar los puntos débiles en las defensas del sistema exige más que recoger datos retrospectivos y producir estadísticas resumidas. Las causas subyacentes de los sucesos notificados no siempre son evidentes inmediatamente; por lo tanto, la investigación de los informes de sucesos relacionados con la seguridad operacional, y de toda otra información relativa a peligros posibles, debería ir acompañada de la supervisión de la eficacia de la seguridad operacional.

3.8.5 La ejecución de un programa eficaz de vigilancia de la seguridad operacional exige que OSINERGMIN y las organizaciones que supervisa:

a) Determinen los indicadores pertinentes de la eficacia de la seguridad operacional

b) Establezcan un sistema de notificación de sucesos relacionados con la seguridad operacional.

c) Establezcan un sistema para la investigación de sucesos relacionados con la seguridad operacional.

d) Elaboren procedimientos para la integración de datos de seguridad operacional provenientes de todas las fuentes disponibles.

e) Elaboren procedimientos para el análisis de los datos y la producción de informes periódicos de eficacia de la seguridad operacional.

Apéndice 1 del Capítulo 3

TRES CONCEPTOS BÁSICOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

La gestión eficaz de la seguridad operacional comprende tres conceptos básicos.

Seguidamente se describen las características de cada uno:

a) Un enfoque de OSINERGMIN integral respecto a la seguridad operacional — Esto prevé, por ejemplo:

1) La responsabilidad respecto a la seguridad operacional en la organización se asigna al Gerente General como prueba del compromiso de OSINERGMIN respecto a la seguridad operacional desde los niveles más altos de la organización.

2) Principios de seguridad operacional claramente enunciados, con políticas de apoyo de la organización.

3) Objetivos de seguridad operacional de OSINERGMIN, con un plan de gestión para alcanzar estos objetivos.

4) Funciones y responsabilidades bien definidas, con líneas de rendición de cuentas específicas respecto a la seguridad operacional que se publican y están disponibles para todo el personal relacionado con la seguridad operacional.

5) Establecer un área encargada de la seguridad operacional.

6) Pruebas demostrables de una cultura de seguridad operacional positiva en toda la organización.

7) Dedicación a un proceso de vigilancia de la seguridad operacional que es independiente del personal de operaciones.

8) Sistema de documentación con políticas, prácticas, principios y procedimientos de OSINERGMIN que repercuten en la seguridad operacional.

9) Examen periódico de los planes de mejoramiento de la seguridad operacional.

10) Procesos formales de revisión de la seguridad operacional.

b) Instrumentos de organización eficaces para aplicar las normas de seguridad operacional Por ejemplo, esto incluye lo siguiente:

1) Asignación de recursos basada en los riesgos.

2) Selección, contratación, instrucción y perfeccionamiento eficaces del personal

3) Definición, por OSINERGMIN, de las competencias específicas (y de los requisitos de instrucción en seguridad operacional) para todo el personal con funciones relacionadas con la eficacia de la seguridad operacional.

4) Normas definidas para la contratación de servicios

5) Aplicación de métodos de identificación de peligros, evaluación de riesgos y gestión eficaz de los recursos para controlar los riesgos identificados.

6) Disposiciones que permiten al personal comunicar preocupaciones importantes respecto a la seguridad operacional al nivel de dirección apropiado, para resolverlas y retorno de información sobre las medidas tomadas.

7) Planificación de respuesta para casos de emergencia y simulacros para comprobar la eficacia del plan.

c) **Un sistema formal para la vigilancia de la seguridad operacional** — Esto incluye elementos como:

1) Un sistema para capturar informes sobre sucesos relacionados con la seguridad operacional o condiciones inseguras.

2) Un sistema de auditoría de la seguridad operacional planificada e integral que tiene la flexibilidad necesaria para concentrarse en problemas de seguridad operacional específicos a medida que se plantean.

3) Un sistema para realizar investigaciones de seguridad operacional internas, aplicar medidas correctivas y difundir información sobre seguridad operacional para todo el personal afectado.

4) Sistemas para usar eficazmente los datos sobre seguridad operacional para el análisis de la eficacia y la supervisión de los cambios en la organización como parte del proceso de gestión de riesgos.

5) Examen sistemático y asimilación de las mejores prácticas de seguridad operacional.

6) Examen periódico de la eficacia continúa del SGS por un órgano independiente.

7) Control por los supervisores del trabajo en curso en todas las actividades críticas para la seguridad operacional, para confirmar el cumplimiento de todos los requisitos reglamentarios y normas y procedimientos de OSINERGMIN.

8) Sistema integral para documentar todos los reglamentos de seguridad operacional de OSINERGMIN, políticas de la organización, objetivos de seguridad operacional, normas, informes de seguridad operacional, etc., que sean aplicables y para que dicha documentación esté disponible para todo el personal afectado.

9) Disposiciones para la promoción permanente de la seguridad operacional basada en la eficacia de la seguridad operacional interna.

CAPÍTULO 4

PELIGROS

4.1 OBJETIVO Y CONTENIDO.

El capítulo presenta los fundamentos de identificación y análisis del peligro. El capítulo incluye lo siguiente:

- Peligros y consecuencias ·
- Primero fundamento: Entendiendo los peligros ·
- Segundo fundamento: Identificación del peligro ·
- Tercer fundamento: Análisis del peligro
- Cuarto fundamental - Documentación de los peligros

4.2 PELIGROS Y SUS CONSECUENCIAS

4.2.1 La identificación de peligros y la gestión de riesgos de seguridad son los principales procesos en la gestión de seguridad. Ellos no son del todo nuevos, como tampoco ellos han sido desarrollados como una consecuencia reciente de interés a la gestión de seguridad y, en particular, al Sistema de Gestión de Seguridad (SGS). La identificación de peligros y la gestión de riesgos de seguridad son los componentes dogmáticos que son la base del concepto del sistema de seguridad. Todo este concepto fue desarrollado hace cuarenta años, cuando se diseñaban proyectos de ingeniería. La diferencia entre el sistema tradicional de gestión de seguridad y el actual es que, debido a sus raíces de la ingeniería, la seguridad del sistema se enfocaba sobre todo en las implicaciones de seguridad de aspectos técnicos y los componentes del sistema y algo de implicancia del componente humano. La gestión de seguridad, se sigue construyendo sobre el dogma de seguridad del sistema (la identificación del peligro y la gestión de riesgos de seguridad), y amplía la perspectiva para incluir Factores Humanos y el desempeño humano como consideraciones claves de seguridad durante el diseño y la operación del sistema.

4.2.2 La diferenciación entre peligros y riesgos de seguridad es a menudo una fuente de dificultad y confusión. Para desarrollar las prácticas de gestiones de seguridad que son relevantes y eficaces, es esencial el tener muy en claro que es un peligro y que es un riesgo de seguridad. Este capítulo habla de peligros exclusivamente, mientras el Capítulo 5 habla de riesgos de seguridad. En el proceso de desarrollo del concepto de peligro, y asistir en el entendimiento de la diferencia entre peligros y riesgos de seguridad, **el proceso de análisis divide el concepto total de peligro en dos componentes: el peligro en sí mismo, y sus consecuencias.** El entendimiento claro de la diferencia entre estos dos componentes es también esencial para la práctica de gestión de seguridad.

4.2.3 ***Un peligro es definido como una condición, objeto o actividad que potencialmente puede causar lesiones al personal, daños al ambiente, equipamiento o estructuras, pérdida de personal, o reducción de la habilidad de desempeñar una función determinada.*** En sistemas en los cuales las personas deben actuar activamente, estrechamente y recíprocamente con la tecnología para alcanzar objetivos de producción por la entrega de servicios son conocidos como sistemas socio-técnicos. La gran mayoría de las organizaciones industriales son socio-técnicas. Los peligros son componentes normales o elementos de sistemas socio-técnicos. Ellos son integrales a los contextos donde la entrega de servicios por sistemas de producción socio-técnicos ocurre. Y por ellos mismos, los peligros no son " malas cosas". Los peligros no necesariamente son perjudiciales o negativos a

un sistema. Es sólo cuando el peligro interfasa con las operaciones del sistema orientado a la entrega del servicio donde su daño potencial se convierte en una preocupación de seguridad.

4.2.4 Consideremos, por ejemplo la lluvia, un componente normal del entorno natural. La lluvia es un peligro: *condición, objeto o actividad que potencialmente puede causar lesiones al personal, daños al ambiente, equipamiento o estructuras, pérdida de personal, o reducción de la habilidad de desempeñar una función determinada.* Una lluvia de 3mm (En una hora tres (3) litros) en Lima por 15 minutos, por si sola, no necesariamente encierra un peligro potencial a las actividades normales de los habitantes de la ciudad. Es más, riega las áreas verdes, moja las pistas y veredas para que no levanten polvo. Sin embargo, 3mm de lluvia de manera esporádica por varias horas, convirtió a varias avenidas de Lima en pequeños ríos, por donde los vehículos circulaban con dificultad. En los conos de la ciudad la situación fue peor, según los reportes de Indeci. Los techos precarios de cerca de 40 viviendas se desplomaron en Comas, San Juan de Miraflores y San Juan de Lurigancho. Reportó el diario el Comercio del sábado 9 de enero del 2010. Este ejemplo aclara lo expuesto en el párrafo anterior: los peligros no son " malas cosas" ó tienen una connotación negativa Los peligros son la parte incorporada a los contextos operacionales y sus consecuencias pueden mitigadas, por estrategias, que serán explicadas posteriormente en este Manual, que permitan contener el daño potencial de los peligros.

4.2.5 Una ***consecuencia es definida como el resultado potencial de un peligro.*** El daño potencial de un peligro materializado por una o muchas consecuencias. En el ejemplo de la lluvia tenida en Lima, sí el caudal de 3mm hubiese sido constante por más de doce (12) horas una consecuencia sería, mayor avenidas afectadas por la falta de sistema de drenaje en las vías. Una consecuencia aún más seria podría ser la inundación ó mayor cantidad de techos colapsados, porque las viviendas generalmente no tienen un techo con una ligera inclinación que permita drenar el agua acumulada. Es importante, por lo tanto, describir todas las consecuencias probables de un peligro durante el análisis de peligro, y no sólo los más obvios o inmediatos.

4.2.6 Las consecuencias de los peligros trae dos puntos importantes para tener en cuenta. Primero, los peligros pertenecen al presente. Ellos son, en la mayoría de los casos, parte del contexto operacional y por lo tanto ellos están presentes. Como los componentes físicos del contexto operacional la mayor parte de los peligros son, y deberían ser, detectados por auditorias, inspecciones, etc. Las consecuencias, por otro lado, pertenecen en el futuro. Ellos no se materializan hasta que los peligros interactúen con ciertas operaciones del sistema. Esto es, como una consecuencia de esta interacción es como los peligros pueden liberar su daño potencial. Esto genera un principio esencial de gestión de seguridad: las estrategias de mitigación deberían orientarse activamente a contener el daño potencial de los peligros y no estar a la espera hasta que las consecuencias de los peligros ocurran y luego reactivamente orientar tales consecuencias. Siguiendo el ejemplo anterior: cambio climático, un niño moderado. Lluvias frecuentes con mayor intensidad. Diagnóstico que se conoce con anterioridad **Presente.** Las **consecuencias** ya conocidas. La Municipalidad de Lima elabora un plan de lluvias que incluye un diseño urbano con zonas de drenaje en las vías y la colocación de diques y canaletas en los cerros para adaptar la ciudad a los cambios climáticos. Comercio 09/012010. **Reactivo**

4.2.7 Segundo, para el objetivo de gestión de seguridad, las consecuencias de los peligros deberían ser descritas en términos operacionales. Muchos peligros son definidos considerando solo el extremo de su daño potencial: pérdida de la vida humana. Muchos otros, son definidos como pérdida de la propiedad, daño ecológico y otras consecuencias similares de alto nivel, dificultando de esta manera el diseño de estrategias mitigación, excepto la cancelación de la operación. Para diseñar estrategias de mitigación orientadas a aspectos de seguridad las consecuencias deben ser redactadas en términos operacionales que en condiciones extremas

4.3 PRIMER FUNDAMENTO: ENTENDIMIENTO DE LOS PELIGROS.

4.3.1 Como ya hemos expuesto, existe una tendencia de confundir peligros con sus consecuencias. Cuando esta confusión ocurre, la descripción del peligro en términos operacionales refleja más bien las consecuencias que el peligro por sí mismo. En otras palabras, no es raro ver que los peligros son descritos como sus consecuencias

4.3.2 El identificar un peligro como una de sus consecuencias no sólo disfraza su verdadera naturaleza y el daño potencial del peligro en cuestión, sino también interfiere con la identificación de otras consecuencias importantes del peligro.

4.3.3 Sin embargo, los peligros bien identificados permiten la identificación de la naturaleza y el daño potencial del peligro, también permite deducir correctamente las fuentes o los mecanismos que lo generan y, el más importante, la magnitud de sus consecuencias.

4.3.4 Los peligros pueden ser agrupados en tres (3) grandes bloques: Peligros del entorno, peligros de los procesos y peligros de la información para la toma de decisiones.

4.3.5 **Peligros del entorno:** Los peligros del entorno surgen cuando hay fuerzas externas que podrían afectar la viabilidad del modelo de la organización, incluyendo los fundamentos que conducen los objetivos totales y las estrategias que definen aquel modelo.

4.3.6 **Peligros de los procesos:** son los que indican que los procesos de negocio:

- No estén claramente definidos,
- No estén completamente alineados con las estrategias de la organización,
- No se desarrollen efectiva y eficientemente para satisfacer las necesidades del cliente y/o grupos de interés
- No agreguen valor a los grupos de interés , o
- Expongan a los activos financieros, físicos e intelectuales a niveles inaceptables de pérdidas, a riesgos, o a malversaciones o mal uso.

4.3.7 **Los peligros de Información para la Toma de Decisiones**: son los peligros que indican que la información utilizada para soportar decisiones estratégicas, operacionales y financieras no sea relevante ni confiable.

4.4 SEGUNDO FUNDAMENTO: IDENTIFICACIÓN DE LOS PELIGROS.

De los procesos internos de OSINERGMIN

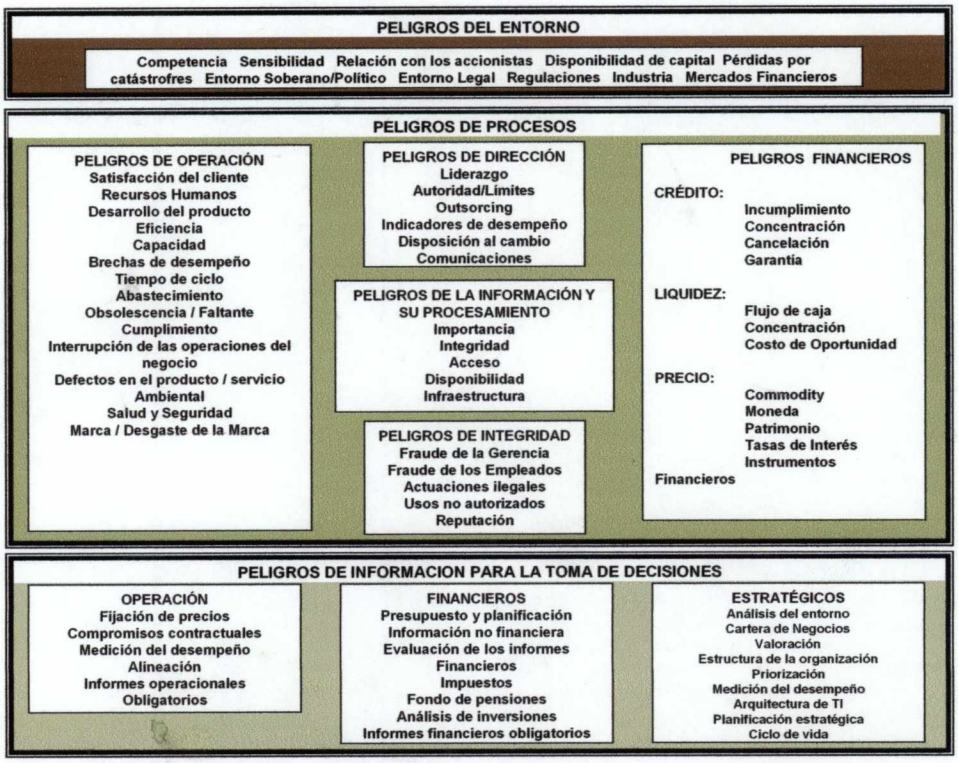
4.4.1 En el capitulo I se comentó que OSINERGMIN para el cumplimiento del marco normativo desarrolla una estructura organizacional con procesos estratégicos (creadores de valor), procesos operacionales y de apoyo como (generadores de valor)

4.4.2 Se comentó también que en los procesos estratégicos OSINERGMIN tendría incertidumbres (peligros) generadas por variables del entorno que están fuera de su control, que sería conveniente convertirlas a riesgos para poder medirlas y así establecer las estrategias de mitigación respectivas.

4.4.3 Asimismo, los procesos estratégicos tendrían otros peligros que no son generadas por variables del entorno, si no por, peligros de información para la toma de decisiones tales como, análisis del entorno, medición del desempeño, arquitectura de las tecnologías de información, planificación estratégica etc.

4.4.4 Del mismo modo en los procesos operacionales, habría incertidumbres (peligros) en los procesos operacionales.

4.4.5 El modelo de peligros internacional es el modelo que mejor se adapta a la organización, modelo diseñado por James W. De Loach 1988. De Loach co- autor del libro Managing *Business Risk: Integrated Approach,* publicado por *The Economist Intelligence Unit en 1995. Su ultimo libro, Enterprise- Wide Risk Management: Strategies for linking risk and opportunity*, fue publicado por *Financial Times* en Junio del 2000 y fue el primer libro escrito sobre gestión de riegos para las empresas. Asimismo perteneció al COSO Advisory Board brindando asesoramiento en el desarrollo de la nueva herramienta de gestión de riesgos recientemente implantada por **COSO**. **(Nota 1)**



Fuente: James W. Deloach, 1988

Nota 1: Debido al mundo económico integrado que existe hoy en día se ha creado la necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales, surge así un **nuevo concepto de control interno** donde se brinda una estructura común el cual es documentado en el denominado **informe COSO (Nota: 2)**

Nota: 2 El COSO posee cinco (5) componentes que son 1) Ambiente de Control. 2) Evaluación de Riesgo 3) Control Gerencial. 4) Componente de información y comunicación. 5) Supervisión. Los cinco componentes contenidos en la Resolución de Contraloría General Nº 320-2006-CG y la Resolución de Contraloría General Nº 458-2008-CG.

4.4.6 Este modelo universal se adapta a la organización, es decir se saca o se incluye variables de peligro, así como dijimos, en OSINERGMIN, en las variables del entorno, tendrían como peligro adicional la injerencia política entre otras.

En relación al programa de seguridad operacional

4.4.7 El espectro de peligros de los explotadores ó proveedores de servicio que OSINERGMIN supervisa es muy amplio y pude estar relacionado con las siguientes áreas.

a) **Factores de diseño**, incluyendo el diseño de equipamiento y de las tareas.

b) **Procedimientos y prácticas operacionales**, incluyendo su documentación y listas de verificación.

c) **Comunicaciones,** incluyendo medios, terminología.

d) **Factores organizacionales,** tales como las políticas de la compañía para la selección, entrenamiento, remuneración y la asignación de recursos.

e) **Factores ambientales de trabajo,** tales como el ruido ambiente y las vibraciones, temperatura, iluminación y la disponibilidad de ropa y equipo de protección.

f) **Factores reglamentarios,** incluyendo la aplicabilidad y cumplimiento de los reglamentos, la certificación del equipamiento, personal y procedimientos, y una supervisión adecuada.

g) **Defensas** incluyendo factores tales como la provisión de sistemas de detección y alarmas, y hasta dónde el equipamiento resistente y a prueba de errores y fallas.

h) **Performance humana**, incluyendo condiciones de salud y limitaciones físicas.

4.4.8 Como hemos mencionado en el Capítulo 3, los peligros pueden ser identificados después de acontecimientos reales de actos no deseados (accidentes o incidentes), o ellos pueden ser identificados por procesos proactivos y predictivos direccionado a la identificación de peligros antes de que ellos precipiten acontecimientos no deseados ó de seguridad. Hay una variedad de las fuentes de identificación de peligros. Algunas fuentes son internas a la organización mientras otras fuentes son externas a la organización.

4.4.9 Ejemplo de fuentes internas de identificación de peligros:

- Auditorias Internas de Calidad y/o Seguridad.
- Sistema voluntario de reportes de la organización
- Supervisión de los procesos
- Análisis de tendencias
- Retroalimentación de los cursos de entrenamiento
- Investigación y seguimiento de los reportes de los supervisores de los incidentes

4.4.10 Ejemplo de fuentes externas de identificación de peligros:

- Reportes de accidentes
- Sistema de reporte de incidentes de OSINERGMIN
- Auditorias de terceros
- Sistema de intercambio de información

4.4.11 El punto fundamental que hay que tener en claro, es que ninguna fuente o programa sustituye a otros completamente, ni esto hace que otras fuentes o programas sean redundantes o innecesarias. La identificación de peligros conducida en prácticas maduras de gestión de seguridad recurre a una combinación juiciosa de fuentes internas y externas, procesos reactivos, proactivos y predictivos.

4.4.12 Todo el personal dentro de OSINERGMIN debería recibir el entrenamiento apropiado de gestión de seguridad, en un nivel conmensurado a sus responsabilidades, de modo que cada uno en la organización esté preparado y sea capaz de identificar y reportar peligros. Desde esta perspectiva, la identificación y el reporte de los son la responsabilidad de todos. Sin embargo, la organización debe designar el área o la persona con la responsabilidad de identificar y analizar los peligros.

4.4.13 Como los peligros son identificados dependerá de los recursos y restricciones en cada organización en particular. Algunas organizaciones desplegarán programas de identificación de peligros comprensivos, intensivos en tecnología. Otras organizaciones desplegarán la identificación de peligros con un programa modesto adaptado a su tamaño y la complejidad de las operaciones. Sin embargo, la identificación de peligros, independientemente de la puesta en práctica, la complejidad y el tamaño, debe ser un proceso formal, claramente descrito en la documentación de seguridad de organización.

4.4.14 En prácticas de gestión maduras de seguridad, la identificación de peligros es una actividad continua que nunca para o descansa. Esto es una parte integral incorporada a los procesos de la organización direccionado obviamente a la entrega de los servicios de la organización. Sin embargo, hay tres condiciones específicas en las cuales hay que tener especial atención. Estas tres condiciones deberían provocar un proceso de identificación de peligros más a fondo y de gran alcance, e incluir:

- Cuando la organización experimenta un aumento inexplicado de acontecimientos ó no conformidades ó actos no deseados.
- Cuando se realicen cambios operacionales importantes, cambios al personal clave u otro equipo principal o sistemas.
- Antes y durante los períodos de cambios significativos en la organización, incluyendo crecimiento rápido o contracción, fusiones corporativas, adquisiciones o reducción del tamaño.

4.5 TERCER FUNDAMENTO: ANALISIS DE LOS PELIGROS.

4.5.1 La identificación de peligros es una perdida de tiempo a no ser que la información de seguridad sea extraída de una colección de datos. El primero paso de desarrollar la información de seguridad es el análisis del peligro

4.5.2 El análisis de peligro es, en la esencia, un proceso de tres pasos:

- Primero paso: **Identifique el riesgo genérico** (formulación del peligro)

- Segundo paso: Desglose el peligro genérico en **peligros específicos** o componentes específicos del peligro genérico. Cada peligro específico probablemente tendrá un conjunto diferente y único de factores causales, haciendo así cada peligro específico diferente y único por naturaleza.

- Tercer paso: Una los peligros específicos con **potenciales consecuencias específicas,** por ejemplo; acontecimientos específicos o resultados.

4.5.3 Un ejemplo que nos pude ilustrar sobre la formulación del peligro genérico, peligros específicos y consecuencias. Emisión de gases tóxicos a la atmosfera por los países desarrollados. El siguiente proceso de tres (3) pasos podríamos aplicar:

- **Paso A:** Identifique el riesgo genérico.
  - Cambio Climático

- **Paso B:** Identifique los peligros específicos o componentes específicos del peligro genérico.

- Falta de lluvias en zona de la sierra
- Elevación de la temperatura del mar
- Lluvias en la zona del litoral

- **Paso C:** Una los peligros específicos con potenciales consecuencias específicas.
  - La falta de lluvias en la zona de la sierra podría afectar las reservas de agua para la ciudad de Lima.
  - La falta de lluvias en la zona de la sierra podría afectar la generación de energía por las hidroeléctricas y el abastecimiento de agua en la cuenca del sur.
  - La elevación de la temperatura del mar podría generar la migración de la anchoveta.
  - La elevación de la temperatura del mar podría generar el incremento de lluvias en el litoral
  - El incremento de las lluvias en el litoral.....

Nota: En el ejemplo académico del párrafo anterior, no están incluidos todos los componentes específicos del peligro así como todas sus consecuencias.

4.6 CUARTO FUNDAMENTO: DOCUMENTACIÓN DE LOS PELIGROS.

4.6.1 Los peligros típicamente se perpetúan en un sistema y entregan principalmente su daño potencial porque existe la ausencia o la ineficacia de identificación de peligros. La carencia de identificación de peligros es a menudo el resultado de:

- No pensar en las condiciones operacionales, con el potencial de desatar el daño potencial de peligros;
- No saber de las condiciones operacionales, con el potencial de desatar el daño potencial de peligros
- Desgana para considerar o investigar condiciones operacionales con el potencial de desatar el daño potencial de peligros.
- Desgana para invertir dinero para investigar condiciones operacionales con el potencial de desatar el daño potencial de peligros.

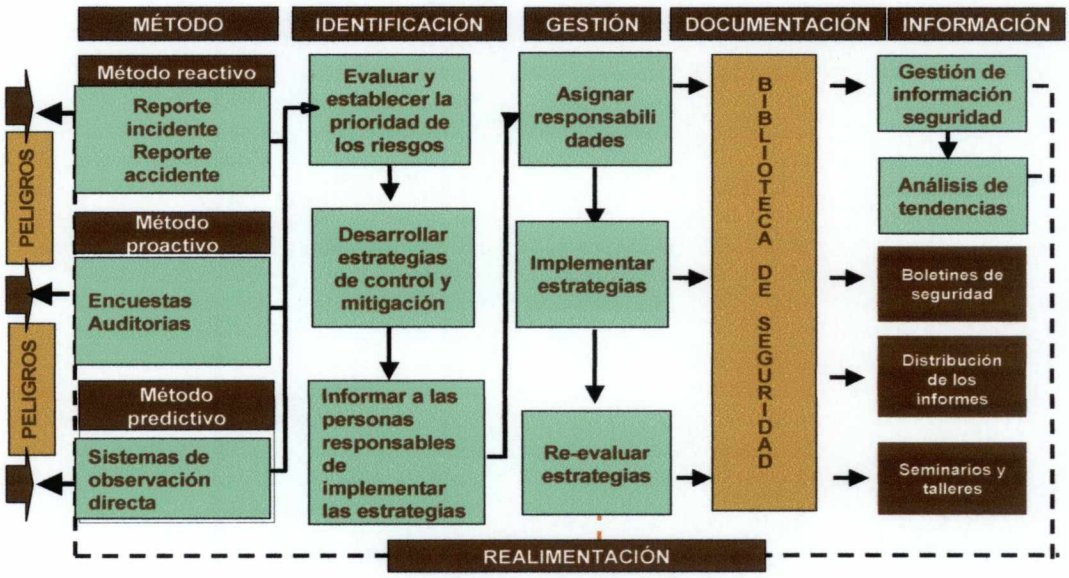
4.6.2 La inconciencia y la desgana sólo puede ser vencido por el conocimiento. La documentación formal de peligros es por lo tanto una exigencia esencial para la identificación de peligros así como un rasgo de gestión de seguridad en grado de madurez. La información de seguridad (por ejemplo, datos analizados en bruto) y la inteligencia de seguridad (por ejemplo, la información de seguridad que ha sido corroborada y más ha sido analizado añadiendo el contexto) se combinan para generar el conocimiento de seguridad que formalmente debe residir en la organización, no en la cabeza de algunos miembros de la organización. El archivo formal del conocimiento de seguridad es un salvaguarda contra la volatilidad de la información. Además, una organización que tiene el conocimiento histórico de seguridad hará decisiones de seguridad basadas sobre hechos y no sobre opiniones.

4.6.3 La gestión apropiada de documentación en cuanto a la identificación de peligros es importante como un procedimiento formal que permita traducir la información cruda operacional de seguridad en el conocimiento de peligros. Con la compilación continua y la gestión formal de este conocimiento relacionado con el peligro se logra " la biblioteca de seguridad " de una organización. Para desarrollar conocimiento sobre los peligros y así construir " la biblioteca de seguridad ", se debe recordar que el seguimiento y el análisis de peligros se facilitan estandarizando:

- La definición de los términos usados.
- El entendimiento de los términos usados.
- La información validada de seguridad recolectada.

- El reporte (por ejemplo, lo que la organización espera);
- La forma en que se va medir la información de seguridad recolectada.
- La gestión de información de seguridad recolectada

4.6.4 En la siguiente figura se ilustra el proceso de documentación de peligro. Los peligros constantemente son identificados por fuentes reactivas, proactivas y predictivas y los métodos subyacentes de colección de seguridad de la información. La colección, la identificación y la información del peligro son evaluadas en términos de consecuencias, y las prioridades y responsabilidades en cuanto a respuestas de estrategias de mitigación. Toda esta información, incluyendo peligros, consecuencias, prioridades, responsabilidades y estrategias, debe ser guardada en la biblioteca de seguridad de la organización. El producto de la biblioteca de seguridad no solamente es para preservar la memoria corporativa de seguridad, ya que esta se convierte en una fuente de conocimiento de seguridad para ser usado como referencia por la organización en la toma de decisiones en aspectos de seguridad. El conocimiento de seguridad incorporado a la biblioteca de seguridad permite proveer la retroalimentación y tener un control de referencia contra que se va a medir la gestión de análisis y consecuencias del peligro así como la eficacia de las fuentes ó métodos de recolección de información de seguridad. También esta, provee los insumos para un análisis de tendencias de seguridad así como fuente para propósitos educativos



Fuente: OACI

CAPÍTULO 5

GESTIÓN DE RIESGOS

5.1 OBJETIVO Y CONTENIDO.

5.1.1 Objetivo: Establecer los fundamentos para gestionar los riesgos.

5.1.2 El capitulo también contiene:

- Definición de riesgo de seguridad
- Primer fundamento: Gestión del riesgo de seguridad
- Segundo fundamento: Probabilidad del riesgo de seguridad
- Tercer fundamento: Severidad del riesgo de seguridad
- Cuarto fundamento: Tolerabilidad del riesgo de seguridad
- Quinto fundamento: Control/mitigación del riesgo de seguridad

5.2 DEFINICIÓN DE RIESGO DE SEGURIDAD.

5.2.1 El capítulo 2 de este Manual define la seguridad como el resultado de la gestión de un número de procesos de organización. La gestión de estos procesos de organización tiene el objetivo de mantener bajo control los riesgos de seguridad de la organización. El punto clave en esta perspectiva es tener bien en claro el concepto de seguridad como resultado, y la gestión de riesgos de seguridad como el proceso.

5.2.2 El capítulo 4 de este Manual en adición al comentario de que la identificación de peligros es una de las dos actividades principales que apoyan la gestión de seguridad. La identificación de peligros también contribuye a la robustecer los otros procesos de la organización indirectamente relacionados con la gestión de seguridad. En OSINERGMIN el proceso de identificación de peligros potenciales está directamente relacionado a las acciones preventivas en su sistema de gestión de calidad como también en los procesos de salud y seguridad ambiental. Para asegurar una identificación apropiada de los peligros así como su análisis correspondiente, el Capítulo 4 establece una diferenciación clara entre peligros, como las fuentes de daño potencial, y sus consecuencias de seguridad descritas en términos operacionales.

5.2.3 La gestión de riesgos de seguridad es otra actividad principal que apoya la gestión de seguridad y contribuye también indirectamente con otros procesos de la organización. El término de gestión de riesgos de seguridad, opuesto al término genérico de gestión de riesgos, tiene la intención de transmitir la noción de que la gestión de la seguridad no tiene directamente por objeto el riesgo de la gestión de recursos financieros ó el riesgo legal ó el riesgo económico y así sucesivamente, sino va más allá, a la gestión de la riesgos de seguridad. Va más allá, porque los riesgos son asociados y sistémicos

5.2.4 Una común fuente de peligro es que actividades de la gestión de seguridad frecuentemente no progresan más allá de la identificación de peligros y su respectivo análisis, o en otros casos se realiza un salto directo de la identificación de peligros al despliegue de las estrategias de mitigación, evitando de esta manera, la evaluación y la priorización de los riesgos de seguridad de las consecuencias de los peligros. Después de todo, una vez que las fuentes de peligro o daño son identificadas, y sus consecuencias analizadas y estamos de acuerdo, entonces las

estrategias de mitigación diseñadas para protegerse contra las consecuencias pueden ser desplegadas. Este punto de vista sería correcto si uno se adhiere al siguiente concepto "la seguridad como la primera prioridad", y nos concentramos en la prevención de malos resultados. Sin embargo, bajo el concepto de gestión de seguridad, el estar acuerdo sobre las consecuencias de peligros identificados y cuya descripción se haya realizado en términos operacionales no es suficiente para el despliegue de las estrategias de mitigación. Es necesario evaluar la seriedad de las consecuencias, como la definición de prioridades para la asignación de los recursos cuando proponemos las estrategias de mitigación.

5.2.5 Ya todos sabemos este axioma básico de gestión que uno no puede gerenciar lo que no puede medir. Por lo tanto, es esencial de algún modo medir la seriedad de las consecuencias de los peligros. Esto es la contribución esencial de la gestión de riesgos de seguridad al proceso de gestión de seguridad. "La puesta de un número " a las consecuencias de los peligros, provee al proceso de gestión de seguridad de la organización de los **principios base** para tomar decisiones sobre los riesgos de seguridad, para la subsecuente asignación de recursos por la organización a fin de contener el daño potencial de los peligros. De este modo, la gestión de riesgos de seguridad completa la trilogía de gestión básica de seguridad de riesgos **" peligros- consecuencias- riesgos de seguridad "** y asegura la priorización de recursos para su mitigación respectiva

5.2.6 El riesgo, en su sentido propio y más amplio, ha sido sujeto a mucha discusión y la literatura sobre el tópico es abundante. Potencial para la confusión existe, ya que en parte es debido al mal empleo del término y al significado generalmente vago que se tiene.
Más allá de esto, es esencial establecer una definición clara de riesgo de seguridad, y unir tal definición a los conceptos de peligro y consecuencia expresada en términos operacionales.

5.2.7 Incluso después de afinar la definición del término genérico de riesgo a términos mas específicos de seguridad, la confusión todavía seguía latente. Esto es porque la noción de riesgo es artificial. Riesgos de seguridad no son componentes tangibles o visibles de ningún ambiente físico o natural; es necesario pensar acerca de los riesgos de la seguridad para entender o formar una imagen de ellos. Los peligros y consecuencias, por otra parte, son los componentes tangibles o visibles de un ambiente físico o natural, y por lo tanto intuitivos en términos de entendimiento y visualización. La noción de riesgo de seguridad es como crear algo en nuestra mente por ideas en forma sistemática. En palabras simples, mientras los peligros y consecuencias son los componentes físicos del mundo natural, los riesgos de seguridad realmente no existen en el mundo natural. El riesgo de seguridad es un producto de generación de ideas de la mente humana que tiene la intención de medir la seriedad, " o poner un número ", a las consecuencias de los peligros.

5.2.8 El ***riesgo de seguridad es definido como la evaluación, expresado en términos de probabilidad y severidad predicha, de las consecuencia (s) de un peligro tomando como referencia la peor situación previsible.*** Típicamente, los riesgos de seguridad son designados a través de una convención alfanumérica que permite su medición. Usando el ejemplo de la lluvia en ciudad de Lima en el Capítulo 4.

- Una lluvia de 3mm (En una hora tres (3) litros) en Lima. **Es el peligro**

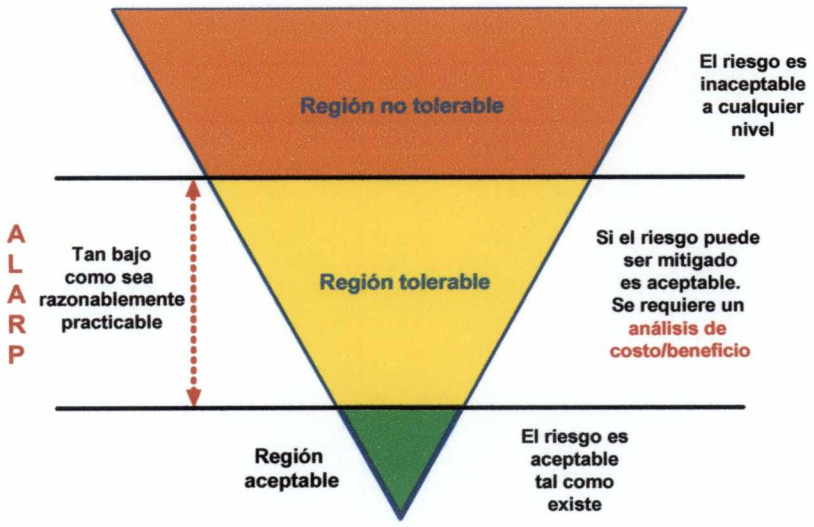
- 3mm de lluvia de manera esporádica por varias horas, convirtió a varias avenidas de Lima en pequeños ríos, por donde los vehículos circulaban con dificultad. En los conos de la ciudad la situación fue peor, según los reportes de Indeci. Los techos precarios de cerca de 40 viviendas se desplomaron en Comas, San Juan de Miraflores y San Juan de Lurigancho. **Son las consecuencias del peligro**

- La evaluación de las consecuencias expresadas en términos de probabilidad y severidad en términos de la convención alfa numérica. **Es el riesgo de seguridad.**

5.3 PRIMER FUNDAMENTO: GESTIÓN DE RIESGO DE SEGURIDAD.

5.3.1 La gestión de riesgos de seguridad es un término genérico que abarca la evaluación y la mitigación de los riesgos de seguridad de las consecuencias de los peligros que amenazan a las capacidades de una organización, a un nivel tan bajo como razonablemente sea practicable (**ALARP**). (**Anacronismo muy usado, que en inglés significa as low as reasonably practicable)** El objetivo de gestión de riesgos de seguridad es proporcionar las herramientas para una asignación de los recursos a todos los riesgos evaluados en forma equilibrada y también a aquellos riesgos de seguridad donde el control y la mitigación son viables. La gestión de riesgos de seguridad es un componente por lo tanto clave del proceso de gestión de seguridad. Su valor añadido, sin embargo, está en el hecho de que la solicitud de asignación de recursos se encuentra soportada por datos, claramente sustentable y de fácil explicación.

5.3.2 En el siguiente gráfico se muestra en forma genérica una representación visual, ampliamente adoptada al proceso de gestión de riesgos de seguridad. Durante la evaluación de los riesgos de seguridad generado por las consecuencias de los peligros, algunos riesgos se ubicaran inicialmente en la región no tolerable, otros en las regiones tolerable y aceptable respectivamente



5.3.3 Los riesgos de seguridad evaluados que se ubican inicialmente en la región intolerable son inaceptables en cualquier circunstancia. La probabilidad y/o la severidad de la consecuencia (s) del riesgo (s) son de tal magnitud, que el daño potencial del riesgo plantea tal amenaza a la viabilidad de la organización que requieren la acción de mitigación inmediata. Por lo general, dos (2) alternativas están disponibles a la organización para llevar el riesgo de seguridad a las regiones tolerables o aceptables: (1) asignar recursos para reducir la exposición y/o la magnitud de la consecuencia (s) del daño potencial del riesgo (s), ó (2) si la mitigación no es posible, cancelar la (s) operación (es).

5.3.4 Los riesgos de seguridad evaluados que se ubican inicialmente en la región tolerable son aceptables, a condición de que las estrategias de mitigación garanticen que, al grado previsible, la probabilidad y/o la severidad de la consecuencia (s) del o los riesgo (s) son mantenidas en el control de organización. Los mismos criterios de

control se aplican a los riesgos de seguridad que se ubicaron inicialmente en la región intolerable y que como resultado de las acciones de mitigación se ubican en la región tolerable. Un riesgo de seguridad evaluado inicialmente intolerable qué por resultado también de la mitigación y su reevaluación se ubica ahora en la región tolerable debe permanecer "protegido" con acciones de supervisión que garanticen su control. **En ambos casos, requieren un análisis de costo-beneficio**

5.3.5 La sigla ALARP es usada para describir que un riesgo de seguridad ha sido reducido a un nivel que *"es tan bajo como razonablemente practicable"*(**as low as reasonably practicable.)** En la determinación que es " razonablemente practicable " en el contexto de gestión de riesgos de seguridad, deberían entrar en consideración tanto la viabilidad técnica de reducir el riesgo de seguridad, como el costo. Esto debe incluir un análisis de costo-beneficio. La exposición que tiene un riesgo para la seguridad en un sistema, *es tan bajo como razonablemente practicable* (ALARP), significa que cualquier nueva reducción de riesgo es impracticable o sus costos de reducirlos son muy altos. Cabe, sin embargo, tener en cuenta que, cuando una organización "acepta" un riesgo de seguridad, esto no significa que el riesgo de seguridad es eliminado. Siempre hay un riesgo residual, sobretodo cuando el ser humano está presente, sin embargo, la organización ha aceptado que el riesgo residual de seguridad es lo suficientemente baja que se ve compensado por los beneficios.

5.3.6 Los riesgos de seguridad evaluados que se ubican inicialmente en la región aceptable son aceptables de por si y no requieren ninguna acción de mitigación para reducir, eliminar y la probabilidad y/o la severidad de la consecuencia (s) de riesgo (s)

5.3.7 Los análisis de beneficio del costo están en el corazón de gestión de riesgos de seguridad. Hay dos costos distintos para ser considerados en el análisis de costo beneficio: costos directos y costos indirectos.

5.3.8 Los costos directos son los costos obvios y son fáciles para determinar. Ellos sobre todo se relacionan con el daño físico ó material Los elevados costos de un accidente se pueden reducir con una cobertura de seguro. Se debe tener en cuenta, sin embargo, que la cobertura de seguro no hace nada para que la probabilidad y/o la severidad de la consecuencia (s) de riesgo (s) este bajo control de la organización, esto sólo transfiere el riesgo monetario de la organización al asegurador. Pero comprar un seguro no es todo. Simplemente la compra del seguro para transferir el riesgo monetario apenas puede ser considerado una estrategia de gestión de seguridad.

5.3.9 Los costos indirectos incluyen todos aquellos gastos que directamente no son cubiertos por el seguro. Los costos indirectos pueden ser más altos que los costos directos que son el resultado de la pérdida de control por la organización de ciertas consecuencias extremas de peligros. Tales costos no son a veces obvios y a menudo no son tomados en cuenta. Algunos ejemplos de los costos no asegurados:

- Pérdida de negocio y daño a la reputación de la organización.
- Pérdidas por utilización de equipos. Esto se compara con el ingreso perdido. El equipo de reemplazo debería ser comprado o arrendado. El tiempo de entrega, las innovaciones técnicas ameritan un reentrenamiento del personal.
- Pérdida de productividad de personal. Si el personal es perjudicado por un accidente y por ende no puede trabajar, la legislación todavía puede requerir que ellos sigan recibiendo alguna forma de compensación. También, este personal tendrá que ser substituida al menos para el corto plazo, incurriendo en los gastos de salarios y entrenamiento, horas extraordinarias, así como imponente una carga de trabajo aumentada sobre los trabajadores experimentados.

- Seguros. Deducibles. La obligación del asegurado de cubrir una parte del costo de cualquier acontecimiento debe ser pagada. Un sistema inseguro las primas son mayores. El tener un de gestión de seguridad podría ayudar a la organización a una renegociación

- Multas y citas. Las autoridades de gobierno pueden imponer multas y citas, incluyendo posiblemente el cerrar operaciones inseguras.

5.3.10 El análisis del costo beneficio brinda resultados que pueden ser numéricamente precisos y analíticamente exactos. Sin embargo, hay factores menos exactos y numéricos que intervienen el análisis. Estos factores podrían ser:

- **Gestión.** ¿El riesgo de seguridad es compatible con la política y los objetivos de seguridad de la organización?

- **Capacidad para afrontar los costos.** ¿Impide la naturaleza del riesgo una solución eficaz con relación a los costos?

- **Legal.** ¿Esta el riesgo de seguridad dentro de las normas establecidas y de la capacidad de hacerlas cumplir?

- **Cultural**. ¿Cómo el personal de la organización y los otros grupos de interés ven este riesgo?

- **Mercado**. ¿Se compromete la capacidad de competir y el buen funcionamiento de la empresa que OSINERGMIN supervisa con respecto a otros si no se reduce o elimina el riesgo?

- **Político**. ¿Habrá un precio político por la no gestionar el riesgo de seguridad?

- **Público.** ¿Cuanta influencia tendrán los medios de comunicación o los grupos de interés en la opinión del público respecto a este riesgo?

5.4 SEGUNDO FUNDAMENTO: PROBABILIDAD DEL RIESGO DE SEGURIDAD.

5.4.1 El proceso de traer los riesgos de seguridad donde la(s) consecuencia (s) de lo(s) peligros están bajo el control de la organización empieza evaluando la probabilidad que la consecuencia (s) del peligro se materialice durante operaciones. **Este concepto se conoce como la evaluación de la probabilidad de riesgo de seguridad.**

5.4.2 La probabilidad de riesgo de seguridad es definida ***como la probabilidad que un acontecimiento inseguro pueda ocurrir.*** Pueden ayudar a la definición de la probabilidad preguntas tales como:

a) ¿Hay antecedentes de sucesos similares, o este es un caso aislado?

b) ¿Qué otro equipo o componentes del mismo tipo pueden tener defectos similares?

c) ¿Cuántos miembros del personal de operaciones o de mantenimiento siguen, o deben seguir, los procedimientos en cuestión?

d) ¿Durante qué porcentaje de tiempo se usa el equipo o el procedimiento sospechoso?

e) ¿Existen implicaciones de organización, gestión o reglamentación que podrían reflejar amenazas más grandes para el público?

Basándose en estas consideraciones, se puede evaluar la probabilidad de que un suceso ocurra

5.4.3 Basado en las consideraciones que surgen de las respuestas a preguntas como aquellos catalogados en el párrafo 5.4.2, la probabilidad de la probabilidad que un acontecimiento inseguro pueda ocurrir, puede ser establecida, y su importancia evaluada usando una tabla de probabilidad de riesgo de seguridad

5.4.4 El siguiente cuadro presenta una tabla típica de ocurrencias de probabilidad de riesgo de seguridad, en este caso, es una tabla de cinco puntos. La tabla incluye una definición cualitativa de la probabilidad de ocurrencia de un acontecimiento inseguro, una explicación del significado de cada definición cualitativa, y una asignación numérica a cada definición. Debe quedar claro que esto solo es un ejemplo presentado para objetivos educativos. Aunque las consideraciones para la elaboración de esta tabla, así como la tabla de severidad, la evaluación de riesgo y las matrices de tolerabilidad que serán tratadas en los párrafos siguientes, conceptualmente hablando, se han tomado de los estándares actuales de la industria, el nivel de detalle y complejidad de las tablas y matrices deberán ser adaptadas y conmensuradas a las necesidades particulares y complejas de las organizaciones, si es necesario. Hay organizaciones que incluyen tanto definiciones cualitativas como cuantitativas. De la misma manera, algunas tablas se extienden hasta quince puntos.

Probabilidad del evento		
Definición cualitativa	**Significado**	**Valor**
Frecuente	Probable que ocurra muchas veces (ha ocurrido frecuentemente)	**5 (0.9-1.0)**
Ocasional	Probable que ocurra algunas veces (ha ocurrido infrecuentemente)	**4 (0.7-0.8)**
Remoto	Improbable, pero es posible que ocurra (ocurre raramente)	**3 (0.4-0.6)**
Improbable	Muy improbable que ocurra (no se conoce que haya ocurrido)	**2 (0.2-0.3)**
Extremadamente improbable	Casi inconcebible que el evento ocurra	**1 (0.0-0.1)**

5.4.5 En este cuadro hemos definido no solo las variables cualitativas sino las variables cuantitativas. Por ejemplo: la probabilidad la mediremos del 0 al 1. Si en el análisis calculamos la probabilidad en 0.75 corresponderá a que el acontecimiento inseguro podría ocurrir en forma ocasional. Esta asignación numérica no es un estándar.

5.5 TERCER FUNDAMENTO: SEVERIDAD DEL RIESGO DE SEGURIDAD.

5.5.1 Una vez determinada la probabilidad del acontecimiento, se debe evaluar la naturaleza de las consecuencias perjudiciales en caso de que el acontecimiento

ocurra realmente. Las consecuencias posibles rigen el grado de urgencia de la medida de seguridad requerida. Si hay un riesgo considerable de consecuencias muy graves, o si el riesgo de lesiones graves o de daños a los bienes o al medio ambiente es elevado, se justifican medidas de seguimiento urgentes. Al evaluar la gravedad de las consecuencias del suceso, podrían hacerse los siguientes tipos de preguntas:

a) ¿Cuántas **vidas peligran**? *(Empleados, personas que se encuentren en el lugar y el público en general).*

b) ¿Cuál es la extensión probable de los *daños a* **los bienes o financieros?** *(Pérdidas directas para el explotador, daños a la infraestructura, daños indirectos a terceros, repercusiones financieras y repercusiones económicas para el Estado).*

c) ¿Qué probabilidades hay de **repercusiones en el medio ambiente**? *(Derramamiento de combustible u otro producto peligroso y daño físico del hábitat natural).*

d) ¿Qué probabilidades hay de **repercusiones políticas** y de **interés de los medios de comunicación?**

5.5.2 Usando los mismos considerandos del segundo fundamento, la severidad también puede ser evaluada utilizando una tabla como la mostrada en el siguiente gráfico:

Severidad de los eventos		
Definiciones	**Significado**	**Valor**
Catastrófico	▪ Destrucción de equipamiento ▪ Muertes múltiples	**A (10)**
Peligroso	▪ Una reducción importante de los márgenes de seguridad, daño físico o una carga de trabajo tal que los operadores no pueden desempeñar sus tareas en forma precisa y completa. ▪ Lesiones serias o muertes de una cantidad de gente. ▪ Daños mayores al equipamiento.	**B (8-9)**
Mayor	▪ Una reducción significativa de los márgenes de seguridad, una reducción en la habilidad del operador en responder a condiciones operativas adversas como resultado del incremento de la carga de trabajo, o como resultado de condiciones que impiden su eficiencia. ▪ Incidente serio. ▪ Lesiones a las personas.	**C (5-7)**
Menor	▪ Interferencia. ▪ Limitaciones operativas. ▪ Utilización de procedimientos de emergencia. ▪ Incidentes menores.	**D (3-4)**
Insignificante	▪ Consecuencias leves	**E (0-2)**

5.6 CUARTO FUNDAMENTO: TOLERABILIDAD DEL RIESGO DE SEGURIDAD.

5.6.1 Una vez que el riesgo ha sido evaluado en términos de probabilidad y severidad, el siguiente paso es la evaluación del riesgo**, la tolerabilidad ó también conocido como impacto al riesgo = Probabilidad x Severidad**

5.6.2 La siguiente figura nos puede aclarar mejor como vamos a hacer la evaluación del riesgo

Probabilidad del riesgo	Severidad del riesgo				
	Catastrófico A	Peligroso B	Mayor C	Menor D	Insignificante E
5 – Frecuente	5A (1x10)	5B (1X9)	5C (1X7)	5D (1X4)	5E (1X2)
4 – Ocasional	4A (0.8X10)	4B (0.8X9)	4C (0.8x7)	4D (0.8x4)	4E (0.8x2)
3 – Remoto	3A (0.6x10)	3B (0.6X9)	3C (0.6X7)	3D (0.6X4)	3E (0.6x2)
2 – Improbable	2A (0.3x10)	2B (0.3X9)	2C (0.3X7)	2D (0.3X4)	2E (0.3X2)
1 – Extremadamente improbable	1A (0.1X10)	1B (0.1X9)	1C (0.1X7)	1D (0.1X4)	1E (0.1X2)

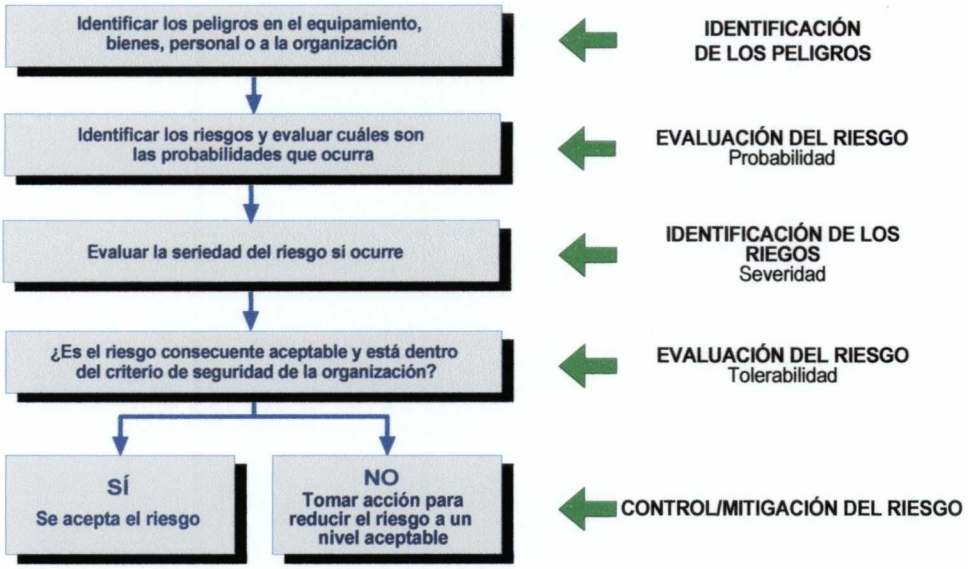
5.6.3 ¿Qué hemos realizado? Hemos aplicado **Probabilidad x Severidad,** es decir, hemos unido las dos (2) tablas anteriores. En esta nueva tabla de apreciación cualitativa y cuantitativa a la vez hemos agregado el concepto de los colores del semáforo de transito, rojo para el no tolerable, ámbar para el tolerable y verde para el aceptable. Asimismo vemos un color azul y es un color que esta pegado al rojo, que lo explicaremos en el siguiente párrafo. La representación por colores representa la tolerabilidad al riesgo.

5.6.4 Comentamos en el párrafo 5.3.4 que los riesgos de seguridad evaluados que se ubican inicialmente en la región tolerable son aceptables, a condición de que las estrategias de mitigación garanticen que, al grado previsible, la probabilidad y/o la severidad de la consecuencia (s) del o los riesgo (s) son mantenidas en el control de organización. Dependiendo de la naturaleza de la organización, los límites de los colores pueden variar, en las organizaciones donde la tolerabilidad ámbar es muy grande sería conveniente establecer que los riesgos que se encuentren bastante pegado al grado de tolerabilidad rojo deben tener bastante prioridad de ejecutar las acciones de mitigación respectivas y un control más estricto por la organización, de acuerdo a lo mostrado en el siguiente gráfico

Impacto al riesgo	Criterio sugerido
5A, 5B, 5C, 4A, 4B, (10 – 9 - 7- 8 - 7.2)	Inaceptable bajo las circunstancias existentes. Decisiones de la dirección de mitigar y controlar el riesgo o parar las operaciones.
5D, 4C, 3A, 3B, 3C, (4 – 5.6 – 6 – 5.4 – 4.2)	El control/mitigación del riesgo requiere una decisión urgente de la dirección
5E,4D, 3D, 2A, 2B,2C. (2-3.2-2.4-3-2.7-2.1)	Aceptable después de revisar la operación
4E, 3E, 2D,2E,1A,1B, 1C, 1D, 1E.	Aceptable

5.7 QUINTO FUNDAMENTO: CONTROL/ MITIGACIÓN DEL RIESGO DE SEGURIDAD.

5.7.1 A continuación se muestra el proceso de gestión de riesgos de seguridad en un formato gráfico:



Mitigación de riesgos.

5.7.1 **Mitigación.** Medidas que eliminan el peligro potencial o que reducen la probabilidad o severidad del riesgo.

5.7.2 Por lo que respecta a los riesgos, no existe una seguridad absoluta. Los riesgos tienen que ser mantenidos en el nivel "*mas bajo como razonablemente practicable*" (***ALARP***). Esto quiere decir que el riesgo debe equilibrarse con el tiempo, el costo y la dificultad de adoptar medidas para reducir o eliminar el riesgo.

5.7.3 Cuando se considera que la tolerabilidad al riesgo es no aceptable, es necesario introducir medidas de control, cuanto más elevado el riesgo, mayor será la urgencia. El nivel de riesgo puede disminuirse sea reduciendo la severidad de las posibles consecuencias, sea reduciendo la probabilidad de que ocurra, **sea reduciendo la exposición a ese riesgo.**

5.7.4 La solución óptima variará, dependiendo de las circunstancias y exigencias. Para formular medidas de seguridad apropiadas, es necesario comprender si las defensas existentes son adecuadas. Cabe hacer las preguntas siguientes:

Análisis de las defensas.

5.7.5 En todo sistema de seguridad operacional, las defensas para proteger a las personas, los bienes o al medio ambiente son un componente importante. Estas defensas pueden emplearse para:

a) Reducir la probabilidad de que ocurran sucesos indeseables.

b) Reducir la gravedad de las consecuencias relacionadas con los sucesos indeseables.

5.7.6 Las defensas pueden clasificarse en los dos tipos que siguen:

a) **Defensas físicas**. Estas defensas incluyen objetos que desalientan o impiden actos inapropiados, o que mitigan las consecuencias de los sucesos (por ejemplo: sistemas de alarmas en un panel de de una planta de generación eléctrica, sistema de protección de datos del sistema informático de OSINERGMIN, etc.).

b) **Defensas administrativas**. Estas defensas incluyen los procedimientos y prácticas que mitigan la probabilidad de un accidente (por ejemplo: reglamentos y/o normas técnicas dispuestas por el Estado del Perú para los explotadores ó proveedores de servicio en los subsectores que son del ámbito de OSINERGMIN, la supervisión y fiscalización que realiza OSINERGMIN, el sistema de gestión por indicadores, el sistema de salud de las personas y seguridad ambiental)

5.7.7 Antes de seleccionar las estrategias de mitigación de riesgos apropiadas es importante comprender por qué el sistema de defensas existente era inadecuado. Cabe hacer las preguntas siguientes:

a) ¿Había defensas para protegerse contra esos peligros?

b) ¿Funcionaron las defensas como estaba previsto?

c) ¿Eran prácticas las defensas para usarlas en condiciones de trabajo reales?

d) ¿Conocía el personal afectado los riesgos y las defensas existentes?

e) ¿Son necesarias medidas adicionales de mitigación de riesgos?

Estrategias de mitigación de riesgos

5.7.8 Hay una variedad de estrategias para la mitigación de riesgos, por ejemplo:

a) **Evitar la exposición.** Se evita la tarea, práctica, operación o actividad que entraña riesgos porque el riesgo excede los beneficios.

b) **Reducir las pérdidas**. Se inician actividades para reducir la frecuencia de los sucesos peligrosos o la magnitud de las consecuencias.

c) **Separar la exposición** (separación o duplicación). Se toman medidas para aislar los efectos del riesgo o crear redundancia para protegerse de los riesgos, es decir, reducir la severidad del riesgo (por ejemplo, protegiéndose de daños indirectos en el caso de una falla de material o previendo sistemas de reserva para reducir la probabilidad de una falla total del sistema).

Generación de ideas.

5.7.9 Generar las ideas necesarias a fin de crear las medidas apropiadas para mitigar el riesgo constituye un reto. Elaborar medidas para mitigar los riesgos frecuentemente exige creatividad, ingenio y, por sobre todo, una mente abierta para considerar todas las soluciones posibles. El pensamiento de quienes están cerca del problema (y que generalmente tienen más experiencia) a menudo está afectado por métodos habituales y tendencias naturales. Una participación amplia, que incluye representantes de los diversos interesados, tiende a ayudar a superar las posturas rígidas. Pensar más allá de los parámetros establecidos por la experiencia y los conocimientos personales es fundamental para resolver eficazmente los problemas en un mundo complejo. Habría que considerar cuidadosamente todas las ideas nuevas antes de rechazar cualquiera de ellas.

Evaluación de las opciones para mitigar riesgos

5.7.10 Cuando se evalúan las opciones para mitigar los riesgos, no todas ofrecen el mismo potencial. Es necesario evaluar la eficacia de cada opción antes de adoptar una decisión. Es importante considerar toda la gama de medidas de control posibles y también considerar la compensación entre las diversas medidas para encontrar una solución óptima. Cada opción propuesta para mitigar los riesgos debería ser examinada desde perspectivas como las que siguen:

a) **Eficacia.** ¿Reducirá o eliminará los riesgos identificados? ¿En qué medida mitigan los riesgos otras opciones? La eficacia puede considerarse como una continuidad:

1) **Nivel uno** (medidas de ingeniería). La medida de seguridad **elimina** el riesgo; por ejemplo, previendo interruptores de seguridad para impedir que una turbina de generación eléctrica entre en sobre velocidad).

2) **Nivel dos** (medidas de control). La medida de seguridad acepta el riesgo pero ajusta el sistema para **mitigar** el riesgo reduciéndolo a un nivel manejable; por ejemplo, imponiendo condiciones de utilización más restrictivas en el manejo del acceso de información externa para reducir la probabilidad de de ingreso de un virus al sistema informático de OSINERGMIN.

3) **Nivel tres** (medidas de personal). Las medidas adoptadas aceptan que el peligro no se puede eliminar (nivel uno) ni controlar (nivel dos), de modo que el personal debe aprender a **enfrentarlo**; por ejemplo, agregando una advertencia, una lista de verificación revisada e instrucción adicional.

b) **Costo-beneficio.** ¿Superan los costos los beneficios percibidos? El potencial de beneficios, ¿será proporcional a las repercusiones del cambio que se necesita?

c) **Práctica.** ¿Es **factible** y apropiado en términos de tecnología disponible, factibilidad financiera y administrativa, legislación y reglamentos, voluntad política, etc.?

d) **Reto.** ¿Puede la medida para mitigar el riesgo resistir el análisis crítico de todos los interesados (empleados, alta dirección, partes interesadas y organizaciones del Estado, etc.)?

e) **Aceptación** de cada interesado. ¿Cuánta aceptación (o resistencia) puede esperarse de las partes interesadas? (Las conversaciones con los interesados durante la fase de **evaluación de riesgos** pueden indicar cuál es la opción que prefieren para mitigar los riesgos).

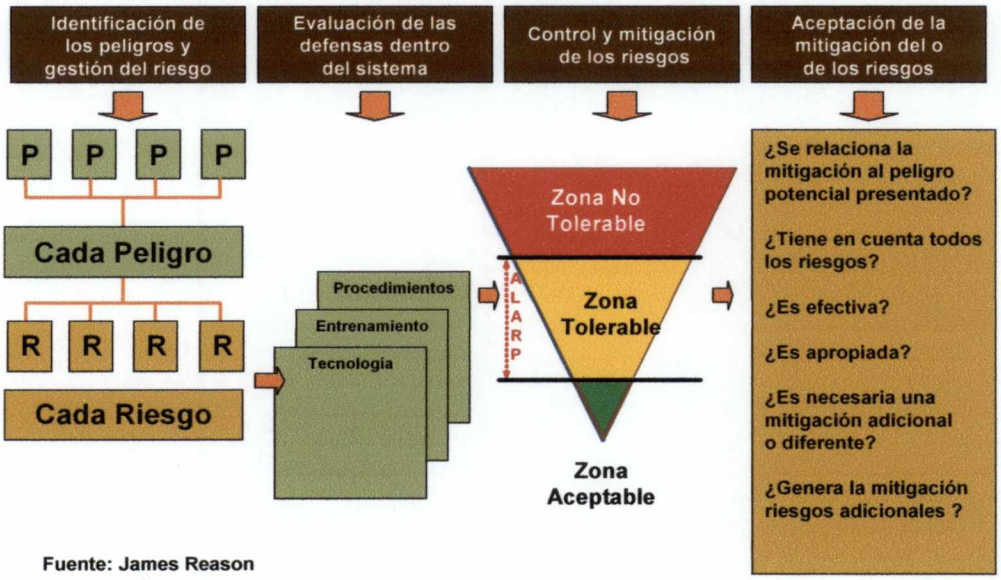
f) **Cumplimiento obligatorio.** Si se ponen en vigor nuevas reglas (leyes, reglamentos, normas, especificaciones técnicas, etc.), ¿se pueden hacer cumplir?

g) **Duración.** ¿Resistirá la medida la prueba del tiempo? ¿Será de beneficio temporario o será útil a largo plazo?

h) **Riesgos residuales.** Una vez puesta en vigor la medida para mitigar los riesgos, ¿cuáles serán los riesgos residuales con relación al peligro original? ¿Cuál es la capacidad para mitigar los riesgos residuales?

i) **Nuevos problemas.** ¿Qué nuevos problemas, o nuevos riesgos (quizá peores), introducirá el cambio propuesto?

5. 7.11 En la siguiente figura, se presenta todo el proceso de mitigación de riesgos en un formato gráfico:



Fuente: James Reason

CAPÍTULO 6

ESTABLECIMIENTO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD

6.1 OBJETIVO Y CONTENIDO.

6.1.1 Este capítulo se concentra en los factores que deben considerarse al establecer un SGS. El capítulo incluye lo siguiente:

- Conceptos Introductorios
- Principios generales de un SGS
- Primer paso: Planificación
- Segundo paso: Compromiso de la Alta Dirección respecto a la Seguridad Operacional: Políticas y Objetivos de Seguridad.
- Tercer paso: Organización.
- Cuarto paso: Identificación de peligros.
- Quinto paso: Gestión de riesgos.
- Sexto paso: Capacidad de investigación.
- Séptimo paso: Capacidad de análisis de seguridad operacional
- Octavo paso: Promoción de la seguridad operacional y capacitación.
- Noveno paso: Documentación sobre gestión de la seguridad operacional y gestión de la información
- Décimo paso: Vigilancia de la Seguridad Operacional y supervisión de la eficacia de la seguridad operacional

6.2 CONCEPTOS INTRODUCTORIOS.

6.2.1 Un SGS puede ser comparado con una caja de herramientas. Es una caja de herramientas que contiene todos los instrumentos que OSINERGMIN tiene para ser capaz de controlar los riesgos de seguridad de las consecuencias de los peligros durante el desarrollo de las actividades que permitan cumplir su misión, que es la razón por qué la organización existe. La organización por sí misma, podría generar peligros durante el desarrollo de sus actividades. Es importante reconocer que el SGS por sí mismo no es, ni un instrumento, ni ningún proceso. El SGS es la actual caja de herramientas de OSINERGMIN, donde actualmente contiene los instrumentos empleados para conducir los dos procesos básicos de gestión seguridad (la identificación de riesgo y la gestión de riesgos de seguridad) en sus sistemas de Salud y Seguridad de la persona y Seguridad Ambiental.

6.2.2 Como una caja de herramientas, el SGS debe asegurar que cuando son necesarios instrumentos específicos para la identificación de peligros y la gestión de riesgos de seguridad:

a) Estén al alcance de la mano y listos para usar los instrumentos adecuados para la ejecución de la tarea.

b) Instrumentos y tarea correctamente relacionados.

c) Los instrumentos son diseñados a las necesidades y restricciones de la organización.

d) Los instrumentos pueden fácilmente ser encontrados dentro de la caja de herramientas, sin la innecesaria perdida de tiempo y recursos.

Esta perspectiva es importante, porque el SGS simplemente es un caparazón protector que asegura el almacenaje apropiado y oportuno, la disponibilidad y la utilización de los instrumentos necesarios para entregar procesos específicos de gestión de seguridad en la organización. Sin los apropiados instrumentos, el SGS es sólo un caparazón vacío.

6.2.3 Una característica importante que comentamos anteriormente, es que la gestión de seguridad no se restringe a solamente una actividad específica de la organización, generalmente lo más visible (Salud y Seguridad de las Personas), que podría generar peligros. La gestión de seguridad dirige todas las actividades de la organización. El alcance de SGS, por lo tanto, abarca todas las actividades de la organización.

6.2.4 El SGS debe comenzar con la alta dirección. Una gestión eficaz de la seguridad requiere algo más que establecer una estructura orgánica y promulgar reglas y procedimientos, requiere una dedicación y un compromiso genuinos de la alta dirección. Las actitudes, las decisiones y los métodos de funcionamiento en el nivel de toma de decisiones demuestran la prioridad que se otorga a la seguridad. La indicación inicial del compromiso respecto a la seguridad se refleja en la declaración y los objetivos de la organización.

6.2.5 La asignación de recursos adecuados es un indicador clave de la dedicación de la administración a la seguridad. Establecer una estructura de gestión apropiada, asignar responsabilidades y líneas de rendición de cuentas y destinar los recursos necesarios deben ser tareas acordes con los objetivos de seguridad declarados de la organización. Personal suficiente con experiencia, instrucción oportuna y pertinente, y financiación para el equipo y las instalaciones que se necesitan son elementos fundamentales para crear un entorno de trabajo en que cada uno toma la seguridad con seriedad.

6.2.6 En las culturas de seguridad efectivas, hay líneas de rendición de cuentas claras, obligaciones claramente definidas y procedimientos bien entendidos. El personal comprende claramente sus responsabilidades y sabe de qué debe informar, a quién y cuándo. La administración superior examina no solo la eficacia financiera de la organización sino también la eficacia en materia de seguridad

6.2.7 Por consiguiente, la cultura de seguridad es tanto una cuestión de actitud como de estructura, relacionada con los individuos y las organizaciones; tiene que ver con la necesidad de percibir los problemas de seguridad y también con la de conjugarlos con las medidas pertinentes. La cultura de seguridad está relacionada con cosas intangibles como las actitudes personales y el estilo de la organización; por lo tanto, es difícil medirla, especialmente cuando el criterio principal es la ausencia de accidentes e incidentes. Aun así, las actitudes personales y el estilo de la empresa permiten o facilitan la existencia de condiciones y actos inseguros que son precursores de accidentes e incidentes.

6.3 CARACTERISTICAS GENERALES DE UN SGS.

6.3.1 Las características generales de un SGS son:

a) Sistemático
b) Proactivo
c) Explicito

6.3.2 **Sistemático.** Las actividades de gestión de la seguridad están de acuerdo a un plan predeterminado y se aplican de manera consistente a través de toda la organización.

6.3.3 **Proactivo.** Una aproximación que enfatiza la identificación de los peligros y el control y mitigación de los riesgos, antes que puedan ocurrir eventos que afectan la seguridad.

6.3.4 **Explícito.** Todas las actividades de gestión de la seguridad están documentadas y son visibles.

6.3.5 Iniciar y hacer funcionar un proceso eficaz de gestión de la seguridad puede ser una tarea difícil. La adopción de un enfoque sistémico ayudará a que los elementos necesarios para construir un sistema eficaz estén presentes. En esta sección se exponen 10 pasos para integrar los diversos elementos en un SGS coherente. Implantar simultáneamente todas las funciones de un SMS sería una tarea abrumadora, o casi imposible, por lo que debe abordarse gradualmente. Esto permitiría a la organización adaptarse y conocer los requisitos y los resultados de cada paso antes de proceder.

6.3.6 Si bien hay cierta lógica en la secuencia de los pasos descritos, no es obligatoria. Algunos pasos pueden postergarse hasta que llegue un momento más apropiado. El progreso se puede observar empleando la lista de confirmación de las tareas presentada en cada paso para destacar las medidas necesarias.

6.4 PRIMER PASO: PLANIFICACIÓN

Examen

6.4.1 De conformidad con la práctica de gestión general, la gestión de la seguridad comienza con una planificación cuidadosa. A OSINERGMIN que procura mejorar sus procesos de gestión de la seguridad le convendría nombrar un grupo de funcionarios clave para que lleven a cabo esta fase de planificación.

6.4.2 El grupo de planificación (o establecimiento) quizá pueda aprovechar las fuerzas existentes calculando las capacidades de la organización para la gestión de la seguridad (incluyendo experiencia, conocimientos, procesos, procedimientos, recursos, etc.). Se debe reconocer la falta de experiencia en gestión de la seguridad y también identificar los recursos necesarios para ayudar a elaborar e implantar el SGS. Muchas dependencias operacionales quizá ya tengan procedimientos internos para la investigación de incidentes y la identificación de peligros, la supervisión de la seguridad, etc., se los debería examinar, y quizá modificar para integrarlos en el SGS. Es importante que la organización vuelva a usar tantos procedimientos ya existentes como sea posible, pues no es necesario remplazar los procedimientos y procesos que son conocidos y eficaces. Cuando se construye sobre una base de experiencia como esa, la elaboración de un SGS causa menos trastorno. Durante este proceso de examen, el grupo de planificación también debería examinar las mejores prácticas del sector empleadas en la gestión de la seguridad.

Evaluación de la seguridad

6.4.3 El diseño e implantación de un SGS probablemente será un cambio importante para la organización, que puede generar nuevos peligros para la seguridad. La sinergia de un grupo de funcionarios experimentados que objetan y ponen en duda todos los aspectos del enfoque de la organización, actual y previsto, respecto a la gestión de la seguridad debería reducir el riesgo de tener sorpresas en la implantación del SGS, aumentar el conocimiento del grupo respecto a la situación y a las necesidades actuales y preparar el camino para implantar eficazmente el cambio.

Indicadores de eficacia de la seguridad operacional y objetivos de seguridad operacional

6.4.4 El grupo de planificación debería definir los indicadores de eficacia de la seguridad operacional y establecer los objetivos de esa eficacia tanto para la organización como para las empresas que supervisa OSINERGMIN para su programa de seguridad operacional. Estos indicadores y objetivos deben ser realistas y tomar en cuenta varias cosas: tamaño, complejidad, tipo de explotación, base de recursos, etc. de la organización y/o empresas que se supervisan. También debe fijarse un período realista para alcanzar los objetivos convenidos. Aun cuando establecer esos indicadores y objetivos pueda ser difícil, los mismos proporcionan la base para evaluar el éxito del SGS.

Estrategia de seguridad operacional

6.4.5 Basándose en los objetivos de seguridad, el grupo de planificación puede elaborar una estrategia realista para satisfacer esas necesidades. La estrategia debería combinar tanto elementos de reacción como preventivos. Dependiendo del número de nuevas iniciativas que se consideren y de los recursos disponibles, podría ser conveniente adoptar un enfoque por etapas. La estrategia también podría definir el grado de formalidad que la organización necesita con respecto a su **"sistema para realizar la gestión de la seguridad".** Durante la elaboración de la estrategia es necesaria la aportación de la Alta Dirección.

Plan

6.4.6 La fase de planificación debería dar como resultado un plan detallado para la elaboración e implantación del SGS. El plan debería considerar aspectos tales como: objetivos, estrategia, procesos de gestión y actividades de seguridad operacional, recursos necesarios y plazos.

Lista de confirmación núm. 1

PLANIFICACIÓN

- Se ha designado al área responsable y al grupo de planificación de la seguridad operacional.
- El grupo de planificación:
  - constituye una base de experiencia apropiada;
  - se reúne regularmente con la administración superior;
  - recibe recursos (incluido el tiempo para las reuniones).
  -
- El grupo de planificación elabora una estrategia y un plan de implantación realistas para un SGS que satisfará las necesidades de la organización en materia de seguridad operacional.
- La administración superior respalda el plan.

6.4.7 Para que el grupo de planificación elabore la estrategia y un plan de implantación realista para un SGS debe determinar cual sería la estructura del SGS para OSINERGMIN y después contrastarla con la actual estructura de la organización, determinar la brecha y hacer el plan de implantación.

Planteamiento de una estructura de un SGS para OSINERGMIN

6.4.8 Los componentes de un SGS para OSINERGMIN podrían ser los siguientes:

a) **Política y objetivos de seguridad**

b) **Gestión del riesgo de seguridad**

c) **Aseguramiento de la seguridad**

d) **Promoción de la seguridad**

6.4.9Los elementos de un SGS para OSINERGMIN podrían ser los siguientes:

a) **Política y objetivos de seguridad**

1) Responsabilidad y compromiso de la dirección
2) Responsabilidades de seguridad de los gerentes
3) Designación del personal clave de seguridad
4) Plan de implementación del SMS
5) Coordinación del plan de respuesta a la emergencia
6) Documentación

b) **Gestión del riesgo de seguridad**

1) Procesos de identificación de peligros
2) Procesos de evaluación y mitigación del riesgo
3) Investigaciones internas de seguridad

c) **Aseguramiento de la seguridad**

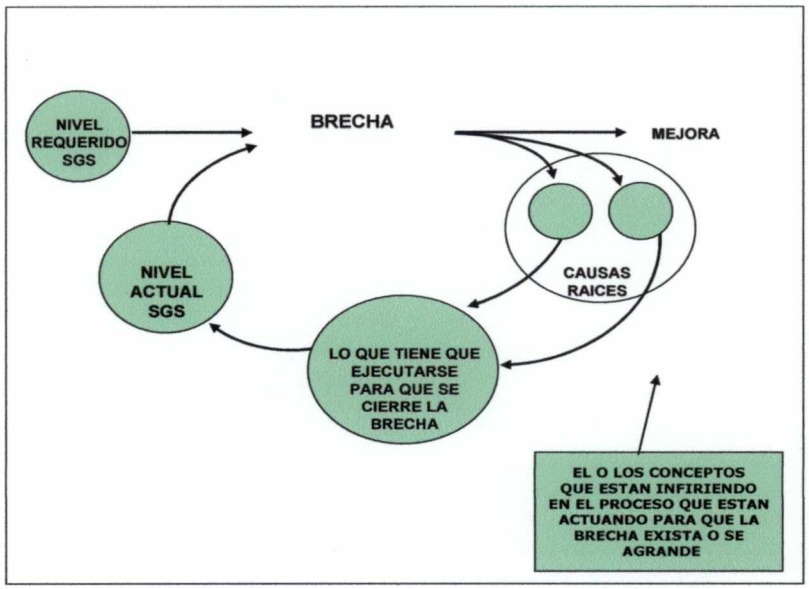
1) Monitoreo y medición de la performance de la seguridad
2) Gestión del cambio
3) Mejora continua del sistema de seguridad

d) **Promoción de la seguridad**

1) Entrenamiento y educación
2) Comunicación de seguridad

Análisis de brechas

6.4.10 El análisis de brechas podríamos aplicar la siguiente metodología



6.5 SEGUNDO PASO: COMPROMISO DE LA ALTA DIRECCIÓN RESPECTO A LA SEGURIDAD OPERACIONAL: POLITICA Y OBJETIVOS DE SEGURIDAD

6.5.1 La responsabilidad final por la seguridad operacional incumbe sobretodo a la alta dirección de OSINERGMIN. Las características de la actitud de la organización respecto a la seguridad operacional — su cultura de seguridad operacional — se deben determinar desde el principio, en la medida en que la alta dirección acepte **la responsabilidad de que las operaciones sean seguras, particularmente por una gestión preventiva de los riesgos.** (Esta percepción también es compartida por la Contraloría General de la Republica y también por una buena analista como Beatriz Boza, ver artículo ¿Autonomía y responsabilidad? para los organismos reguladores, Comercio del 21 de Enero del 2010 página A 4)

6.5.2 El éxito del SGS depende de la medida en que la alta dirección dedique el tiempo, los recursos y la atención que son necesarios para la seguridad operacional como una cuestión básica de gestión. Aquí, los actos son más elocuentes que las palabras. Lo que la administración hace por la seguridad operacional determinará la cultura de seguridad operacional de OSINERGMIN y, por lo tanto, la eficacia de la seguridad operacional.

6.5.3 Las políticas y los objetivos de seguridad operacional determinan lo que OSINERGMIN procura alcanzar y cómo habrá de hacerlo. El compromiso de la administración respecto a la seguridad operacional se demuestra a todo el personal de la organización por medio de, principalmente, las declaraciones de la política y los objetivos de seguridad operacional.

Política de seguridad operacional

6.5.4 El compromiso de la alta dirección respecto a la seguridad operacional debería expresarse formalmente en una declaración de la **política de seguridad operacional** de la organización. Esta declaración debería reflejar **la filosofía** de la organización respecto a la gestión de la seguridad y transformarse en los cimientos sobre los que se construirá el SGS de OSINERGMIN. La política de seguridad describe los métodos y procesos que empleará la organización para lograr los resultados deseados en materia de seguridad operacional y servirá para recordar **"cómo hacemos aquí las cosas".** La creación de una cultura de seguridad operacional positiva comienza con la exposición de una dirección clara e inequívoca.

6.5.5 Una política de seguridad operacional puede adoptar diferentes formas, pero típicamente incluirá declaraciones relacionadas con:

- El objetivo general de seguridad operacional de la organización.
- El compromiso de la alta dirección respecto a la meta de asegurar que todos los aspectos de la explotación satisfagan los objetivos de eficacia de la seguridad operacional.
- El compromiso de la organización de proporcionar los recursos necesarios para la gestión eficaz de la seguridad operacional.
- El compromiso de la organización de hacer que la seguridad operacional sea de alta prioridad.
- La política de la organización respecto a la responsabilidad y rendición de cuentas por la seguridad operacional en todos los niveles de la organización.

6.5.6 La política de seguridad operacional debería constar en un documento escrito, publicado y aprobado por la autoridad del nivel de administración más alto de OSINERGMIN, y comunicada a todo el personal. En el Apéndice 1 de este capítulo se incluye un ejemplo de declaración de política de seguridad operacional de una empresa. Esta declaración constituye una indicación tangible el compromiso de la alta dirección respecto a la seguridad operacional. Una alternativa para este tipo de declaración es una declaración del gerente general sobre el compromiso de la organización respecto al mantenimiento de los niveles de seguridad operacional más elevados. En el Apéndice 2 de este capítulo figura un ejemplo de los temas que debería incluir una declaración de este tipo.

6.5.7 A la hora de preparar la política de seguridad operacional, la alta dirección debería consultar ampliamente con el personal clave a cargo de las actividades operacionales, tales como supervisión y fiscalización. Una consulta asegura que el documento sea importante para el personal, dándole a éste el sentimiento de que la declaración le pertenece. La política de seguridad operacional de OSINERGMIN también debe ser compatible con los reglamentos del Estado.

Objetivos de seguridad operacional

6.5.8 La forma en que OSINERGMIN debería fijar sus objetivos de seguridad operacional debe estar en estrecha relación con la política de seguridad operacional (y la cultura de seguridad operacional). Los objetivos claramente expresados pueden conducir a una dedicación a la acción que reforzará la seguridad operacional en la organización. OSINERGMIN debería fijar sus objetivos de manera formal — enunciando claramente su visión, definiendo los resultados deseados, puntualizando las etapas que deben cumplirse para lograr los objetivos y documentando los procesos.

Lista de confirmación núm. 2

COMPROMISO DE LA ALTA DIRECCIÓN RESPECTO A LA SEGURIDAD OPERACIONAL: POLITICAS Y OBJETIVOS

1. La alta dirección participa en el SGS y ha asumido un compromiso al respecto.
2. La alta dirección ha aprobado la política y los objetivos de seguridad operacional de la organización, el plan de implantación del SGS y las normas de seguridad operacional.
3. Se ha comunicado al personal todo esto, con el respaldo visible de la alta dirección.
4. La política de seguridad operacional ha sido elaborada por la alta dirección y el personal y el gerente general la ha firmado. Esta política:
   - cuenta con la dedicación y la participación de todo el personal;
   - está en armonía con otras políticas operacionales;
   - contiene orientación para aplicarla;
   - expone las responsabilidades y las líneas de rendición de cuentas de directores, jefes y empleados;
   - se refleja en las acciones y decisiones de todo el personal;
   - ha sido comunicada a todo el personal; y
   - se examina periódicamente.
5. Los objetivos y metas de seguridad operacional son prácticos y posibles, y su pertinencia se examina periódicamente.
6. Se han establecido normas de eficacia (que incluyen plazos).
7. Han quedado claramente comprendidas las responsabilidades respecto a las decisiones.
8. Los funcionarios examinan y hacen rendir cuentas a los responsables de los progresos alcanzados con respecto a los objetivos de seguridad operacional.
9. Se han asignado recursos apropiados para dar apoyo al área encargada de seguridad operacional.
10. La alta dirección compromete recursos para corregir los peligros que crean riesgos inaceptables.
11. La alta dirección ha establecido un sistema de notificación para los problemas de seguridad operacional.
12. La alta dirección alienta activamente la participación en los diversos programas de seguridad operacional del SGS.
13. La alta dirección promueve una cultura de seguridad operacional positiva mediante la cual:
    - se procura activamente obtener información sobre seguridad operacional;
    - se capacita al personal para sus responsabilidades en materia de seguridad operacional;
    - la seguridad operacional es una responsabilidad compartida;
    - la información relacionada con la seguridad operacional se difunde entre todo el personal afectado;
    - las fallas y los peligros posibles del sistema conducen prontamente a averiguaciones de la administración y a las reformas necesarias;
    - existe un programa formal para evaluar periódicamente la eficacia de la seguridad operacional; y
    - las nuevas ideas relacionadas con la seguridad operacional son bien recibidas.

6.6 TERCER PASO: ORGANIZACIÓN

6.6.1 El modo en que OSINERGMIN emplee su método para llevar a cabo sus actividades y realizar la gestión de la seguridad operacional influirá en su capacidad para recuperarse de la adversidad (o de situaciones peligrosas) y para reducir los riesgos. Para establecer una organización eficaz que dará apoyo al SGS es fundamental considerar varios puntos, por ejemplo:

- Nombramiento de un área encargada del SGS.
- Una estructura orgánica que facilite la gestión de la seguridad operacional.
- Una declaración de responsabilidades y de rendición de cuentas.
- Creación de un comité de seguridad operacional.
- Capacitación y competencia.

6.6.2 Una de las primeras tareas para establecer un SGS es designar el área que será encargada de su gestión. Las actividades de gestión de la seguridad operacional necesitan un coordinador (un promotor) como la fuerza que impulsará los cambios sistémicos necesarios para implantar la seguridad operacional en todo OSINERGMIN. Sus responsabilidades incluyen promover la conciencia de la seguridad operacional y asegurarse de que la gestión de la seguridad operacional tiene el mismo nivel de prioridad en toda la organización que cualquier otro proceso.

6.6.3 El jefe de área designado debería ser responsable de todos los aspectos de funcionamiento del SGS. Esto incluiría asegurar que la documentación de seguridad operacional refleja con precisión el entorno actual, supervisar la eficacia de las medidas correctivas, proporcionar informes periódicos sobre la eficacia de la seguridad operacional y proveer asesoramiento independiente al gerente general, a los directivos de alto nivel y a otros miembros del personal sobre cuestiones relacionadas con la seguridad operacional.

Estructura orgánica y declaración de responsabilidades y líneas de rendición de cuentas

6.6.4 La estructura orgánica en OSINERGMIN, sería, salvo mejor parecer, el Área de Control de la Gestión, donde habría que incrementar sus responsabilidades e incluir en el sistema de Gestión del Desempeño los objetivos de seguridad. El sistema de Gestión de Desempeño instalado en OSINERGMIN es una buena herramienta de rendición de cuentas.

Comité de seguridad operacional

6.6.5 Además de ser necesario el grupo de planificación inicial de un SGS (Primer paso), sería conveniente que OSINERGMIN establezca también un comité de seguridad operacional. El comité de seguridad operacional, de establecerse, cuyo presidente sería el gerente general, debería incluir al jefe del área encargada del SGS así como funcionarios de alto nivel. El objetivo del comité de seguridad operacional es proveer un foro para examinar problemas relacionados con la eficacia de la seguridad operacional de la organización y el estado del SGS. El comité de seguridad operacional formula recomendaciones respecto a las decisiones de política de seguridad operacional y examina los resultados de la eficacia de la seguridad operacional. Durante la fase de implantación inicial de un SMS, el comité debería examinar también el progreso del proceso de implantación. Las atribuciones del comité de seguridad operacional deberían estar documentadas en el manual de gestión de la seguridad operacional de la organización.

Documentación

6.6.6 La documentación de SGS debe estar a cargo del jefe del área encargado donde incluirá entre otros aspectos:

- Documentación y registros del SMS.
- Registros de gestión.
- El manual de sistemas de gestión de la seguridad operacional

Lista de confirmación núm. 3

ORGANIZACIÓN

1) La estructura orgánica facilita:
   - las líneas de comunicación entre el jefe de área encargado del SGS y el gerente general y con los funcionarios de alto nivel;
   - la definición clara de autoridades, responsabilidades y rendición de cuentas evitando malentendidos, superposiciones y conflictos (por ejemplo, entre el jefe del área encargado del SGS y los funcionarios de alto nivel); y
   - la identificación de peligros y vigilancia de la seguridad operacional.

2) Se ha nombrado el jefe de área encargado del SGS (con la capacidad y las competencias apropiadas).

3) Las funciones y responsabilidades del jefe de área encargado del SGS (y del personal) están claramente definidas y documentadas.

4) El comité de seguridad operacional se reúne regularmente para examinar los resultados respecto a la seguridad operacional y formular recomendaciones para la administración superior.

5) El jefe del área designado del SGS y su personal han recibido instrucción adecuada en seguridad operacional.

6) El personal y la administración comprenden y apoyan las funciones del jefe del área encargado del SGS y éste tiene apoyo del gerente general.

6.7 CUARTO PASO: IDENTIFICACIÓN DE PELIGROS

6.7.1 Los riesgos y costos inherentes de las empresas a los subsectores que OSINERGMIN supervisa y las propias de la organización, requieren un proceso racional para la toma de decisiones. La aplicación de procesos de gestión de riesgos es crítica para un programa eficaz de gestión de la seguridad operacional. Los riesgos no pueden eliminarse siempre y no todas las medias concebibles de gestión de la seguridad operacional son económicamente factibles. La gestión de riesgos facilita el equilibrio, comenzando con la identificación de peligros.

6.7.2 Como se dijo en el Capítulo 4, la creación y aplicación de programas eficaces de identificación de peligros es fundamental para una gestión eficaz de la seguridad. Una organización puede partir de una amplia variedad de actividades de seguridad para identificar los peligros o problemas que justifican nuevas medidas. Algunos de estos problemas pueden derivar de peligros específicos de la seguridad operacional que comprometen una parte de la explotación. Otros problemas que merecen atención pueden derivar de deficiencias de organización, por lo que las defensas del sistema que deberían funcionar no funcionan.

6.7.3 La identificación de peligros puede ser por reacción, proactiva y preventiva. La observación de tendencias, la notificación de sucesos y las investigaciones obedecen fundamentalmente a una reacción. Las auditorias, la supervisión son procesos proactivos. Los procesos de identificación de peligros son procesos preventivos.

6.7.4 A OSINERGMIN le interesa saber cuáles son los posibles puntos débiles en las defensas del sistema que podrían conducir a un accidente o comprometer de otro modo la eficiencia de la explotación, el desarrollo de una cultura de seguridad de reporte proactivo, es decir no punitivo si son errores es indispensable. Si los trabajadores de OSINERGMIN van a trabajar en un clima de temor al castigo por descuidos, lapsos y equivocaciones normales en sus obligaciones diarias, probablemente los errores y las condiciones inseguras permanezcan ocultos.

Lista de confirmación núm. 4

IDENTIFICACIÓN DE PELIGROS

1) Se han implantado mecanismos formales (tales como evaluaciones y auditorías de la seguridad operacional) para la identificación sistemática de peligros.

2) Funciona un sistema de notificación de sucesos e incluso un sistema de notificación voluntaria de incidentes.

3) La gerencia general ha proporcionado recursos adecuados para la identificación de peligros.

4) El personal recibe la instrucción necesaria como apoyo a los programas de identificación de peligros.

5) Personal competente administra los programas de identificación de peligros, manteniendo su pertinencia con respecto a las operaciones.

6) El personal involucrado en incidentes registrados o notificados sabe que no será penalizado por errores normales; la administración fomenta un entorno no punitivo (justo).

7) Todos los datos de peligros identificados se registran, almacenan y analizan sistemáticamente.

8) Se han adoptado medidas de seguridad para proteger el material vulnerable.

6.8 QUINTO PASO: GESTIÓN DE RIESGOS

6.8.1 La gestión de riesgos como ya explicamos en forma bastante específica en el Capítulo 5 comprende tres elementos esenciales: identificación de peligros, evaluación de riesgos y mitigación de riesgos. La gestión de riesgos sirve para concentrar las actividades de seguridad operacional en aquellos peligros que presentan riesgos más elevados. Todos los peligros identificados se evalúan críticamente y se ponen en orden de prioridad según su potencial de riesgo. Estos peligros pueden ser evaluados subjetivamente por personal experimentado o pueden ser evaluados empleando técnicas más formales, que a menudo requieren conocimientos analíticos.

6.8.2 Lo que si vamos a recalcar es lo relacionado a las defensas, concepto que muchas organizaciones no tienen bien en claro ó tienen sistemas jóvenes como los de OSINERGMIN en sus sistemas de Salud y Seguridad de las personas y Seguridad

Ambiental. Al evaluar los riesgos, se deben evaluar las defensas que se han adoptado para protegerse de esos peligros. Estas defensas pueden contribuir, por su ausencia, mal uso, diseño deficiente o condiciones, a que se produzca el suceso o exacerbar los riesgos. Por medio un procedimiento de evaluación de riesgos se puede determinar si los riesgos son objeto de una gestión apropiada o si están controlados. Si los riesgos son aceptables, la operación puede continuar. Si los riesgos son inaceptables, deberían adoptarse medidas para aumentar las defensas o bien eliminar o evitar el peligro.

Lista de confirmación núm. 5

GESTIÓN DE RIESGOS

1) Se han establecido criterios para evaluar los riesgos.

2) Personal competente analiza y da orden de prioridad a los riesgos.

3) Se evalúan las medidas viables de control de riesgos.

4) La alta dirección toma medidas para reducir, eliminar o evitar los riesgos.

5) El personal está conciente de las medidas adoptadas para evitar o eliminar los peligros identificados.

6) Se han implantado procedimientos para confirmar que las medidas adoptadas tienen el efecto previsto.

6.9 SEXTO PASO: CAPACIDAD DE INVESTIGACIÓN

6.9.1 Así como en un sistema de gestión de calidad, los auditores externos califican sus observaciones en: no conformidad mayor, no conformidad menor, requiere corrección y oportunidad de mejora. Del mismo modo las observaciones relacionadas con la seguridad operacional deben investigarse. A menudo estas observaciones revelan que había varios signos de advertencia. La investigación de sucesos ó de observaciones puede identificar los signos de advertencia, haciendo que los signos similares se puedan reconocer en el futuro, antes de que se produzcan sucesos peligrosos (no conformidades).

6.9.2 Si bien OSINERGMIN investiga accidentes e incidentes graves que deben notificarse obligatoriamente, un SGS eficaz debe incluir la misma capacidad de investigar esos sucesos desde una perspectiva de la organización. Sin embargo, **es necesario poner en claro, que el valor de estas investigaciones para la gestión de la seguridad operacional es proporcional a la calidad de la actividad de investigación.** Sin una metodología estructurada, es difícil integrar y analizar toda la información pertinente extraída de esas investigaciones para evaluar eficientemente los riesgos y darles prioridad y para recomendar las medidas que son necesarias para mejorar la seguridad operacional. Determinar la culpa no debe ser la actividad primaria de esas investigaciones de seguridad operacional.

6.9.3 Identificar la experiencia que debe extraerse de un suceso relacionado con la seguridad operacional requiere comprender no sólo **qué** ocurrió, sino también **por qué** ocurrió. Una comprensión completa de por qué ocurrió un suceso requiere una investigación que mira más allá de las causas obvias y se concentra en identificar todos los factores, algunos de los cuales pueden estar relacionados con puntos débiles en las defensas del sistema o en otros problemas de la organización.

Lista de confirmación núm. 6

CAPACIDAD DE INVESTIGACIÓN

1) El personal de operaciones clave ha recibido instrucción formal en investigaciones de seguridad operacional.

2) Cada informe sobre peligros e incidentes se evalúa con una investigación de seguridad operacional más a fondo cuando es necesario.

3) La gerencia general apoya la adquisición y el análisis de información relacionada con la seguridad operacional.

4) La gerencia general se interesa activamente en los resultados de las investigaciones y aplica procedimientos de gestión de riesgos para los peligros identificados.

5) La experiencia adquirida en seguridad operacional se difunde ampliamente.

6) Se informa al área responsable de la normatividad de las cuestiones de seguridad operacional importantes que podrían afectar a otros explotadores o que requieren medidas adicionales de reglamentación.

6.10 SÉPTIMO PASO: CAPACIDAD DE ANÁLISIS DE SEGURIDAD OPERACIONAL

6.10.1 El análisis de seguridad operacional es el proceso de organizar y evaluar hechos objetivamente. Siguiendo las reglas básicas de la lógica y empleando métodos reconocidos e instrumentos analíticos, los hechos conocidos se consideran sistemáticamente de modo que puedan extraerse conclusiones válidas. Cuando el análisis se realiza bien, otras personas que siguen el mismo razonamiento llegarán a las mismas conclusiones.

6.10.2 El análisis de seguridad operacional se aplica en áreas tales como:

a) Análisis de tendencias.

b) Investigación de sucesos.

c) Identificación de peligros.

d) Evaluación de riesgos.

e) Evaluación de medidas de mitigación de riesgos.

f) Supervisión de la eficacia de la seguridad operacional.

6.10.3 El análisis de seguridad operacional requiere habilidades particulares y experiencia. Ofrecer argumentos convincentes para el cambio depende de una buena capacidad analítica.

Lista de confirmación núm. 7

CAPACIDAD DE ANÁLISIS DE SEGURIDAD OPERACIONAL

1) El jefe del área encargada del SGS tiene experiencia o ha recibido instrucción en métodos analíticos, o tiene acceso a analistas de seguridad operacional competentes.
2) Se dispone de instrumentos analíticos (y apoyo de especialistas) para efectuar los análisis de seguridad operacional.
3) La organización mantiene una base de datos de seguridad operacional fiable.
4) Se tiene acceso a otras fuentes de información.
5) La información sobre peligros y los datos sobre eficacia se controlan regularmente (análisis de tendencias, etc.).
6) Los análisis de seguridad operacional están sujetos a un proceso de prueba (evaluación entre colegas).
7) Se hacen recomendaciones de seguridad operacional a la gerencia general y se toman medidas correctivas que se siguen de cerca para asegurarse de que son apropiadas y eficaces.

6.11 OCTAVO PASO: PROMOCIÓN DE LA SEGURIDAD OPERACIONAL Y CAPACITACIÓN

6.11.1 Mantener al personal de OSINERGMIN informado acerca de los problemas de seguridad operacional actuales, por medio de instrucción, literatura y participación en cursos y seminarios sobre seguridad operacional, etc., mejora el estado de la seguridad operacional en la organización. Proveer a todo el personal de instrucción apropiada (independientemente de la disciplina profesional de cada uno) es una indicación del compromiso de la alta dirección respecto a un SGS eficaz. (Una administración débil quizá considere la instrucción como un gasto, en vez de considerarla una inversión en la viabilidad futura de la organización).

6.11.2 Los empleados nuevos deben saber qué se espera de ellos y cómo funciona el SGS de OSINERGMIN. La instrucción inicial debería poner de relieve "cómo hacemos aquí las cosas". Los empleados con más experiencia pueden necesitar cursos de actualización para determinados procedimientos de seguridad operacional en que la participación directa de ellos puede ser necesaria. Independientemente de su nivel de experiencia, todos los empleados se benefician de la información sobre los peligros identificados, las medidas de seguridad operacional adoptadas, la experiencia adquirida al respecto, etc.

Lista de confirmación núm. 8

PROMOCIÓN DE LA SEGURIDAD OPERACIONAL Y CAPACITACIÓN

1) La alta dirección reconoce que todos los niveles de la organización necesitan instrucción en gestión de la seguridad operacional y que las necesidades varían.
2) Las descripciones de puestos reflejan los requisitos de competencia.
3) Todo el personal recibe cursos de familiarización sobre seguridad operacional y participa en la instrucción permanente específica para la gestión de la seguridad operacional.
4) OSINERGMIN tiene un programa eficaz para la promoción oportuna de cuestiones de seguridad operacional.
5) Los miembros del personal están conscientes de su función en los elementos del SGS pertinentes a sus obligaciones.
6) Se imparte instrucción adicional sobre conciencia de la seguridad operacional cuando el entorno de las operaciones cambia (requisitos, reglamentarios, etc.).
7) El personal comprende que la gestión de la seguridad operacional no tiene ninguna relación con atribuir culpas.

6.12 NOVENO PASO: DOCUMENTACIÓN SOBRE GESTIÓN DE LA SEGURIDAD OPERACIONAL Y GESTIÓN DE LA INFORMACIÓN

6.12.1 Las organizaciones que tienen éxito y logran una gestión de la seguridad operacional responsable siguen un enfoque disciplinado en cuanto a la gestión de la documentación y la información. Se necesita documentación oficial para dar al SGS un fundamento autorizado, que clarifique la relación de la gestión de la seguridad operacional con las otras funciones de la organización, la forma en que las actividades de gestión de la seguridad operacional se integran con estas otras funciones y cómo las actividades de gestión de la seguridad operacional están relacionadas con la política de seguridad operacional de la organización. Esta información debe figurar en un manual de gestión de la seguridad operacional.

6.12.2 La documentación: Política de seguridad y objetivos, define, documenta y respalda la política de seguridad confirmando los objetivos identificados durante la fase de planificación, incluyendo un compromiso para:

- Cumplir los más altos estándares de seguridad.
- Observar todos los reglamentos aplicables, así como las normas internacionales y las mejores prácticas.
- Proveer los recursos adecuados.
- Cumplir con la seguridad como responsabilidad primaria de todos los gerentes.
- Asegurar que la política es comprendida, implementada y mantenida en todos los niveles.

6.12.3 Manual del sistema de gestión de seguridad:

- Instrumento clave para comunicar la aproximación de la organización en materia de seguridad a toda la organización.
- Documenta todos los aspectos del SGS, incluyendo la política de seguridad, objetivos, procedimientos y responsabilidades individuales en materia de seguridad.

6.12.4 Contenido del Manual:

1. Alcance del sistema de gestión de la seguridad.
2. La política y objetivos de seguridad.
3. Responsabilidades de seguridad.
4. Personal clave de seguridad.
5. Procedimientos de control de la documentación.
6. Esquemas de identificación del peligro y gestión del riesgo.
7. Monitoreo de la performance de la seguridad.
8. Planificación de respuesta a la emergencia.
9. Gestión del cambio.
10. Auditoría de seguridad.
11. Promoción de la seguridad.
12. Actividades contratadas

Lista de confirmación núm. 9

DOCUMENTACIÓN SOBRE GESTIÓN DE LA SEGURIDAD OPERACIONAL Y GESTIÓN DE LA INFORMACIÓN

1) La administración responde a la necesidad de un control cuidadoso de la documentación y los datos.
2) El SGS está bien documentado en un manual de gestión de la seguridad operacional.
3) Los documentos se actualizan regularmente y están disponibles para quienes los necesitan.
4) Se han adoptado medidas fiables para la protección de información delicada sobre seguridad operacional.
5) Se dispone del equipo apropiado y de apoyo técnico para la gestión de la información sobre seguridad operacional.
6) Las bases de datos sobre seguridad operacional se emplean para el análisis de la seguridad operacional y la supervisión de la eficacia.
7) El personal competente tiene acceso a las bases de datos sobre seguridad operacional.
8) El personal ha recibido la instrucción necesaria para usar y mantener el sistema de gestión de la información sobre seguridad operacional.

6.13 DÉCIMO PASO: VIGILANCIA DE LA SEGURIDAD OPERACIONAL Y SUPERVISIÓN DE LA EFICACIA DE LA SEGURIDAD OPERACIONAL

6.13.1 Un enfoque sistémico para la gestión de la seguridad operacional requiere **"cerrar el ciclo".** También se necesita retorno de información para evaluar si los **nueve** primeros pasos funcionan bien. Esto se logra por medio de la vigilancia de la seguridad operacional y la supervisión de la eficacia de la seguridad operacional.

6.13.2 La **vigilancia de la seguridad operacional** se puede llevar a cabo por medio de inspecciones, encuestas y auditorías. ¿Hace nuestro personal lo que debe hacer? En OSINERGMIN, se realizan regularmente auditorías formales de calidad, con una pequeña instrucción ese mismo equipo podría pasar a la vez una auditoría de seguridad. Las auditorías de la seguridad operacional garantizan al personal y a la administración que las actividades de la organización se realizan del modo que debe ser (es decir, con seguridad).

6.13.3 La **supervisión de la eficacia de la seguridad operacional** valida el SGS, confirmando no sólo que las personas hacen lo que deben hacer, sino también que los esfuerzos colectivos han logrado los objetivos de seguridad operacional de la organización. Por evaluaciones regulares, la administración puede perseguir el mejoramiento continuo de la gestión de la seguridad operacional y asegurarse de que el SGS sigue siendo eficaz y pertinente para las operaciones de la organización. Sistema de Gestión del desempeño de OSINERGMIN.

6.14 CONCLUSIÓN

6.14.1 La gestión exitosa de la seguridad es una responsabilidad funcional de todos los niveles de gestión y de supervisión de la organización **(Sistemático).**

6.14.2 El principio debe estar reflejado en la estructura de la organización **(Explicito).**

6.14.3 La organización debe definir, documentar y comunicar las líneas individuales de responsabilidad y autoridad con respecto a la gestión de la seguridad en las operaciones **(Explicito).**

6.14.4 Los medios para administrar la seguridad dentro de la organización incluye la identificación del peligro, la gestión del riesgo, el aseguramiento de la seguridad y la promoción de la seguridad **(Proactivo).**

Lista de confirmación núm. 10

VIGILANCIA DE LA SEGURIDAD OPERACIONAL Y SUPERVISIÓN DE LA EFICACIA DE LA SEGURIDAD OPERACIONAL

1) Se han aceptado indicadores de eficacia de la seguridad operacional y se han fijado objetivos de seguridad operacional realistas.
2) Se han asignado recursos adecuados para las funciones de vigilancia de la seguridad operacional y supervisión de la eficacia de la seguridad operacional.
3) Se procura obtener información del personal y éste la proporciona sin temer repercusiones.
4) Se realizan regularmente auditorías de la seguridad operacional en todas las áreas operacionales de la organización (incluidas las actividades de las entidades contratistas).
5) La vigilancia de la seguridad operacional incluye el examen sistemático de toda la información recibida, por ejemplo: evaluaciones de seguridad operacional, resultados del programa de gestión de calidad, análisis de tendencias de seguridad operacional, encuestas y auditorías de seguridad operacional.
6) Los resultados se comunican al personal y cuando es necesario se ponen en práctica medidas de reforma para reforzar el sistema.

Apéndice 1 del Capítulo 6

EJEMPLO DE DECLARACIÓN DE POLÍTICA DE SEGURIDAD OPERACIONAL

La seguridad operacional es la primera prioridad en todas nuestras actividades. Hemos asumido el compromiso de aplicar, elaborar y mejorar las estrategias, los sistemas de gestión y los procesos para asegurarnos de que todas nuestras actividades como organismo supervisor mantienen el nivel más elevado de eficacia de la seguridad operacional y se ajustan a las normas nacionales.

Nuestro compromiso es:

a) Elaborar e incorporar una cultura de seguridad operacional en todas nuestras actividades como un organismo supervisor de la inversión en energía y minería, que reconoce la importancia y el valor de una gestión eficaz de la seguridad operacional y que, en todo momento, la seguridad operacional es lo más importante.

b) Definir claramente para todo el personal sus responsabilidades y su obligación de rendir cuentas respecto a la elaboración y puesta en práctica de una estrategia de seguridad operacional en la supervisión de la inversión en energía y minería y su eficacia.

c) Reducir los riesgos relacionados con las operaciones de las empresas explotadoras y/o proveedoras de servicio del ámbito de OSINERGMIN hasta el nivel más bajo prácticamente posible o que se puede alcanzar.

d) Asegurarnos de que los sistemas y servicios obtenidos por contratación externa y que repercuten en la seguridad de nuestras actividades cumplan las normas de seguridad operacional pertinentes.

e) Elaborar activamente y mejorar nuestros procesos de seguridad operacional para que sean conformes a las normas nacionales establecidas.

f) Cumplir, y cuando sea posible sobrepasar, los requisitos y las normas de la ley y los reglamentos.

g) Asegurarnos de que todos los miembros del personal poseen información e instrucción sobre seguridad operacional, que son competentes en cuestiones de seguridad operacional y que solamente se les asignan tareas acordes con sus competencias.

h) Asegurarnos de que se dispone de recursos humanos con conocimientos e instrucción suficientes para poner en práctica la estrategia y la política de seguridad operacional.

i) Establecer y medir nuestra eficacia de la seguridad operacional de acuerdo con objetivos y metas realistas.

j) Alcanzar los niveles más altos de las normas y la eficacia de la seguridad operacional en todas nuestras actividades como supervisor de la inversión en energía y minería.

k) Mejorar continuamente nuestra eficacia en materia de seguridad operacional.

Apéndice 2 del Capítulo 6

TEMAS QUE DEBERÍAN FIGURAR EN LA DECLARACIÓN DE UN GERENTE GENERAL SOBRE EL COMPROMISO DE LA ORGANIZACIÓN RESPECTO A LA SEGURIDAD OPERACIONAL

Seguidamente se indican los temas que frecuentemente se incluyen en las declaraciones sobre el compromiso de la organización respecto a la seguridad operacional. Después de cada tema figuran los asuntos que comúnmente se tratan para ampliar la postura de la organización sobre ese tema.

a) **Valores básicos**. Entre nuestros valores básicos, incluimos:

1) seguridad operacional, salud y medio ambiente;
2) comportamiento ético; y
3) valoración de las personas.

b) **Principios de seguridad operacional fundamentales**. Nuestros principios de seguridad operacional fundamentales son:

1) La seguridad operacional es una actividad básica y un valor personal.

2) La seguridad operacional es una fuente de nuestras ventajas

3) Nuestra organización será más fuerte si hacemos que la excelencia en la seguridad operacional sea parte integrante de todas las actividades de supervisión.

4) Todos los accidentes y los incidentes graves pueden evitarse.

5) Los funcionarios de todos los niveles son responsables de nuestra eficacia en materia de seguridad operacional, comenzando por el Gerente General.

c) **Elementos básicos de nuestro enfoque de la seguridad operacional**. Los cinco elementos básicos de nuestro enfoque de la seguridad operacional incluyen:

1) **Compromiso de la Alta Dirección:**
   - La excelencia de la seguridad operacional será un componente de nuestra misión.
   - La alta dirección hará que los funcionarios y todos los empleados sean responsables de la eficacia de la seguridad operacional.

2) **Responsabilidad y rendición de cuentas de todos los empleados:**
   - La eficacia de la seguridad operacional será una parte importante de nuestro sistema de evaluación de jefes y empleados.
   - Reconoceremos y premiaremos la eficacia en materia de seguridad operacional.
   - Antes de realizar un trabajo, haremos que todos estén conscientes de las normas y procedimientos de seguridad operacional, así como de la responsabilidad personal de cada uno de observarlos.

3) **Expectativa claramente comunicada de no tener ningún accidente:**
   - Tendremos un objetivo de seguridad personal expresado formalmente por escrito y nos aseguraremos de que todos comprendan y acepten este objetivo.

- Tendremos un sistema de comunicaciones y motivación para mantener a nuestros empleados concentrados en el objetivo de la seguridad operacional.

4) **Auditorías y medición de la eficacia para mejorar:**

- La administración se asegurará de que se realizan regularmente auditorías de la seguridad operacional.
- Concentraremos nuestras auditorías en el comportamiento de las personas así como en las condiciones de los lugares de trabajo.
- Estableceremos indicadores de eficacia que nos ayuden a evaluar nuestra eficacia de la seguridad operacional.

5) **Responsabilidad de todos los empleados:**

- Cada uno de nosotros deberá aceptar la responsabilidad de su propio comportamiento y rendir cuentas del mismo.
- Cada uno de nosotros tendrá la oportunidad de participar en la elaboración de normas y procedimientos de seguridad operacional.
- Comunicaremos abiertamente la información acerca de incidentes de seguridad operacional y compartiremos con otros la experiencia adquirida.
- Cada uno de nosotros se preocupará de la seguridad de los demás en nuestra organización.

d) **Objetivos del proceso de seguridad operacional**. Entre nuestros objetivos se incluyen:

1) Todos los niveles de administración estarán claramente dedicados a la seguridad operacional.
2) Tendremos medidas claras de la seguridad operacional de los empleados, con rendición de cuentas clara.
3) Tendremos comunicaciones abiertas sobre la seguridad operacional.
4) Haremos que todo el personal pertinente participe en el proceso de toma de decisiones.
5) Proporcionaremos la instrucción necesaria para crear y mantener conocimientos útiles para el liderazgo en materia de seguridad operacional.
6) La seguridad de nuestros empleados, clientes y proveedores será una cuestión de estrategia de la organización.

Firma: _____

Gerente General o quien corresponda

BIBLIOGRAFÍA

Human error: Models and Management, James Reason, professor of psychology. Departamento de Sicología Universidad de Manchester.

Managing Business Ris : An integrate Approach, published by the Economist Intelligence Unit in 1995, **James W. Deloach** Jr. Managing Director of Protiviti, Inc

Enterprise- wide Risk Management: Strategies for linking risk and opportunity in June 2000. James **W. Deloach** Jr. Managing Director of Protiviti, Inc

ICAO Safety Management, 2008

Resolución de Contraloría General Nº 320-2006-CG

Resolución de Contraloría General Nº 458-2008-CG