Administración de riesgos empresariales de seguridad

Marcelo Serey González

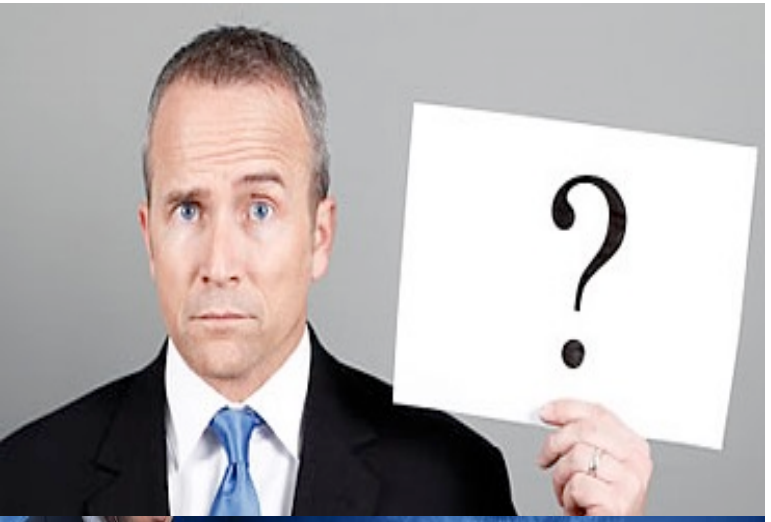
Ing. Prevención de Riesgos

CPO – Asesor de Seguridad Privada

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.



¿COMO PROTEJO MI EMPRESA?

¿Qué quiero proteger? Dinero, productos, personas, imagen etc.

De qué lo quiero proteger? Cuales Amenazas hay entorno a la actividad?

¿Cómo lo voy a proteger? Con qué ?

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

Seguridad como ***Safety*** y **seguridad** como ***Security***:
"Seguridad de los balazos y la seguridad de los costalazos"

Las palabras son la base de la cultura y siendo que tanto **protección** como **seguridad** son al mismo tiempo verbo, adjetivo, adverbio y sustantivo; debemos profundizar en el aprendizaje de conceptos como fundamento del desarrollo profesional.

La seguridad es tanto el proceso como la percepción de control resultante.

La protección y seguridad históricamente estuvieron relacionas con la respuesta a amenazas militares y aunque todavía utilizan ciertas herramientas comunes a la ciencia de la defensa; en la actualidad se han desarrollado por si misma hasta establecer normas y métodos estandarizados reconocidos internacionalmente. Convirtiéndose de paso en una ciencia por derecho propio.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

PROTECCIÓN (traducción de la palabra inglesa Security) son las medidas para prevenir y reaccionar frente a los riesgos que son generados intencionalmente por los humanos (espionaje, sabotaje, hurto y asalto entre otros).

SEGURIDAD (traducción de la palabra inglesa Safety) se utiliza para referirnos a las medidas para prevenir y reaccionar frente a los riesgos de accidentes (por condiciones laborales y fenómenos naturales, entre otros).

"Saber que quiero proteger define el tipo de seguridad que necesitamos respecto a la amenaza que enfrentaremos"

La **PROTECCION INTEGRAL DE RECURSOS** es el término contemporáneo que abarca la integración de medios, tecnología y personal en labores de protección y seguridad física frente a los riesgos generados intencional y accidentalmente por humanos (antrópicos), y los generados por la naturaleza; incluye manejo de emergencias, seguridad industrial, protección contra el fuego. Todo riesgo con su correspondiente afectación económica, por lo cual en muchos casos es sinónimo al término moderno **CONTROL DE PÉRDIDAS.**

El **ESPECIALISTA EN PROTECCION INTEGRAL o DE CONTROL DE PÉRDIDAS** tiene como función identificar todas fuentes de potenciales riesgos de protección (personal interno –indeseable- o agresores externos) y de seguridad (actos no intencionados o fenómenos naturales) para controlarlos.

Ambas funciones, la protección y seguridad comparten una misión en común, proteger a ciertos recursos plenamente identificados frente a comportamientos y condiciones que potencialmente causarán pérdida.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

La seguridad en una organización será el resultado de :

P1 + P2 + M + R1 + C + R2 = SEGURIDAD

- P1: Prevención
- P2: Preparación
- M: Mitigación
- R1: Respuesta
- C: Continuidad
- R2: Recuperación

Curso Jefes de Seguridad Privada

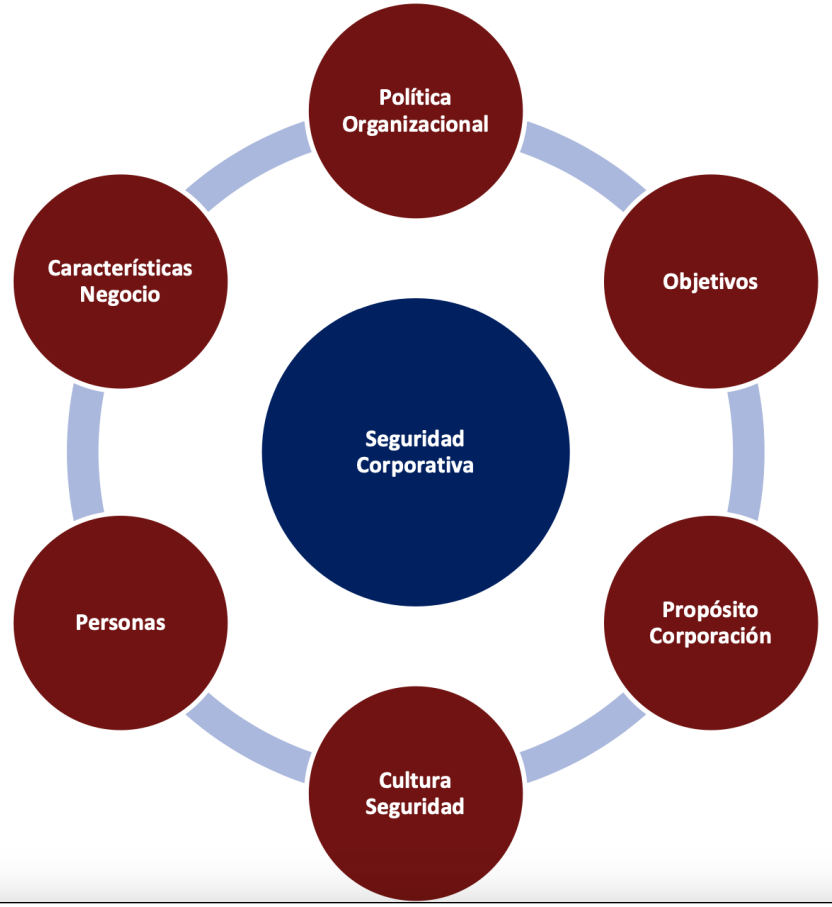
Módulo 1. Control de riesgos empresariales de seguridad.

SISTEMA DE GESTIÓN DE SEGURIDAD CORPORATIVA

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

CULTURA CORPORATIVA DE SEGURIDAD

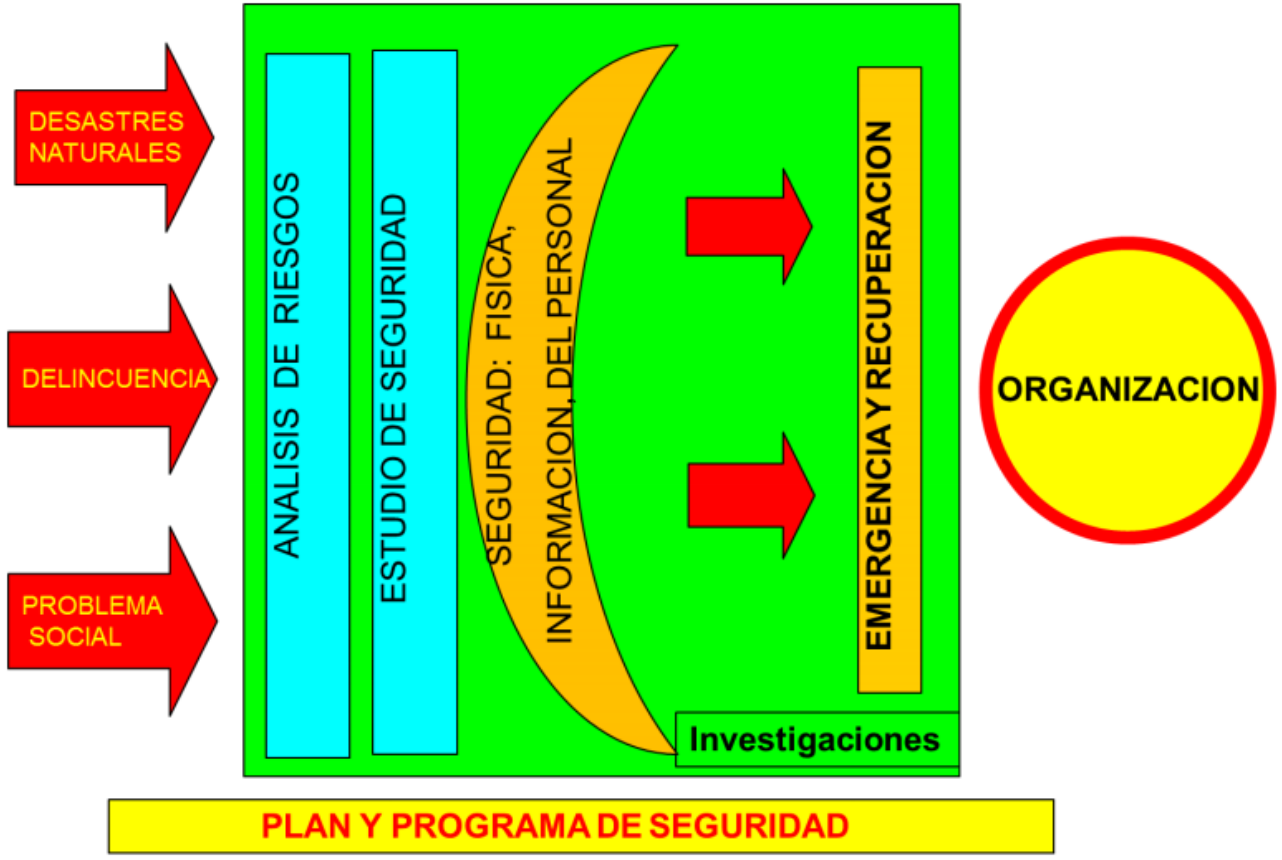


Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

PROGRAMA DE SEGURIDAD EMPRESARIAL

Un sistema de Protección física debe ser capaz de integrar a personas, procedimientos, equipamiento y la tecnología para la protección de los activos.



Los **RECURSOS** que protegemos son “bienes” o “Activos” materiales o intangibles, pero siempre tienen valor para su propietario; es decir que si son robados, perdidos, destruidos o dañados, alguna organización o individuo sufrirá una pérdida. Los recursos a proteger tienen cuatro clasificaciones básicas (que en orden de prioridad incluyen):

- **PERSONAS** Constituyen el capital humano – trabajadores, contratista, clientes, visitantes, la comunidad.
- **INFORMACIÓN** Constituyen capital intelectual: información propietaria desarrollada o acumulada con esfuerzo, datos confidenciales, planes).
- **PROPIEDADES** Constituyen el capital financiero: muebles o inmuebles que poseen características físicas.
- **IMAGEN** Constituyen en el capital comercial: reputación pública, frente a clientes, posicionamiento del negocio).

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

CÓMO IDENTIFICAR ACTIVOS

- Procesos y Funciones
- Infraestructura
  - ✓ Componentes críticos,
  - ✓ Sistemas de protección,
  - ✓ Seguridad.
- Identificar Activos Críticos
  - ✓ Tangibles
  - ✓ Intangibles
  - ✓ Propios
  - ✓ Alquilados

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

IDENTIFICACIÓN DE ACTIVOS

- Trabajo de campo
- Operaciones
- Procedimientos
- RRHH
- Sistemas
- Sistemas electrónicos
- Registros

CÓMO ORGANIZAR LOS ACTIVOS PARA SU CONTROL

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

CONCEPTO DE RIESGO

“Es la Probabilidad y la posibilidad que un hecho suceda, sea éste positivo o negativo; por eso la actual norma ISO 31.000 de “Gestión de Riesgos Empresariales” habla de una incertidumbre entorno al logro de los objetivos de la organización.”

“El riesgo tiene su origen en eventos naturales, fortuitos, accidentales, dolosos.”

FUENTE DE RIESGO es el factor (tangible o intangible) con potencial de crear incertidumbre en la consecución de objetivos. Para que exista una fuente de riesgo, debe existir un peligro o amenaza activado a través de factores de riesgo o vulnerabilidades.

Las **VULNERABILIDADES** son los comportamientos y condiciones que se desvían de la norma (por ello denominamos comportamientos y condiciones sub-estándar); dinámicos y **VULNERABILIDADES** cuando se trata de riesgo puro.

Las **VULNERABILIDADES** son cualquier debilidad o práctica del negocio que puede ser explotada por el adversario que hace a un activo susceptible a daños causados por amenazas naturales o inadvertidas.

VULNERABILIDADES

Las vulnerabilidades se identifican:

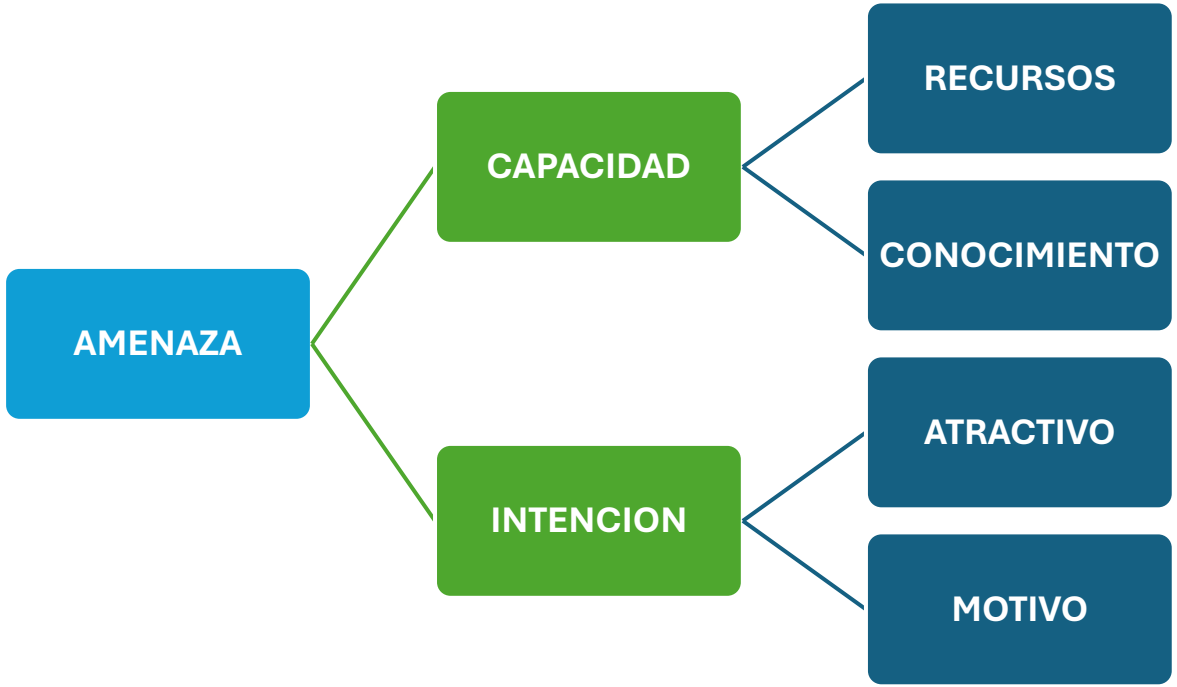
- Recopilando información de entrevistas con personas que trabajan en la instalación.
- Por observación / inspección del sitio.
- Por revisión de documentos.
- Por medio de pruebas diseñadas para destacar la vulnerabilidad y descubrir debilidades o fallas en el diseño o en el sistema, (hardware o electrónica)

"Sólo un análisis de riesgo identifica los activos críticos, determina las amenazas, vulnerabilidades y consecuencias de un evento los cuales determinan a su vez los objetivos de un sistema de Protección física."

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

Mientras el término **PELIGRO** hace referencia a una situación, la **AMENAZA** es un individuo o grupo de personas con elementos – de capacidad e intención – que lo clasifican para causar pérdida de los recursos.



Identificación de Amenazas

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

LA AMENAZA

- Una definición de amenaza para un lugar o empresa debe ser creada durante la evaluación de riesgo y se debe recolectar información específica sobre el adversario.

- Los adversarios pueden estar separados en tres clases: externos, insiders y externos coludidos con internos.

- Para cada clase de adversario se debe definir toda la gama de tácticas (el engaño, la fuerza, el sigilo o cualquier combinación de estas), para acceder a cualquier lugar dado en una empresa,

- El sistema de seguridad debe proteger los activos contra todas estas amenazas. ASIS define el diseño de base de amenazas (DBT, por sus siglas en inglés) como “El adversario contra el cual el elemento debe ser protegido” (Patterson, 2007).

- Determinar la DBT requiere considerar el tipo de amenaza, tácticas, modo de operación, capacidades, niveles de amenaza y la probabilidad de ocurrencia.

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

- La DBT incluye otras características de la amenaza que se debe considerar, tales como vehículos, armas, herramientas o explosivos, así como también la motivación de la amenaza.
- Es crucial que éstas características sean descritas en la DBT porque más tarde, durante la evaluación de vulnerabilidades (vulnerability assesment, VA, por sus siglas en inglés), ellas ayudaran a calibrar la efectividad de los componentes individuales del PPS, así como del sistema general.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

PRINCIPIOS Y CONCEPTOS DE DISEÑO.

- La motivación
- considerar el número de adversarios.
- Equipamiento
- identificacion de los adversarios
- Estimación del impacto de la amenaza
- la probabilidad que el adversario ataque

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

VÁNDALOS

Esta amenaza consiste en pequeños grupos de dos a cinco personas sin armas, cuya intención es dañar activos de la compañía de bajo valor o los vehículos de los empleados aparcados en el lugar. Los ataques son generalmente en la noche, pero también ocurren ataques durante el día.

Los vándalos pueden estar bajo la influencia del alcohol o drogas. Ellos pueden portar herramientas manuales básicas, tales como alicates, cortadores de alambre, destornilladores o martillos, así como latas de pintura en aerosol (spray), pistolas de pintura o similares. Ellos no cuentan con ayuda desde el interior (insiders). Ellos no están altamente motivados y huirán o se rendirán si perciben que pueden ser capturados.

EMPLEADO DESCONTENTO (INSIDER).

Generalmente esta amenaza provendrá de un individuo que actúa en solitario, pero también podría ser un pequeño grupo (dos a cinco personas).

La persona podría estar bajo la influencia del alcohol o drogas, ella o él podría ser mentalmente inestable.

La persona podría portar armas pequeñas, tales como pistola o cuchillo.

El deseo del empleado descontento es atacar a una persona en el lugar, como el administrador, su esposa, o causar daño al equipamiento. Si el objetivo es dañar el equipamiento, la persona puede portar herramientas pequeñas, pero probablemente utilizará herramientas o controles que están presentes en el lugar.

La persona está altamente motivada y no espera ser sorprendida durante el acto, puesto que la persona tiene acceso autorizado.

CRIMINALES.

Pueden ser de una a cinco personas cuyo objetivo es robar objetos de valor de, o en la instalación; su objetivo es obtener beneficios financieros de la venta de los ítems robados.

Portarán herramientas manuales o eléctricas para ingresar al sitio o acceder al activo, y planificarán cuidadosamente su ataque. Podrían portar armas pequeñas, pero es poco probable que las utilicen. Ellos podrían tener ayuda del interior (insiders) y detendrán el ataque si son detectados.

EXTREMISTAS.

Esta amenaza consiste en un grupos de personas medianos a grandes (20 y más) cuyo objetivo es atraer atención sobre una práctica en el blanco escogido. Su motivación es ideológica; podrían ser ambientalistas, grupos proderecho animal, anti o proaborto, o accionistas. Ellos no son violentos, pero se podrían resistir a ser desalojados del sitio e ignoraran órdenes verbales para que se retiren.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

El **RIESGO PURO** o **RIESGO DE SEGURIDAD** se define como la **PROBABILIDAD** de que una amenaza tome ventaja de las vulnerabilidades del recurso y esto cause un **IMPACTO** (consecuencia negativa o pérdida).

El impacto puede ser estimado de manera cualitativa (**SEVERIDAD**) o cuantificado por ejemplo en términos monetarios (**CRITICIDAD**).

		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

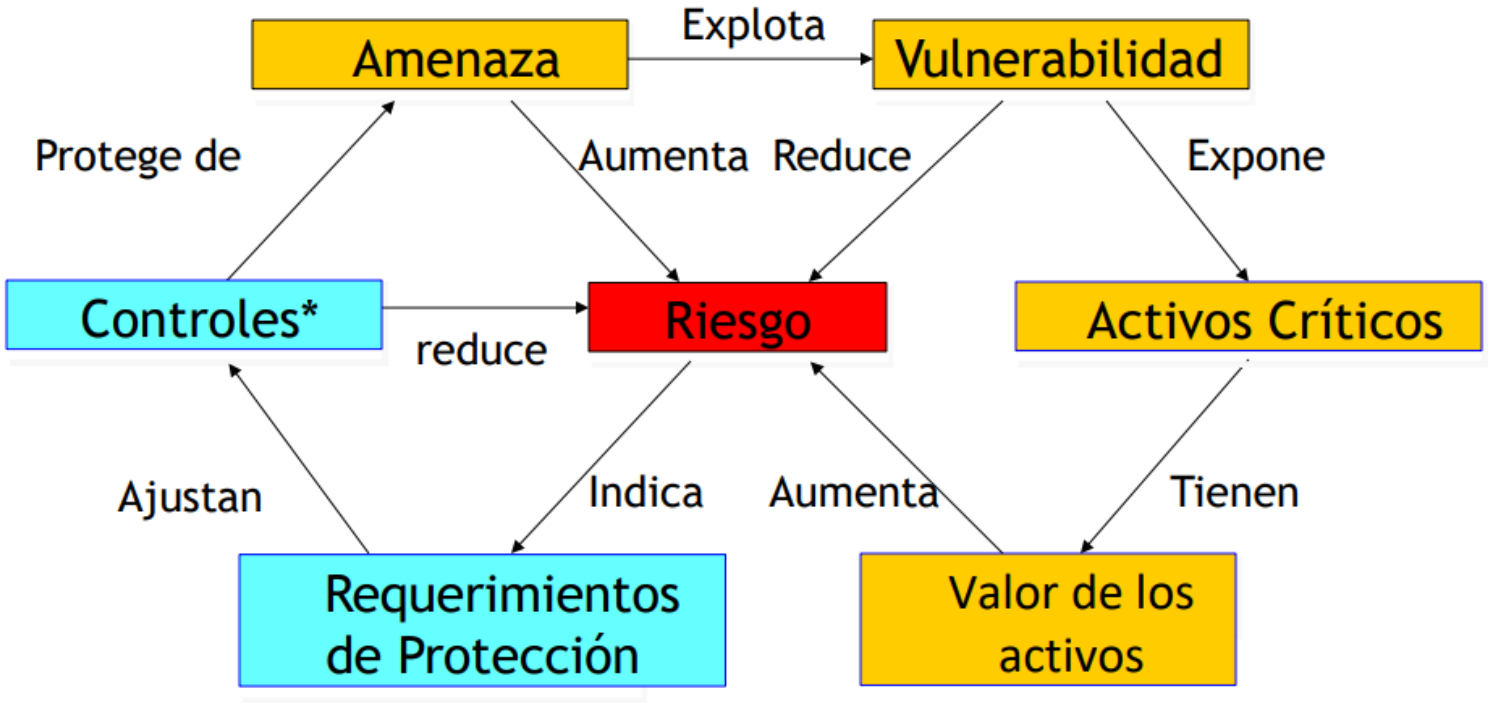
IMPACTO O CONSECUENCIAS:

- Resultado de un suceso que afecta a los objetivos de la organización.
- Es la consecuencia de un resultado en particular.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

RELACIÓN RIESGO, AMENAZAS, VULNERABILIDADES, PÉRDIDA



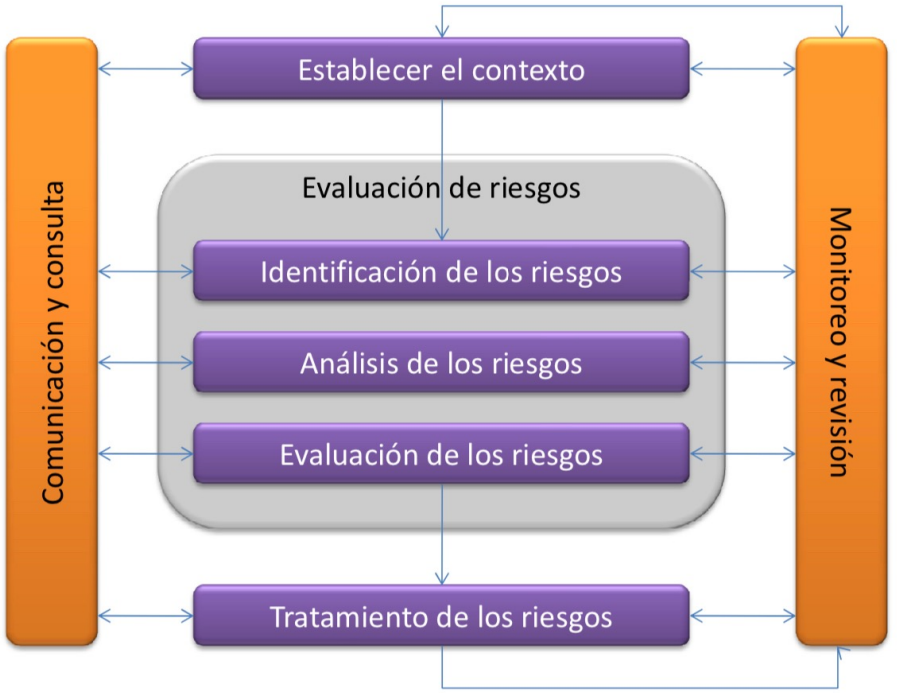
**Controles: Una práctica, procedimiento o mecanismo que reduce el riesgo.*

Fuente: ISO/IEC TR 13335

EL PROCESO DE LA GESTIÓN DE RIESGOS

El proceso usado por ASIS Internacional e IFPO para gestionar los riesgos puros sigue un ciclo de cinco pasos interrelacionados en un ciclo continuo y va de la mano de la norma internacional ISO 31.000.

1. Identificar
2. Evaluar
3. Decidir
4. Comunicar
5. Implementar
6. Supervisar



Paso 1: IDENTIFICAR: Mediante un estudio de seguridad se asocian los recursos con sus fuentes de riesgo:

Identificar pasos en la operación, **recursos** críticos a proteger y sus características.

Determinar las **amenazas** (las personas o situaciones que podrían generar pérdidas) y **vulnerabilidades** (comportamientos y condiciones) de los recursos.

Definir los posibles eventos de **pérdida.**

Paso 2: EVALUAR: Una vez establecido el perfil del evento de pérdida, se realiza el **análisis** y **evaluación** de riegos.

Asignar a una de las siete **categorías** de pérdida.

Estimar la **probabilidad** de ocurrencia del evento y el **impacto** de cada evento de pérdida.

Los riesgos se comparan contra **estándares**, y entro ellos usando el RAC para priorizarlos.

Paso 3: DECIDIR: Se toman decisiones a dos niveles:

Priorizar, empezando con riesgo más serio.

Escoger estrategia para **tratar** los riesgos.

Se seleccionan operativamente las **medidas de control de pérdidas** para reducir el impacto o la probabilidad.

Paso 4: COMUNICAR: Reportar o consultar de manera continua permanente a partes interesadas.

Reportar el resultado de análisis.

Consultar a partes interesadas.

Comunicar los acuerdos logrados.

Paso 5: IMPLEMENTAR: Se ejecutan las **medidas de control.**

Métodos (políticas, procedimientos, instrucciones).

Tecnología (ingeniería, seguridad física y EPP).

Control mediante **personal**.

Paso 6: SUPERVISAR: Los resultados deben generar mejoras y retroalimentar el proceso:

Evaluar **ejecución** del plan de implementación.

Verificar la **efectividad** de contramedidas.

Seguimiento de actos y condiciones y cambios en el escenario.

PASOS PARA LA ADMINISTRACION DE RIESGOS DE SEGURIDAD

TRATAMIENTOS DE RIESGOS

Los riesgos deben ser gestionados cuidadosamente y preferiblemente antes de que se produzcan pérdidas. En ASIS Internacional e IFPO se utilizan cuatro métodos para tratar los riegos de acuerdo al acrónimo formado por las siglas **ETOA**, las opciones estratégicas frente a los riesgo son:

E – Evitar los riesgos: Evitar completamente los riesgos, cambiando las actividades o trasplantando el bien a otros escenario o lugar más favorable. Eliminar la fuente de riesgo o influir en ella es generalmente la única opción cuando el recurso es muy difícil de proteger.

T – Transferir los riesgos: Compartiendo el impacto de las pérdidas. El seguro, la asociación financiera o la subcontratación son maneras usuales de transferir el riesgo.

O – Optimizar los riesgos: Aprovechando el riesgo en busca de oportunidades, adaptando parámetros internos o externos a través de medidas de control de pérdidas para controlar: 1.Exposicion al peligro (por ejemplo separando o distribuyendo los recursos a proteger) 2, Vulnerabilidades; o 3. Consecuencias.

A – Aceptar los riesgos: Decisión informada de aceptar el riesgo cuando éste está dentro de límites tolerables (riesgo tolerable).

CONTROL DE PÉRDIDAS

La ciencia de protección contemporánea pone énfasis en el control de pérdidas como forma de optimizar los riesgos de las organizaciones. Según la teoría WAECUP – teoría del Control de Pérdidas – desarrollada por Bottom y Kostanoski en un libro Proteccion y Control de Pérdidas (MacMillan 1938) las pérdidas pueden tener muchos orígenes diferentes.

P	Practicas no profesionales/no éticas, fraudes ocultación, discriminación, conflictos de interés entre otros.
E	Error en la planeación o ejecución.
R	Robos y comportamientos criminales.
D	Desperdicio y desorden de recursos, tiempos, materiales, mano de obra y espacio.
I	Incidentes y desviaciones de norma que aparentemente no han causado daño.
D	Desastres naturales e intencionales, incluye sabotaje.
A	Accidentes y enfermedades profesionales.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

Las pérdidas cuestan grandes cantidades de dinero, por sus costos directos, así como por sus consecuencias indirectas. Debemos notar que por este motivo existen medidas de control que las organizaciones deben cumplir (a veces inclusive de manera redundante), para controlar pérdidas y asegurar que no se vuelvan a repetir.

A nivel operativo, para asegurar la protección integral siempre deben incluir los tres tipos de medidas de control:

1. Métodos (Crear y modificar políticas, procedimientos e instrucciones)
2. Tecnología (Crear y modificar herramientas físicas y sistemas electrónicos)
3. Personas (Incluir oficial de protección y modificar comportamiento)

Curso Jefes de Seguridad Privada

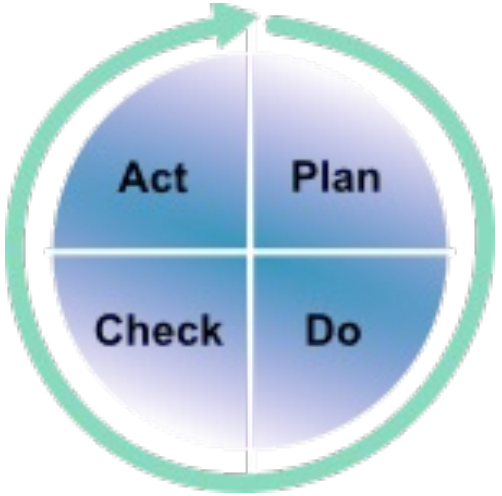
Módulo 1. Control de riesgos empresariales de seguridad.

El programa de control de pérdidas es un ciclo de mejora continua que debe adaptarse a los procesos perceptuales humanos y de mejora continua organizacional cumpliendo las funciones de:

1. Planear 2. Hacer 3. Verificar y 4. Actuar frente a eventos intencionales o accidentales que pueden generar pérdidas a los recursos que protegemos.

Equiparando la mejora continua utilizada en todos los sistemas de gestión al ciclo del control de pérdidas; la fase **PLANEAR** incluye actividades relacionadas con la Apreciación de Riesgos ejecutadas en el Antes:

- Investigar el contexto
- Identificar potenciales eventos de de PERDIDA (proceso de gestión de riego)
- Integrar Medidas de Control
- Instruir a las personas



La fase **Hacer** implica actividades operativas de **Mitigación** de Riesgos ejecutadas por métodos, tecnología y personal en el Durante:

- **D**isuadir potenciales agresores.
- **D**emorar ataques efectivos.
- **D**etectar ataques efectivos.
- **D**etener a los agresores.

La fase **VERIFICAR** involucra actividades de **Control Operacional** de RIESGOS ejecutadas por el equipo de supervisión en el durante:

- **S**imulas eventos de pérdida
- **I**nspeccionar condiciones.
- **O**bservar comportamientos.
- **A**uditar procesos.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

La fase **ACTUAR** ejecuta actividades de **Resiliencia** frente a la materialización de riesgos y mide la capacidad de aprender, se establece en el Después:

- **R**eaccionar inicialmente.
- **R**eportar lo sucedido.
- **R**ecuperar recursos.
- **R**einiciar operaciones.

OTROS CONCEPTOS CLAVES

Todo oficial de protección debe comprender varios conceptos que son claves para su adecuado desempeño en el día a día de sus actividades, algunos de ellos los mencionaremos

DELEGACION DE AUTORIDAD

Un superior delega autoridad a sus ordinarios para repartir la carga de trabajo. Un superior puede delegar autoridad pero la persona debe aceptar su parte de la responsabilidad y recibir las herramientas para cumplir la misión encomendada. La responsabilidad no puede ser delegada totalmente, inclusive en ciertos casos es recomendable la administración por excepción.

ADMINISTRACION POR EXCEPCIÓN

Cuando existen situaciones de emergencias o delicadas, es recomendable que sea el superior inmediato que asuma nuevamente el control.

CADENA DE MANDO

Las comunicaciones deben ir hacia arriba y hacia abajo y horizontalmente, pero siempre a través de una jerarquía organizada con el propósito de lograr eficiencia y orden; Un oficial de protección debe tener cuidado de nunca romper esta cadena porque afectara la unidad de mando.

UNIDAD DE MANDO

Para evitar confusión durante un esfuerzo organizativo, ningún subordinado debe reportar o seguir órdenes de más de un superior.

EXTENSIÓN DEL CONTROL

Es el número de subordinados que un superior puede supervisar adecuadamente. Este número depende del nivel de detalle en el trabajo realizado; siendo recomendada la relación 1:3 para trabajos de alta responsabilidad y 1:12 en el caso de trabajos operativos y rutinarios.

CONCLUSION

Como Jefes de Seguridad debemos estar familiarizados con los conceptos y estándares de la profesión; esta es la diferencia entre el empirismo y la verdadera profesionalización.

El control de perdidas consiste en establecer un entorno que refuerce el cumplimiento de restricciones, para a través de la modificación de amenazas y vulnerabilidades, poder influir en la disminución de probabilidades e impacto de pérdidas.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

¿Es seguro un Sistema? No tiene sentido.

Lo que debería preguntarse el jefe de seguridad es…

¿Está el sistema protegido contra eventos dañinos?
(Broder, 1984).

PROGRAMA DE MANEJO OPERATIVO DE RIESGOS (MOR)

Una herramienta que los gerentes de protección, así como todos los demás oficiales en el departamento de protección pueden usar para –en la práctica – controlar pérdidas o minimizar riesgos, es instituir un programa de Manejo Operativo de Riesgos (MOR) en la organización.

En su forma más elemental, un proceso MOR producirá protección en todos los lugares y niveles (operativo, táctico y estratégico) contestando tres preguntas acerca de cualquier evento, obvio o potencial:

- ¿Qué puede dañarme a mí o a mi organización?
- ¿Cuánto daño puede hacerme a mi o a mi organización?
- ¿Qué puedo hacer acerca de esto?

El programa MOR original fue desarrollo por la Armada de los EE.UU en 1989 y fue adoptado por la US Navy y otras ramas de servicios del Departamento de Defensa poco después. El MOR es un proceso de toma de decisiones en cinco etapas que es diseñado para habilitar a los individuos a identificar peligrosos, evaluar riesgos e implementar controles para reducir es riesgo asociado con cualquier acción u operación.

El proceso MOR subsiste en tres niveles: **Inmediato** (una revisión oral o mental “algo rápido”); **deliberado** (aplicación del proceso de cinco pasos para gestionar los riesgos), y **en profundidad** (un proceso estratégico con una evaluación más completa de riesgo involucrando investigación de los datos disponibles, usos de diagramas, herramientas cuantitativas de análisis y pruebas formales o seguimiento de largo alcance de las fuentes de riesgo asociados con la operación).

El MOR incorpora los cuatro principios de:

1.- Aceptar el riesgo cuando los beneficios pesan más que el costo.
2.- No aceptar riesgos innecesarios.
3.- Anticipar y manejar riesgos planificadamente.
4.- Hacer decisiones de riesgo al nivel apropiado en la organización.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

Mientras el MOR tradicional fue originalmente desarrollado y usado en planeamiento y operaciones militares, es igual de efectivo cuando se utiliza en operaciones de protección cotidianas.

El MOR no tiene que ser complejo para ser efectivo, de hecho, la implementación de un MOR en un nivel básico dentro de organizaciones es la clave de un programa MOR exitoso. Como la mayoría de los sistemas, el MOR utiliza “herramientas” como parte del proceso. Estas herramientas incluyen una matriz de evaluación de riesgos, categorías de impacto de perdidas, la probabilidad de pérdidas y el uso de códigos de evaluación de riesgos.

Aumento de la probabilidad	Aumento de la severidad 1	2	3
1	Bajo -1-	Bajo -2-	Medio -3-
2	Bajo -2-	Medio -4-	Alto -6-
3	Medio -3-	Alto -6-	Alto -9-

MATRIZ DE EVALUACIÓN DE RIESGO

La matriz de Evaluación de Riesgos del MOR, es usada para evidenciar el cumplimiento del proceso, una vez identificación los riesgos. Usar la matriz MOR para cuantificar y priorizar el riesgos no disminuye la naturaleza inherentemente subjetiva de la evolución del riesgo. Sin embargo, la matriz MOR provee un marco consistente para ser usado por varias aplicaciones, cualquier herramienta de evaluación del riesgo debería incluir los elementos del impacto de la pérdida y la probabilidad de la misma.

IMPACTO DE PÉRDIDA, es una medición de la peor consecuencia creíble que puede ocurrir como resultado de un incidente. El impacto es definido por un grado de daño potencial, enfermedad, daño a la propiedad, pérdida de recursos (tiempo, dinero y personal) o potencial para afectar una misión. La combinación de dos o más incidentes puede incrementar el nivel global de riesgo. Los niveles de impacto de pérdida son asignadas como números romanos de acuerdo con el siguiente criterio:

I EXTREMO – El incidente puede causar muerte, pérdida de una instalación/ recursos o resultado es un daño grave.
II ALTO – El acontecimiento puede causar daño severo, enfermedad, daño a la propiedad o degradación al uso eficiente de recursos.
III MEDIO- La eventualidad puede causar daño menor, daño a la propiedad o degradación al uso eficiente de recursos.
IV COMÚN – El incidente presenta una amenaza mínima a la protección personal o a la salud, propiedad o uso eficiente de recursos, poblaciones afectadas, experiencias o información estadística previamente establecida.

PROBABILIDAD DE PÉRDIDA es un grado de lo probable de que un evento ocurra. Al nivel de probabilidad se le asigna una letra de acuerdo con los siguientes criterios:

A INMINENTE – Ocurrencia inmediata o dentro de un corto periodo de tiempo. Se espera que ocurra algunas veces un objeto individual o persona, o frecuentemente a un grupo u organización.

B PROBABLE – Probablemente ocurrirá. Se espera que ocurra alguna vez a un objeto individual o persona, o algunas veces a una organización.

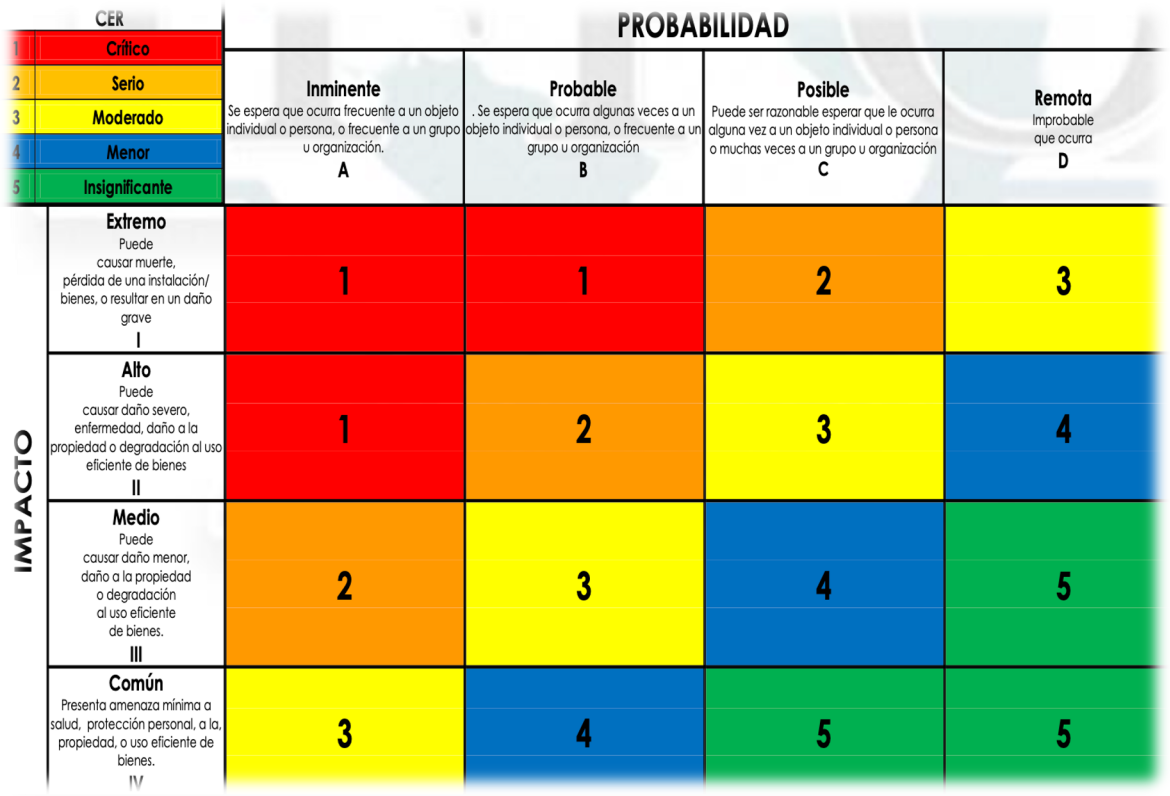
C POSIBLE – Puede ocurrir en el tiempo. Puede ser razonablemente esperado que le ocurra alguna vez a un grupo u organización.

D RETOMA – Improbable que ocurra.

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.



CER		PROBABILIDAD			
		Inminente Se espera que ocurra frecuente a un objeto individual o persona, o frecuente a un grupo u organización. A	**Probable** . Se espera que ocurra algunas veces a un objeto individual o persona, o frecuente a un grupo u organización B	**Posible** Puede ser razonable esperar que le ocurra alguna vez a un objeto individual o persona o muchas veces a un grupo u organización C	**Remota** Improbable que ocurra D
1	Crítico				
2	Serio				
3	Moderado				
4	Menor				
5	Insignificante				
IMPACTO	**Extremo** Puede causar muerte, pérdida de una instalación/ bienes, o resultar en un daño grave I	1	1	2	3
	Alto Puede causar daño severo, enfermedad, daño a la propiedad o degradación al uso eficiente de bienes II	1	2	3	4
	Medio Puede causar daño menor, daño a la propiedad o degradación al uso eficiente de bienes. III	2	3	4	5
	Común Presenta amenaza mínima a salud, protección personal, a la, propiedad, o uso eficiente de bienes. IV	3	4	5	5

El Código de Evaluación de Riesgo (CER), (Risk Assesment Code – RAC en Inglés), es usado para definir el grado de riesgo asociado con impacto y probabilidad del evento.

El CER se deriva de la matriz MOR:

1. Riesgo Crítico.
2. Riesgo Serio.
3. Riesgo Moderado.
4. Riesgo Menor.
5. Riesgo Insignificante.

Fase 1: IDENTIFICAR Mediante un estudio de seguridad se asocian los recursos con sus fuentes de riesgo:

- Identificar pasos en la operación, recursos críticos a proteger y sus características.
- Determinar las amenazas (las personas o situaciones que podrían generar pérdidas) y vulnerabilidades (comportamientos y condiciones) de los recursos.
- Definir los posibles eventos de pérdidas.

Fase 2: EVALUAR

Una vez establecido el perfil del evento de perdida, se realiza el análisis y evaluación de riesgos:

- Asignar a una de las siete categorías de pérdida.
- Estimar la probabilidad de ocurrencia del evento y el impacto de cada evento de pérdida.
- Los riesgos se comparan contra estándares, y entre ellos usando el RAC para priorizarlos.

Fase 3: DECIDIR Se toman decisiones a dos niveles:

- Priorizar, empezando con riesgos más serio.
- Escoger estrategia para tratar los riesgos.
- Se seleccionan operativamente las medidas de control de pérdidas para reducir el impacto o la probabilidad.

Fase 4: COMUNICAR : Reportar y consultar de manera continua permanente a partes interesadas.

- Reportar el resultado del análisis.
- Consultar a partes interesadas.
- Comunicar los acuerdos logrados.

Fase 5: IMPLEMETAR : Se ejecutan las medidas de control.

- Métodos (políticas, procedimientos, instrucciones).
- Tecnología (ingeniaría, seguridad física y EPP).
- Control mediante personal.

Fase 6: SUPERVISAR: Los resultados deben generar mejoras y retroalimentar el proceso:

- Evaluar ejecución del plan de implementación.
- Verificar la efectividad de contramedidas.
- Seguimiento de actos y condiciones y cambios en el escenario.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

MOR Y MODELO ARES

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

El modelo para Administración de Riesgos Empresariales de Seguridad (ARES), integra las herramientas MOR a tres niveles: operativo, táctico y estratégico con los pasos de la gestión de riesgos.

NIVEL OPERATIVO

A nivel **OPERATIVO**, los usuarios y los oficiales de protección física a nivel básico (PSO) se enfocan en:

- **Identificar** continuamente amenazas y vulnerabilidades (comportamientos y condiciones fuera de estándar) que pueden generar perdida. Además de identificar potenciales eventos de pérdida.

- **Comunicar** esos comportamientos y condiciones a supervisores, inspectores, observadores y auditores.

- **Implementar** la corrección de comportamientos y condiciones de acuerdo a lo establecido en procedimientos y sus órdenes de puesto.

NIVEL TÁCTICO

En el nivel **TÁCTICO**, los supervisores de seguridad realizan el proceso completo de seis fases:

- Identificar vulnerabilidades de su área de responsabilidad – por si mismos -, o validando y retroalimentándose de las identificadas por el nivel operativo. Al relacionarlas con amenazas, determinar potenciales eventos y su categoría de riesgo de pérdida, completando así las actividades de apreciación.

- Evaluar estimando probabilidad e impacto utilizando la matriz MOR cualitativa, para de acuerdo al CER priorizar los riesgos.

- Decidir la mezcla de controles apropiada guiándose por matrices de métodos, tecnología y personas (MTP), aplicando CPTED a las actividades operativas de Mitigación (4D).

NIVEL TÁCTICO

- Comunicar utilizando la matriz MOR cualitativa para que todas las partes interesadas sean conscientes de los potenciales eventos de pérdida, desarrollen competencia necesaria, mantengan el compromiso para cumplir las restricciones en comportamientos y condiciones, y de actuar en caso se materialicen los riesgos.

- Implementar los controles MTP, dirigiendo al nivel operativo transformándolos en restricciones específicas de actos y condiciones.

- Supervisar la ejecución de los controles a través de actividades de simulación, inspección, observación y auditoría (control operacional).

NIVEL ESTRATÉGICO

Al nivel **ESTRATÉGICO**, los gerentes y supervisores de protección (CSSM) manejan procesos cuantitativos, cumpliendo las funciones de:

- Identificar objetivos organizaciones, priorizarlos y relacionarlos con los recursos críticos. Caracterizar amenazas y vulnerabilidades asociándolas a esos recursos críticos.

- Evaluar midiendo probabilidad e impacto y la severidad en la matriz MOR cuantitativa, misma que puede alimentarse de la matriz MOR cualitativa del nivel táctico.

- Decidir la estrategia a tomar para controlar riesgos, basándose en datos y guiándose por la matriz de estrategias de riesgo (ETOA), esto redirige los esfuerzos tácticos expresados en la matriz MTP.

NIVEL ESTRATÉGICO

- Comunicar los efectos medidos en cambio de criticalidad a los objetivos y recursos, valorando las pérdidas evitadas y justificando finalmente las inversiones en protección y seguridad.

- Implementar las estratégicas y controles afectados de manera mensurable la caracterización de amenazas y vulnerabilidades.

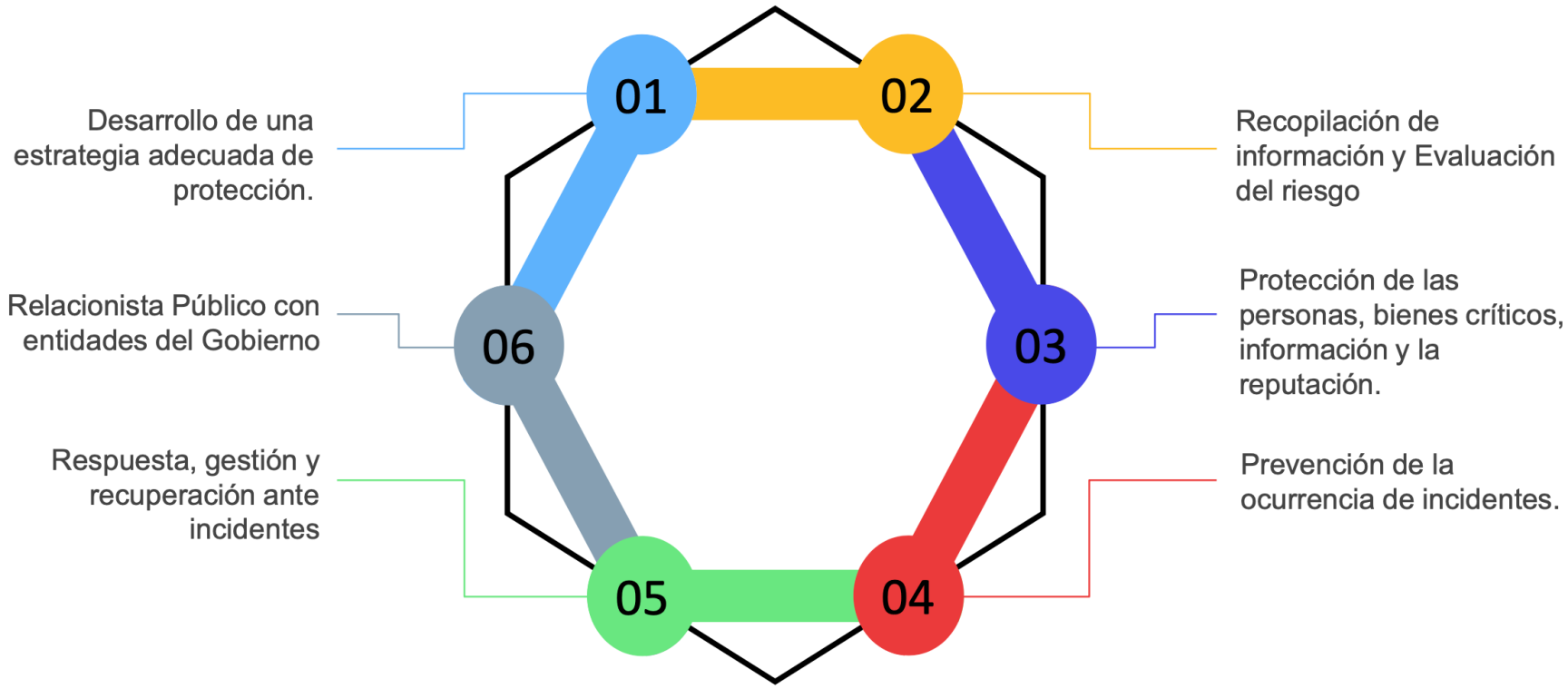
- Supervisar de manera mensurable el efecto en probabilidad e impacto, retroalimentándose con las actividades de control operacional de nivel táctico. Esos resultados se pueden transformar fácilmente en comunicación a todos los niveles a través de la matriz MOR cualitativa.

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

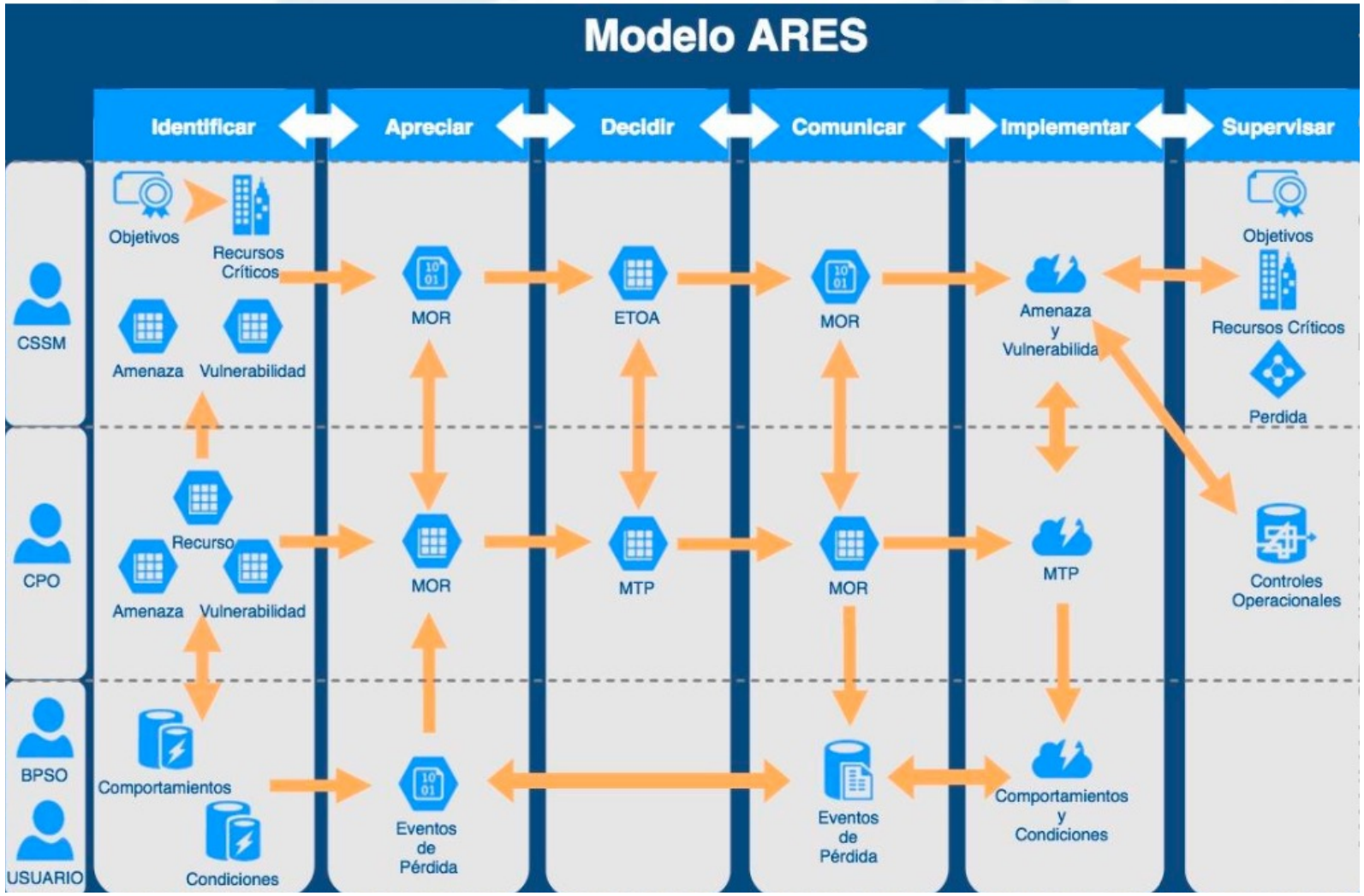
NIVEL ESTRATÉGICO



OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.



Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

LINEAS DE AUTORIDAD	RESPONSABILIDAD	ESTRUCTURA ORGANIZACIONAL	COMUNICACIÓN
•Las líneas de autoridad, responsabilidad y comunicaciones deben ser lo mas clara posibles	•La responsabilidad individual y organizacional debe venir con un nivel apropiado de autoridad	•Deberían considerar su interrelación entre funciones, roles y responsabilidades: MISIÓN.	•Canales abiertos y estructurados para el cumplimiento de la MISIÓN

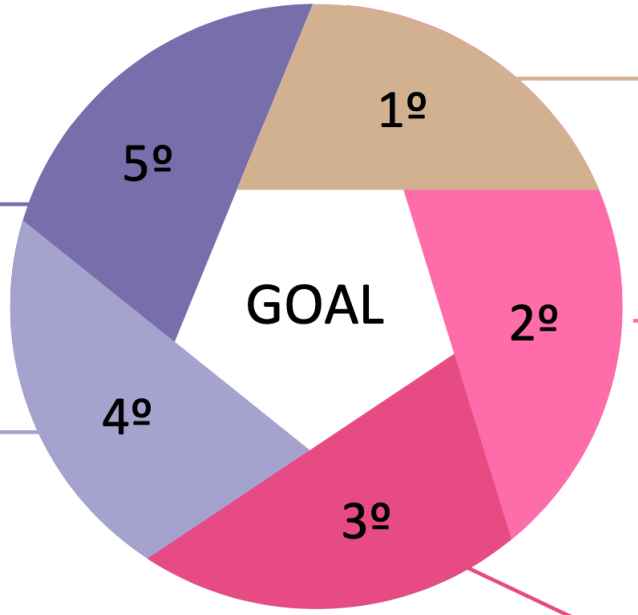
Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

POTENCIADORES DE LA PROTECCION DE ACTIVOS



Consideración de riesgos y amenazas globales.
Consideración del departamento de Seguridad y responsables.
Requerimiento de preparación y educación

SEGURIDADNACIONAL / ENTORNO DE SEGURIDAD INTERNACIONAL

CONVERGENCIADE LAS SOLUCIONES DE SEGURIDAD

Seguridad tradicional con Seguridad IT.
Convergencia de disciplinas, técnicas y herramientas para protección de activos.
Activos: información e intangibles.
La protección es complicada.

GLOBALIZACION EN LOS NEGOCIOS

Pone un amplia gama de vendedores, mercancías, etc. al alcance de las empresas.
Acerca las amenazas / incrementa las vulnerabilidades.
Se incrementan riesgos sobre transacciones comerciales, activos de información, responsabilidad civil, etc.

ESTANDARES Y REGLAMENTACIÓN

Estándares voluntarios, obligatorios o mixtos:
•ISO, ANSI. Reglamentos
Códigos de SSO, SART / OSHAS.
Certificaciones profesionales y licencias:
ASIS, IFPO, IT, CPTED.

TECNOLOGÍA Y TACTO

Buscamos la solución mas rápida.
Tememos y adoramos la tecnología
Confusión: real / aparente.
Aceptación de violencia como normal.
Amamos la tecnología como un juguete.
Distanciamiento y distracción

CONCLUSION

Un programa de Manejo Operativo de Riesgos es una parte esencial en un proceso de administración de riesgos empresariales de seguridad.

El éxito de este programa DEPENDE de que todos en la organización piensen en función de riesgos:

- Debe ser implementado y mantenido por todo el personal, no solo de protección.
- El programa, conceptos y aplicación deben ser entrenados inicial y periódicamente para involucrar a todo el personal.
- El programa debe ser evaluado paródicamente para asegurar la validez en marcha del programa y asegurar cumpliendo de los objetivos, políticas y procedimientos organizacionales.

ORIGEN DEL MODELO ARES

El modelo para la Administración de Riesgos Empresariales de Seguridad (ARES) fue desarrollado inicialmente en el año 2008 como una tesis de postgrado, y actualizada constantemente para IFPO Hispanoamérica. A demás de definir el camino para implementar operacionalmente el Enterprise Segurity Risk Management (ESRM) por sus siglas en inglés; busca integrar la protección de Personas, Información, Propiedades, Imagen y Entorno a modelos ya existentes (o inclusive ya implantados) de Calidad, Seguridad, Protección, Salud y Ambiente (QSSHE).

Sigue un acercamiento estratégico – táctico – operativo basado en coaching de seguridad; integra conceptos de planeación estratégica, teoría de procesos, sistema de gestión de calidad, indicadores de gestión, continuidad de negocio, control interno y neuro lingüística; busca cumplir con las expectativas de todas las partes interesadas “stakeholders”, quienes normalmente desean entender el espectro de los riesgos que enfrentan las complejas organizaciones de hoy en día para asegurarse que estén adecuadamente administradas.

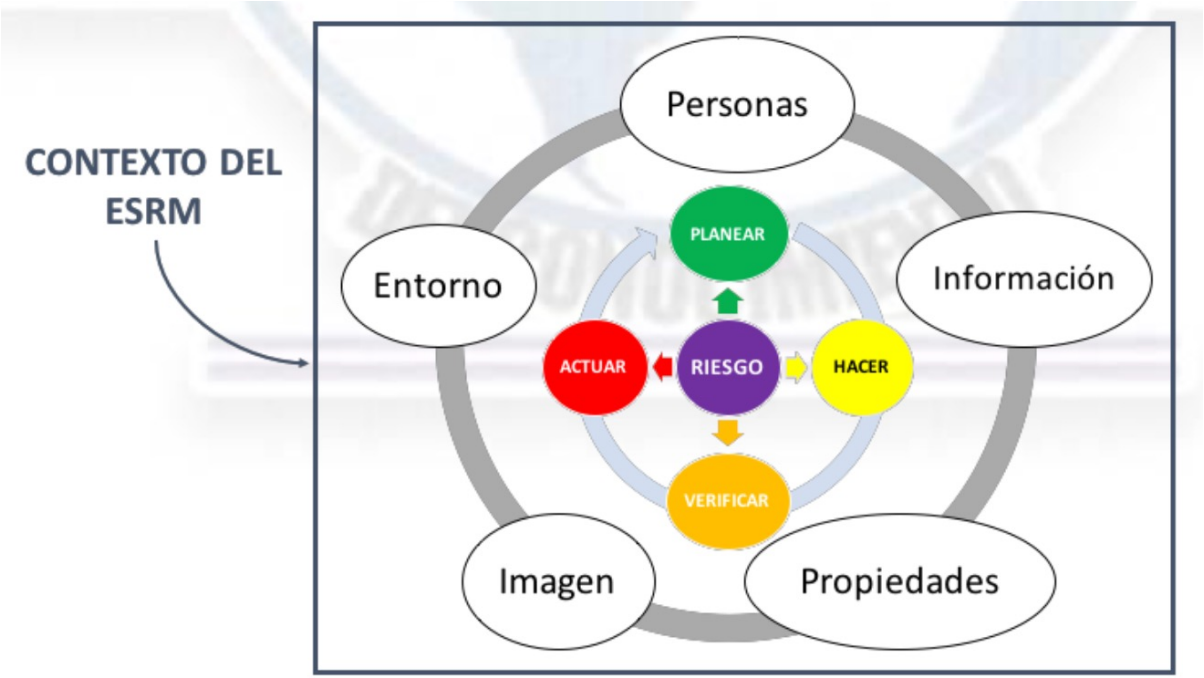
ORIGEN DEL MODELO ARES

Entender las interdependencias entre los riesgos (cuando se materializa el riesgo en un área de la empresa, puede incrementar el impacto de los riesgos en otra área de la organización), por consecuencia la acción de mitigar el riesgo se vuelve más efectiva y puede dirigirse a abarcar múltiples sectores de los negocios generando ahorros.

La propuesta del Modelo ARES es doble; por un lado define un lenguaje común entre las diversas partes preocupadas por los riesgos organizacionales, y luego genera alineamiento estratégico. Esto es importante, ya que no administrar adecuadamente los diferentes tipos de riesgos puede poner en peligro todos los objetivos de la organización (incluyendo sus objetivos primarios).

CARACTERÍSTICAS FUNDAMENTALES

El modelo ARES se orienta a administrar el contexto de control que puede afectar a las organizaciones; es un marco que contempla las etapas de mejora continua (planear – hacer – verificar - actuar) alrededor de la gestión (optimización y no simplemente reducción) de todo tipo de riesgos de su seis fases bajo la concepción de un modelo integrado, integral, multidisciplinario y participativo.



INTEGRADO: Busca como principio fundamental alinearse a los objetivos organizacionales, integrándose a la razón de ser la organización. ARES va a contribuir al logro de objetivos (inclusive puede ayudar a ganar dinero, el proceso de "pensar en riesgos" no debe inmovilizar la acción ni la dinámica organizacional, sino lo contrario.

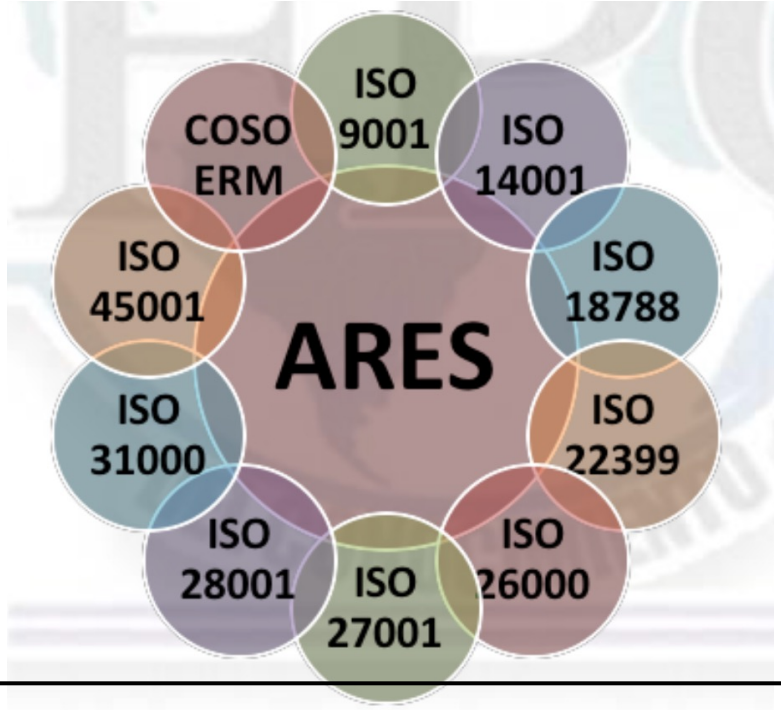
La planificación de la actividad preventiva – mitigadora y recuperadora no debe ser considerada como una actuación de aislada e independiente del resto de las funciones de la organización. Se podría decir que el sentido que tiene la mencionada integración es la administración de riesgos deberá estar incluida tanto en los propios procesos técnicos, como en la propia organización del trabajo y las condiciones en que este se preste, así como en la línea jerárquica de la organización, incluidos todos los niveles de la misma.

La administración de los riesgos empresariales no es un proyecto, un producto o una acción que se realiza por una sola vez (o pero aún por consultores externos a la organización); sino que debe suponer un proceso continuo o constante que debe realizarse día a día en la propia organización, modificándose al mismo ritmo en que se modifican sus situaciones diarias.

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

INTEGRAL: Enfoca sus esfuerzos en procesos organizados para proteger personas, información, propiedades e imagen. ARES resume y acoge todas las mejores prácticas, requerimientos legales y normas aplicables.



MULTIDISCIPLINARIO: Se fundamenta en las técnicas de las ciencias administrativas, estadísticas, seguridad física, seguridad y salud ocupacional, medicina del trabajo, protección del ambiente. Otros aspecto a tener en cuenta es que se definen claros roles. En un mundo de incertidumbres crecientes la figura del director de riesgos organizacional (Chief Risk Officer – CRO), que es el coordinador de los esfuerzos de los diversos gestores de riesgos de la organización, resuelta ya, una necesidad.

PARTICIPATIVO: La administración de riesgos es tarea de todos; busca una actitud participativa a nivel general. ARES se fundamente en liderazgo de la dirección, pero la filosofía a adoptar ante los riesgos debe traducirse en políticas que sean entendidas y aplicadas por todo el personal.

La acción preventiva no debe descansar única y exclusivamente sobre los trabajadores designados por la organización para realizar procesos auxiliares, sino que debe convertirse en un proceso básico y ser llevada a cabo por todos y cada uno de los trabajadores de la organización, durante todas las actividades de su trabajo habitual.

La realización por parte de todos los trabajadores de la organización de las actividades preventivas supondrá que por parte de la empresa se deban definir y asignar unas determinadas funciones y responsabilidades a todos y cada uno de los trabajadores de la organización con independencia de cuál sea su nivel jerárquico o categoría profesional.

Se ha de ser consciente de que las acciones formativas y comunicativas no son hechos aislados, sino que dependen numerosos factores empresariales que, aunque impalpables son muy reales; uno de los más importantes es la creación de una “cultura de seguridad” que asegure:

a) Participación y un compromiso a todos niveles.
b) Una comunicación eficaz que motive a los trabajadores a desarrollar su función con seguridad.
c) Promoción de aptitudes para una contribución responsable.
d) Un liderazgo visible y activo de la dirección para desarrollar y mantener el apoyo a una cultura de seguridad que sea el denominador común compartido por todos los componentes de la organización.

La concienciación del empleado por la seguridad es el principal objetivo a conseguir, para esto se crea un sistema de gestión incidencias que recoge notificaciones continuas por parte de los usuarios (todo incidente de seguridad debe ser reportado y analizando). En vez de dedicar el tiempo de una persona entre cien, tener una centésima parte del tiempo de cada persona enfocado en seguridad.

EQUILIBRADO: Debe entenderse el bien a proteger como algo complejo que posee muchas características, casi ilimitadas como las caras de una esfera; la protección a ese bien debe visualizarse entonces como una esfera que cubre a la primera de manera equilibrada.

Es importante siempre recordar la prioridad de lo que vamos a proteger:

a) Personas
b) Información
c) Propiedades
d) Imagen
e) Entorno

BASADO EN RIESGOS REALES: Muchas veces los esfuerzos de seguridad son incompletos, no coordinados, o su diseño está basado en presunciones erróneas.

Los riesgos varían en importancia relativa e impacto económico a lo largo del tiempo, siendo principios fundamentales:

- Entender clara y actualizadamente los riesgos y como cambian a lo largo del tiempo;
- Anticipar accidentes, enfermedades, tácticas y tendencias criminales para poder prevenirlas; y
- Adaptar el programa de protección continuamente.

El modelo general se implementa en las cuatro fases de mejora, aplicando cuatro acciones principales en cada fase:

Planear – Prevenir

- INVESTIGAR: Entender Misión, Visión, Objetivos de Seguridad, Órdenes de Puesto.
- IDENTIFICAR: Indicadores de Sospecha, Amenazas, Actos y Condiciones esperados.
- INTEGRAR: Métodos, tecnología y Personal de Seguridad.
- INSTRUIR: ¿Todos sabemos que hacer?

Hacer – Mitigar

- DISUADIR: Mediante un entorno de control y presencia de Agente de Control
- DETECTAR: Actos, Condiciones, Sospechosos, Pérdidas
- DEMORAR: Determinar Amenaza, Iniciar respuesta
- DETENER: Uso apropiado y progresivo de la Fuerza

Verificar – Supervisar

- INSPECCIÓN: Verificar Condiciones fuera de lo esperado
- OBSERVACION: Verificar Actos fuera de lo esperado
- SIMULACROS: ¿Qué pasaría si… Estamos listos?
- AUDITORIAS: Pruebas de penetración

Actuar – Responder

- REACCIONAR: Actuar de acuerdo al plan establecido
- REPORTAR: Reportar a los niveles apropiados
- RECUPERAR: Retomar control de del presupuesto
- REINICIAR: Restaurar operaciones a la normalidad

Curso Jefes de Seguridad Privada

Módulo 1. Control de riesgos empresariales de seguridad.

ESQUEMA ANTERIOR (REACTIVO)	ENFOQUE ARES (PHVA)
☐ Evaluación del riesgo es histórica y se realiza eventualmente.	✓ La gestión de riesgo es un proceso continuo y recurrente.
☐ El análisis de riesgo detecta y reacciona.	✓ La gestión de riesgo anticipa y previene.
☐ El análisis de riesgos se enfoca en crímenes y los controles internos.	✓ La gestión de riesgos se enfoca en la identificación, medición y control integral de riesgos, velando que la organización logre objetivos con el menor impacto posible.
☐ Cada función es independiente. Pocas funciones tratan del análisis de riesgo.	✓ La gestión de riesgo está integrado en todas las operaciones y líneas de negocios.
☐ No hay una política de análisis de riesgo.	✓ La política de gestión de riesgo es formal y claramente entendida.

International Organization for Standardization (ISO). (2018, February 15) The new ISO 31000 keeps risk management simple. Consultado de https://www.iso.org/news/ref2263.html.

Maggio, E. J. (2009). Private security in the 21st century: Concepts and applications. Sudbury, MA: Jones & Bartlett.

Brown, S., & Blackmon, K. (2001). Operations management: Policy, practice and performance improvement. Woburn, MA: Butterworth-Heinemann.

International Foundation for Protection Officers (IFPO). (2013, September 18). Certified in Security Supervision and Management (CSSM).

https://www.ifpo.org/training/certified-in-security-supervision-and-management-cssm/•

International Foundation for Protection Officers (IFPO). (2014, January 2).
Training Programs. Consultado de https://www.ifpo.org/training-programs/.

Estándar ANSI/ASIS SPC.1-2009_Resiliencia organizacional sistemas d gestión de la seguridad, la preparación y la continuidad. Requisitos con orientación para su uso
http://www.aenor.es/aenor/normas/ediciones/fichae.asp?codigo=1092