Oficial de Protección Certificado
Certified Protection Officer

CPO©

Gestión de Riesgos

CPO©

INSTRUCTOR

CPP©

Carlos Ramírez Rodríguez, CPP

Consultor internacional en seguridad convergente, ciberseguridad y gestión de riesgos, con amplia experiencia liderando proyectos de protección de infraestructuras críticas en sectores como energía, minería y telecomunicaciones.

Es miembro activo de ASIS International e IFPO, y ha sido expositor en congresos internacionales sobre protección de activos, ciberdefensa y cultura de seguridad.

Fundador de Smart Spartans, empresa dedicada al cumplimiento normativo y la integración de seguridad física y cibernética, y creador de la plataforma SECURIX, una solución tecnológica para la gestión de incidentes y riesgos convergentes.

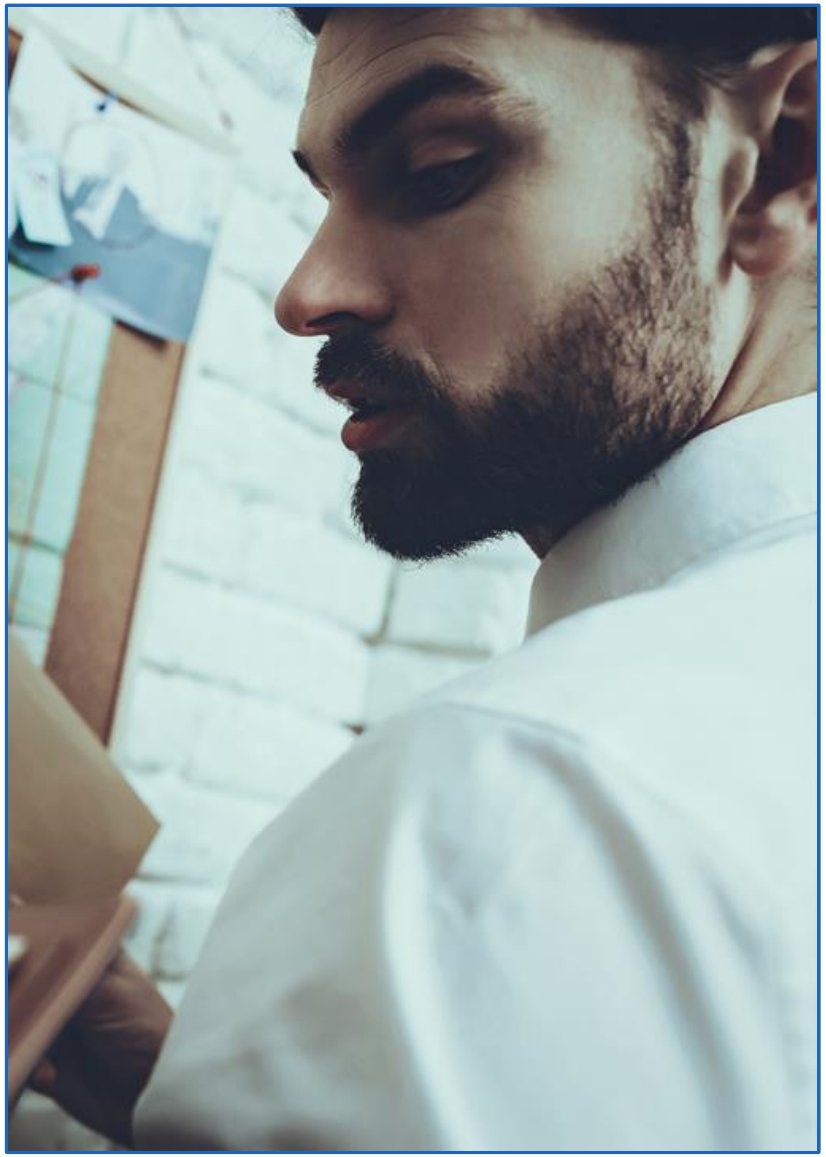
Autor del libro “Defensa Total: Ciberseguridad y Seguridad Física en la Protección de Infraestructuras Críticas”, reconocido por su enfoque innovador en la formación de profesionales de seguridad moderna.

Su misión es elevar el nivel profesional del sector de la protección, inspirando a los futuros Oficiales Certificados CPO a comprender que la verdadera prevención se logra con conocimiento, ética y liderazgo.

Conceptos Clave

CPO©

Conceptos Clave



Todo programa de seguridad comienza con el conocimiento. Antes de hablar de cámaras, barreras o sistemas de control, debemos entender por qué y cómo protegemos, qué es realmente un riesgo, y de qué manera la gestión preventiva se transforma en una herramienta estratégica para las organizaciones.

Aprenderemos los fundamentos que sustentan toda labor profesional de protección:

- Comprender los conceptos básicos que definen la seguridad moderna.
- Aprender a identificar, evaluar y tratar riesgos de manera estructurada.
- Conocer la importancia del control de pérdidas y la prevención del delito mediante el diseño del entorno (CPTED).
- Entender cómo operan los principios de mando, delegación y autoridad, que garantizan el orden y la eficacia en los equipos de seguridad.

Más allá de memorizar definiciones, esta unidad busca que el futuro Oficial Certificado de Protección (CPO) piense como un gestor del riesgo y un líder ético, capaz de anticipar problemas antes de que se conviertan en incidentes.

OBJETIVO DEL CAPÍTULO

OBJETIVO

1. Comprender los conceptos fundamentales que sustentan la labor del Oficial de Protección, diferenciando seguridad, riesgo, amenaza y vulnerabilidad.
2. Identificar los componentes del riesgo y aplicar el proceso de gestión de riesgos en escenarios reales de protección.
3. Analizar y aplicar estrategias de control de pérdidas, orientadas a la prevención de incidentes y la continuidad operativa.
4. Reconocer los principios de diseño ambiental (CPTED) como herramientas efectivas para prevenir el delito desde la planificación de los espacios.
5. Entender la estructura jerárquica y organizacional de la seguridad, incluyendo los conceptos de cadena de mando, unidad de mando, delegación de autoridad y administración por excepción.
6. Valorar el rol profesional del CPO como agente preventivo, ético y estratégico dentro de la cultura de seguridad de una organización.

Conceptos Clave

Antes de aplicar técnicas o procedimientos, el Oficial de Protección debe dominar el lenguaje de su profesión.

Las palabras dan forma a la cultura, y en seguridad, cada término tiene un impacto operativo y ético.

Las palabras construyen cultura

- “Protección” y “Seguridad” son más que acciones; son una forma de pensar.
- Comprender la terminología profesional es el primer paso hacia la excelencia.
- La seguridad ya no es reacción: es ciencia, estrategia y liderazgo.

Antes los oficiales eran vistos solo como “guardias” y hoy son gestores de riesgos, consultores técnicos y guardianes de la reputación corporativa.

¿Seguridad o Protección?

Concepto	Traducción inglesa	Enfocado en...	Tipo de Riesgo
Protección (Security)	Riesgos intencionales	Personas, información, activos	Delitos: sabotaje, espionaje, robo
Seguridad (Safety)	Riesgos accidentales	Instalaciones, entorno laboral	Accidentes, errores humanos, naturaleza

- Security: sabotaje interno en un data center.
- Safety: incendio por sobrecarga eléctrica.

Protección Integral de Recursos

"La protección integral combina medios humanos, tecnológicos y procedimientos para prevenir y reaccionar frente a riesgos intencionales, accidentales y naturales."

- Une la seguridad física, la industrial, la cibernética y la gestión de emergencias.
- Equivale al concepto moderno de Control de Pérdidas.
- Requiere coordinación, entrenamiento y cultura preventiva.

El oficial de Protección Integral

El nuevo perfil del Oficial de Protección:

- Identifica fuentes de riesgo intencional (personas o agresores).
- Controla riesgos no intencionados (accidentes, fenómenos naturales).
- Integra tecnología, procesos y factor humano.

Ejemplo real:

Un oficial detecta comportamientos anómalos en cámaras y activa el protocolo de ciberseguridad → evita una filtración de datos.

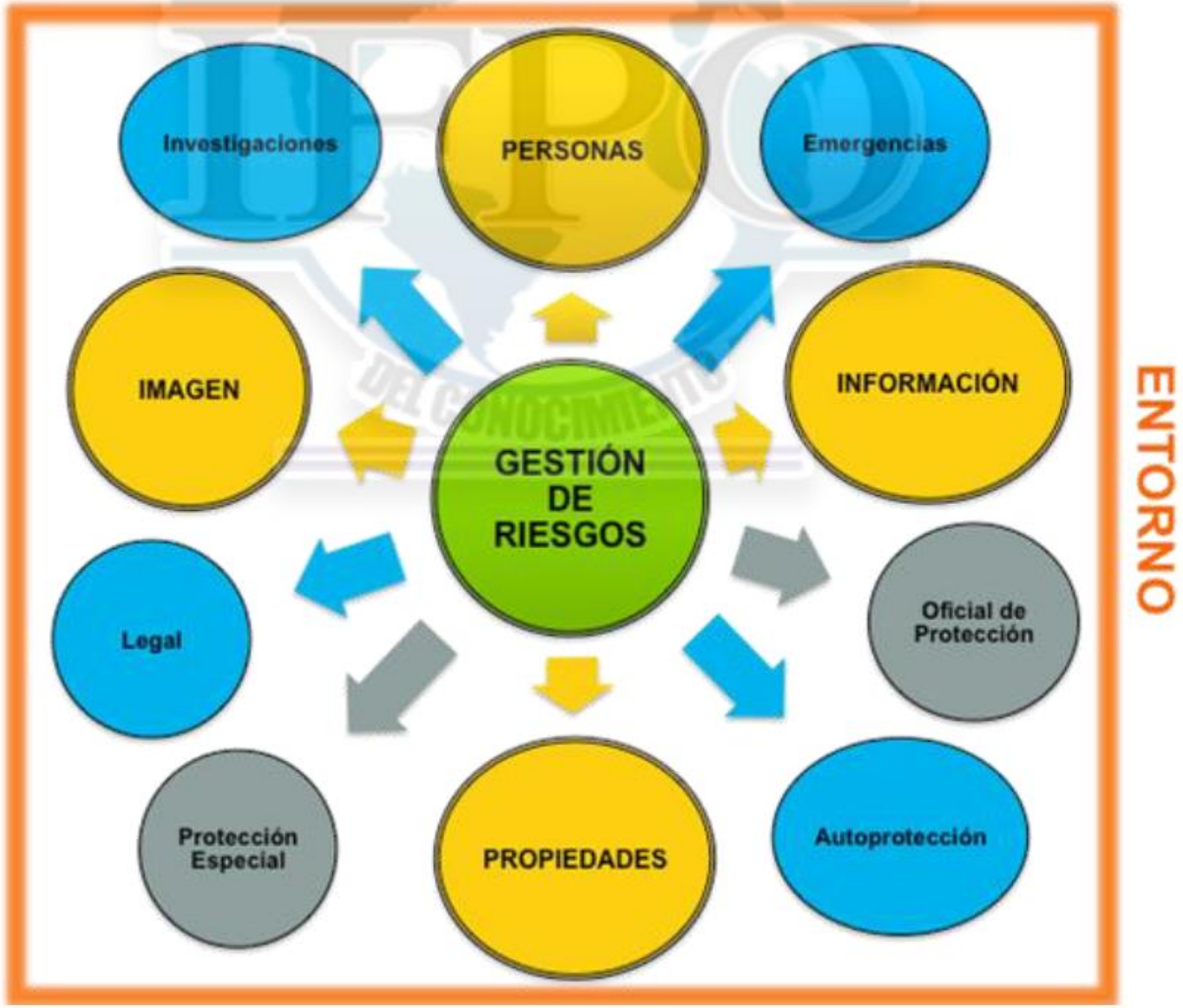
Los Recursos a Proteger

Recurso	Tipo de capital	Ejemplos
Personas	Humano	Trabajadores, visitantes, comunidad
Información	Intelectual	Datos, patentes, planes estratégicos
Propiedades	Financiero	Edificios, equipos, flotas, infraestructura
Imagen	Comercial	Reputación, confianza, marca

Momento de Ustedes:

Haber quienes me pueden identificar un ejemplo de pérdida para cada tipo de recurso.

Sistemas y Subsistemas



Al organizar los esfuerzos de protección integral de recursos se establecen subsistemas para cada recurso a proteger (principales) y otros para actividades de apoyo (auxiliares).

Esta sistematización se ve reflejada en los nombres de las doce unidades que aborda el manual del CPO.

Resumen de Conceptos Clave

- Protección ≠ Seguridad.
- La protección integral abarca todos los riesgos.
- El Oficial de Protección debe pensar en términos de recursos, impacto y prevención.

"Un verdadero profesional de la protección no solo reacciona ante el peligro: lo anticipa, lo entiende y lo controla."

Conceptos asociados al riesgo

El núcleo de toda gestión de protección: el riesgo.
Cada incidente, cada pérdida, cada decisión en seguridad nace o fracasa dependiendo de cómo entendemos y gestionamos el riesgo.
Por eso, el oficial de protección ya no es simple observador del peligro, sino analista, evaluador y gestor del riesgo.
La tarea no es eliminarlo —porque eso es imposible— sino identificarlo, reducirlo y mantenerlo bajo control.
Hablar de riesgo es hablar de probabilidad, vulnerabilidades y consecuencias, pero también de personas, procesos y cultura.Un oficial que no comprende el riesgo actúa a ciegas.Uno que lo domina, puede anticipar los problemas antes de que se conviertan en crisis.

Introducción al concepto de Riesgo

En seguridad, el riesgo es el lenguaje universal.
Cada acción, decisión o medida preventiva nace de la capacidad de entender, medir y controlar los riesgos que enfrentamos.

Definición simple:
“Riesgo es la posibilidad de que ocurra un evento no deseado que cause pérdida o daño.”

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.

Ejemplo: una empresa minera subestimó un riesgo menor (una cámara inactiva en una zona crítica) que luego permitió un robo interno

Azar o mala gestión del riesgo?

Componentes del Riesgo

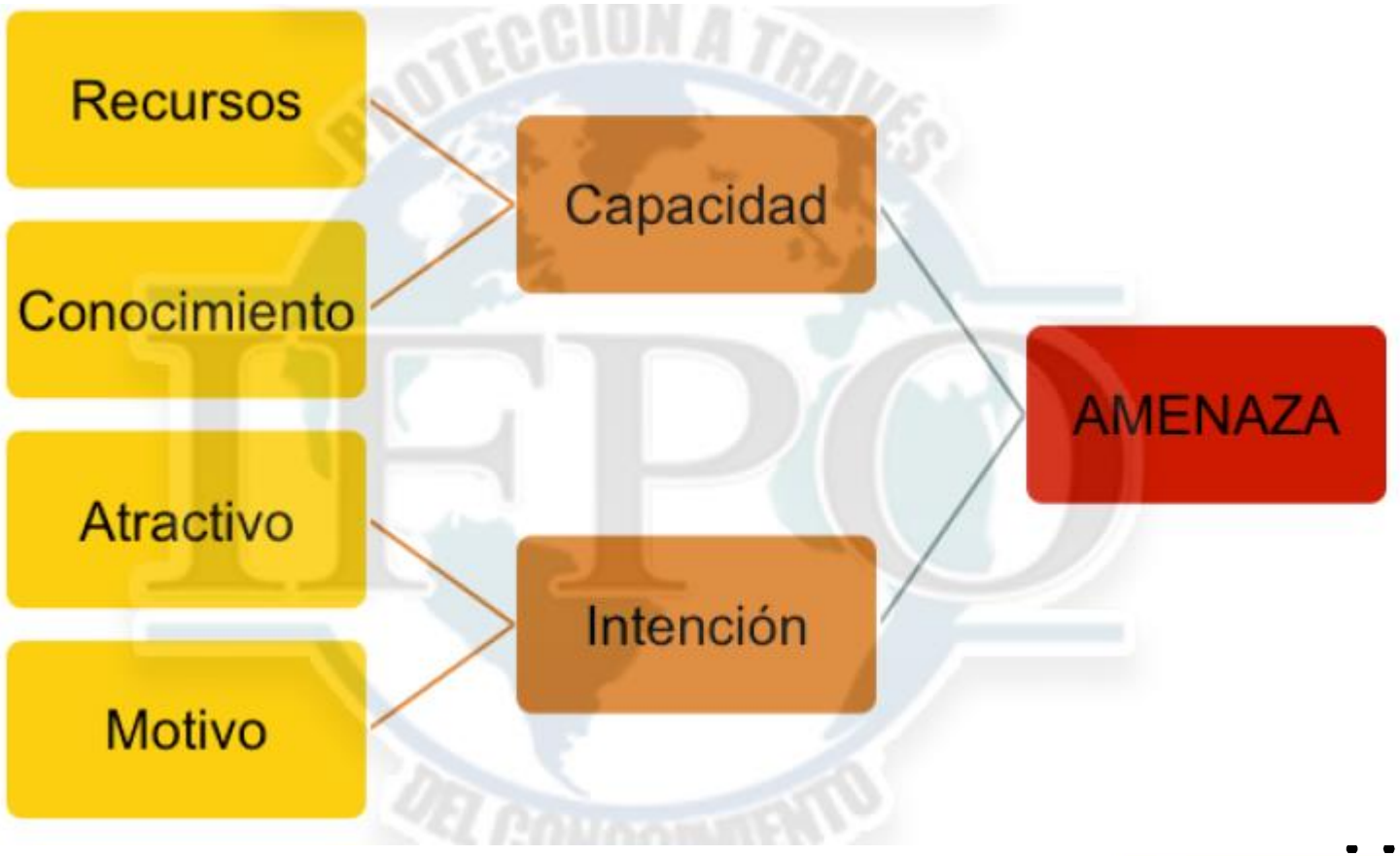
Las tres variables esenciales

Componente	Descripción	Ejemplo
Amenaza	Fuente del peligro o acción que puede causar daño.	Hacker, delincuente, incendio.
Vulnerabilidad	Debilidad que puede ser aprovechada.	Contraseña débil, puerta sin cierre, empleado desatento.
Impacto	Consecuencia o pérdida resultante.	Pérdida de datos, daño físico, reputacional.

Pensemos en un ejemplo real de cada componente (puede ser de su trabajo o una noticia).

Amenaza

AMENAZA es un individuo o grupo de personas con elementos -de capacidad e intención- que lo califican para causar
pérdida en los recursos.



Pérdida

Cuando se establece la relación unívoca entre amenazas y las correspondientes vulnerabilidades se construye un PERFIL DEL EVENTO DE PÉRDIDA.

Relación entre Riesgo y Control

El RIESGO no se elimina
Se CONTROLA

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).

- Ninguna organización puede operar con riesgo cero.
- El objetivo es reducir la probabilidad o el impacto hasta un nivel aceptable.
- Cada control (físico, técnico o humano) actúa sobre una de las variables del riesgo.

Controles
Control físico → cámaras y cerraduras.
Control técnico → firewall o autenticación.
Control humano → capacitación y supervisión.

Ejercicio Práctico

Actividad guiada (10 min):
Identificando los riesgos de tu entorno

1. Anotar en una hoja un área que conozcan (oficina, planta, edificio).
2. Identificar una amenaza, una vulnerabilidad y un impacto posible.
3. Compartamos casos en forma voluntaria.

Objetivo: Comprender que el análisis de riesgo no es teórico, sino parte del trabajo diario del Oficial de Protección.

Algunas Conclusiones acerca del Riesgo…

- “No hay seguridad sin comprensión del riesgo.”
- “El riesgo no se elimina, se administra.”
- “La prevención inteligente es el resultado del análisis.”

Del análisis a la acción: el proceso de gestión de Riesgos

Comprender el riesgo es solo el primer paso.
La verdadera diferencia profesional está en cómo lo gestionamos: cómo lo identificamos, evaluamos, tratamos y monitoreamos.
El proceso de gestión de riesgos convierte la intuición en un método.
Nos permite tomar decisiones basadas en evidencia, priorizar recursos y justificar cada acción de seguridad con lógica técnica.

"Gestionar el riesgo no es eliminarlo, sino controlarlo inteligentemente."

Etapas del proceso

1. Identificación del riesgo – ¿Qué puede pasar?
2. Análisis del riesgo – ¿Por qué puede pasar y con qué consecuencias?
3. Evaluación del riesgo – ¿Qué nivel tiene y qué tan aceptable es?
4. Tratamiento del riesgo – ¿Qué haremos al respecto?
5. Monitoreo y revisión – ¿Funcionan nuestras medidas?

Etapas del proceso

El proceso usado por IFPO para gestionar los riesgos puros sigue un ciclo de seis pasos interrelacionados en un ciclo continuo:

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

Todas las normas y estándares sobre riesgo actualmente se alinean con el ciclo estandarizado para la administración de riesgos, que ha sido establecido en la norma ISO 31.000:2009

Etapas del proceso

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

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

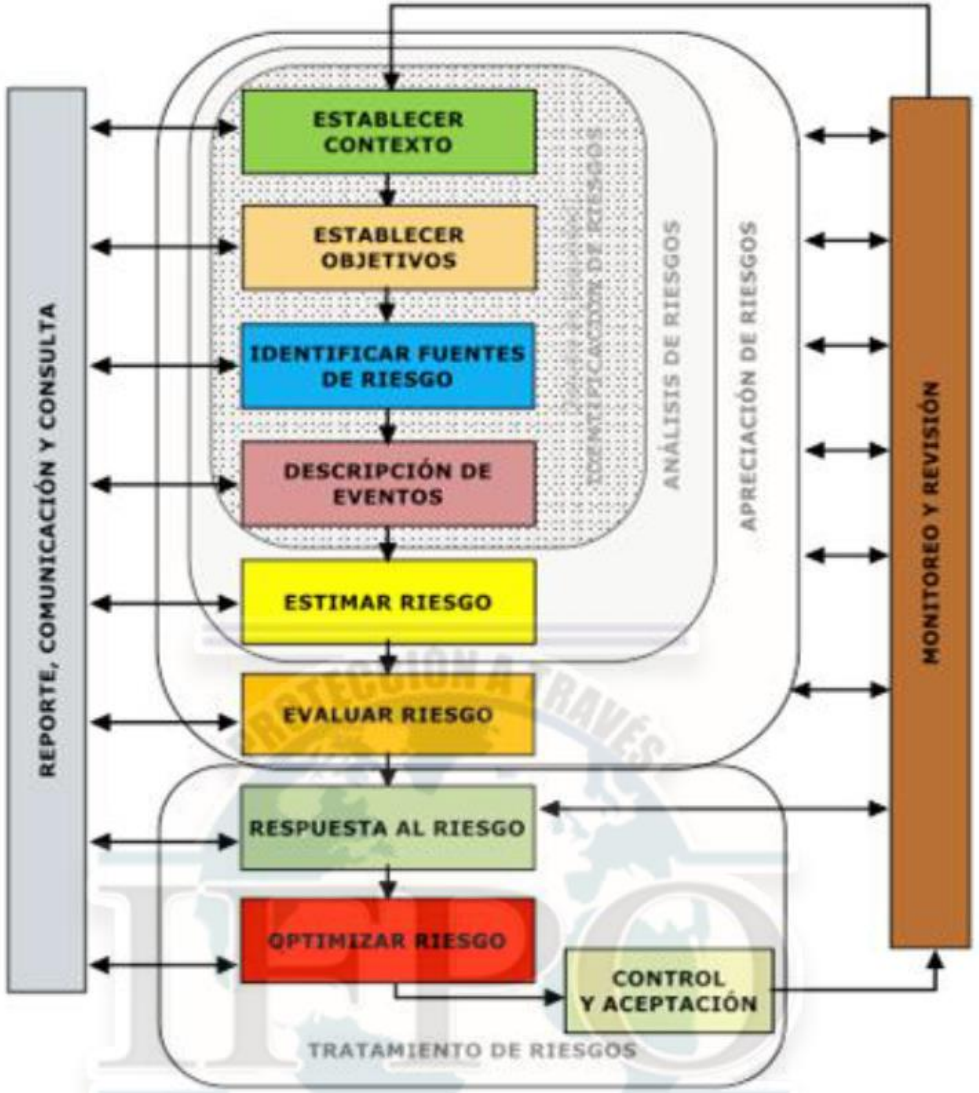
DECIDIR: Se toman decisiones a dos niveles: Estratégico y Táctico - operativo

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

IMPLEMENTAR: Se ejecutan las medidas de control de pérdidas.

SUPERVISAR: Los resultados deben generar mejoras y retroalimentar el proceso

Etapas del proceso



ISO 31.000: Gestión de Riesgos

International Organization for Standardization
ISO
31000

Tratamiento de Riesgos

E – Evitar completamente los riesgos, cambiando de actividad o trasplantando el bien a otro 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: Compartiendo el impacto de las pérdidas. (Seguro, asociación financiera o subcontratación)
O – Optimizar: Aprovechando el riesgo en busca de oportunidades, adaptando parámetros internos o externos a través de medidas de control de pérdidas para controlar: 1. Exposición al peligro; 2. Vulnerabilidades; o 3. Consecuencias.
A – Aceptar: Decisión informada de aceptar el riesgo cuando éste está dentro de límites tolerables (riesgo tolerable).

Control de Pérdidas

El objetivo final de toda gestión de seguridad es reducir pérdidas.
Cada amenaza, cada vulnerabilidad, cada riesgo, tiene un denominador común: puede generar pérdida.
El control de pérdidas busca que los recursos —personas, información, propiedades e imagen— se mantengan disponibles y protegidos frente a cualquier evento adverso, sea intencional o accidental.
En este bloque entenderemos cómo el control de pérdidas es un sistema integral, que combina prevención, detección y respuesta.
También veremos cómo se organiza internamente en subsistemas, y por qué hoy este enfoque se ha convertido en el lenguaje universal de la seguridad corporativa.

"No hay seguridad efectiva sin control de pérdidas; no hay control de pérdidas sin gestión del riesgo."

Control de Pérdidas

P – Prácticas no profesionales / no éticas, como fraude, ocultación, tergiversación, discriminación, conflictos de interés, crimen de cuello blanco, entre otros.
E – Error en la planeación o ejecución.
R – Robo y diversos comportamientos criminales.
D – Desperdicio de recursos, tiempo, materiales, mano de obra y espacio.
I – Incidentes y desviaciones de normas que aparentemente no causan daño.
D – Daños mayores naturales e intencionales, incluye sabotaje.
A – Accidentes y Enfermedades Laborales que causan lesión, reducción del tiempo efectivo de trabajo y compensaciones laborales.

Control de Pérdidas

- Es el conjunto de acciones y medidas orientadas a evitar, reducir o controlar las pérdidas derivadas de incidentes.
- Aplica tanto a pérdidas humanas, materiales, financieras o reputacionales.
- Implica integrar tecnología, procedimientos y factor humano.

El Control de Pérdidas: el corazón de la protección integral

Objetivos del Control de Pérdidas

Objetivos principales

Objetivo	Descripción
🔍 **Detectar riesgos**	Identificar condiciones o actos inseguros antes de que se materialice
🛡️ **Prevenir incidentes**	Evitar la ocurrencia de eventos mediante medidas proactivas.
🚨 **Mitigar el impacto**	Reducir el daño cuando el evento no puede evitarse.
📊 **Registrar y aprender**	Generar datos para mejorar la gestión futura.

Control de Pérdidas

El 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:

PLANEAR incluye actividades relacionadas con la Apreciación de Riesgos ejecutadas en el Antes
HACER implica actividades operativas de Mitigación de Riesgos ejecutadas en el Durante
VERIFICAR involucra actividades de Control Operacional de Riesgos ejecutadas en el Durante
ACTUAR ejecuta actividades de Resiliencia frente a la materialización de riesgos y mide la capacidad de Aprender, se establece en el Después

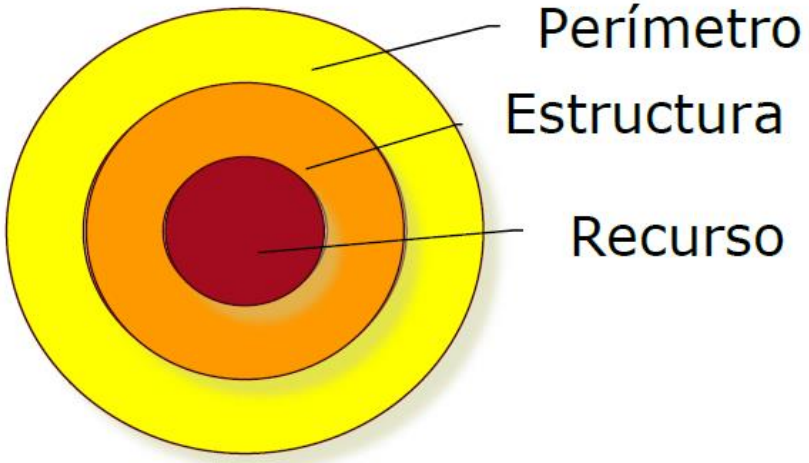
Prevención del Delito por el Diseño del Entorno - CPTED

Prevención del delito mediante el diseño del entorno (CPTED)
Definición: “CPTED es una estrategia de prevención del delito que busca reducir las oportunidades de comisión mediante el diseño, planificación y gestión del entorno físico.”:

Prevención del Delito por el Diseño del Entorno - CPTED

Se apoya en 6 Fundamentos:

DEFENSA EN PROFUNDIDAD: Creando círculos concéntricos de contramedidas en el perímetro, estructura y recursos a proteger.



TERRITORIALIDAD: Marcación de límites y líneas de propiedad bien establecidas. Por ejemplo usando letreros para crear percepción de propiedad y sentimiento de pertenencia.

VIGILANCIA: Observar ciertas áreas hace que la detección y disuasión de la conducta criminal sea más fácil. Existen tres clases de vigilancia:

a. Natural: Manteniendo áreas abiertas para observar, despejar los arbustos cercanos a puntos de acceso.

b. Electrónica: Utilizando ayudas tecnológicas.

c. Organizada: Mediante patrullajes con personal de protección y/o Fuerza Pública.

Prevención del Delito por el Diseño del Entorno - CPTED

CONTROL DE ACCESOS:
Manteniendo límites mediante accesos restringidos hacia un área. El control de accesos tiene seis pasos:

1. Validar
2. Confirmar
3. Registrar
4. Inspeccionar
5. Entregar
6. Permitir

REFUERZOS POSITIVOS: Es un esfuerzo para alejar a las personas de actividades criminales; busca asegurar la disponibilidad, confidencialidad e integridad de los recursos. Esto puede tomar formas como dar refuerzo a actividades positivas, involucrar a los usuarios en actividades voluntarias.

MANTENIMIENTO: El desorden y la suciedad causan pérdidas.
La reparación de daños y mantener orden y limpieza continuamente demuestra interés y disuade el crimen.

Otros Conceptos Clave

Delegación de Autoridad

Administración por excepción

Cadena de Mando

Unidad de Mando

Extensión del control

PREGUNTAS DE AUTOEVALUACIÓN

Manejo Operativo del Riesgo

CPO©

Manejo operativo del Riesgo

La función esencial del profesional de protección es comprender y controlar los riesgos que pueden afectar a las personas, la información, las propiedades y la imagen bajo su responsabilidad. Ningún sistema puede eliminar todos los riesgos, pero sí puede controlarlos mediante planificación metódica y decisiones informadas.

El objetivo es integrar personas, tecnología y procedimientos para reducir la probabilidad y el impacto de pérdidas, a través de un proceso estructurado de Manejo Operativo de Riesgos (MOR).Este proceso convierte la seguridad en una disciplina sistemática, aplicable a todos los niveles :Estratégico – Táctico – Operativo

“La seguridad no es una acción, es un proceso continuo de decisiones inteligentes.”

OBJETIVO DEL CAPÍTULO

- Explicar la base de todas las funciones de protección, independientemente del entorno en que se practiquen.
- Identificar y definir los elementos clave del MOR.
- Explicar el ciclo / proceso de gestión del riesgo.
- Sustentar que la práctica del MOR requiere tanto una evaluación de riesgos exhaustiva como un programa de monitoreo continuo.
- Aprender las herramientas para aplicar las estrategias de Gestión de Riesgos para evaluar una situación, desarrollar un menú de opciones factibles y recomendar soluciones.

Matriz de Evaluación de Riesgos

Cuantificar el riesgo para decidir con criterio

La Matriz de Evaluación de Riesgos del MOR se utiliza una vez identificados los riesgos, para cuantificar y priorizarlos según su impacto y probabilidad.
Aunque la evaluación del riesgo siempre incluye cierto grado de subjetividad, la matriz ofrece un marco uniforme y objetivo para analizar y comparar distintos escenarios.
El impacto de pérdida mide la peor consecuencia creíble de un incidente —desde daños leves hasta pérdidas extremas— según estas categorías:

Matriz de Evaluación de Riesgos

PROBABILIDAD DE PÉRDIDA: cuan probable es que un evento ocurra. A la probabilidad se le asigna una letra por criterios:

A INMINENTE – Ocurrencia inmediata o dentro de un corto período de tiempo.

B PROBABLE – Probablemente ocurrirá.

C POSIBLE – Puede ocurrir en el tiempo.

D REMOTA – Improbable que ocurra.

Matriz de Evaluación de Riesgos

CER		PROBABILIDAD			
1 Crítico 2 Serio 3 Moderado 4 Menor 5 Insignificante		**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
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

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

Matriz de Evaluación de Riesgos

El proceso MOR: una guía para gestionar riesgos con método

El Programa de Manejo Operativo de Riesgos (MOR) estructura la toma de decisiones de protección a través de un proceso continuo de seis etapas. Cada paso busca maximizar la efectividad operacional y minimizar las pérdidas humanas, materiales o informacionales.

1. Identificar: Analizar las operaciones para detectar amenazas y vulnerabilidades en cada fase del trabajo.
2. Apreciar: Evaluar la probabilidad e impacto de cada evento de pérdida y calcular su nivel de riesgo (CER).
3. Decidir: Priorizar los riesgos más críticos, tomar decisiones al nivel jerárquico adecuado y determinar si los beneficios compensan los riesgos.
4. Comunicar: Informar, consultar y coordinar las acciones de control dentro de la cadena de mando.
5. Implementar: Aplicar medidas de control mediante procedimientos operativos, tecnología, ingeniería, barreras y capacitación del personal.
6. Supervisar: Evaluar la eficacia de las medidas, mantener la flexibilidad y ajustar los controles según los resultados.

"El MOR convierte la experiencia en método, y el método en seguridad sostenible."

Modelo ARES

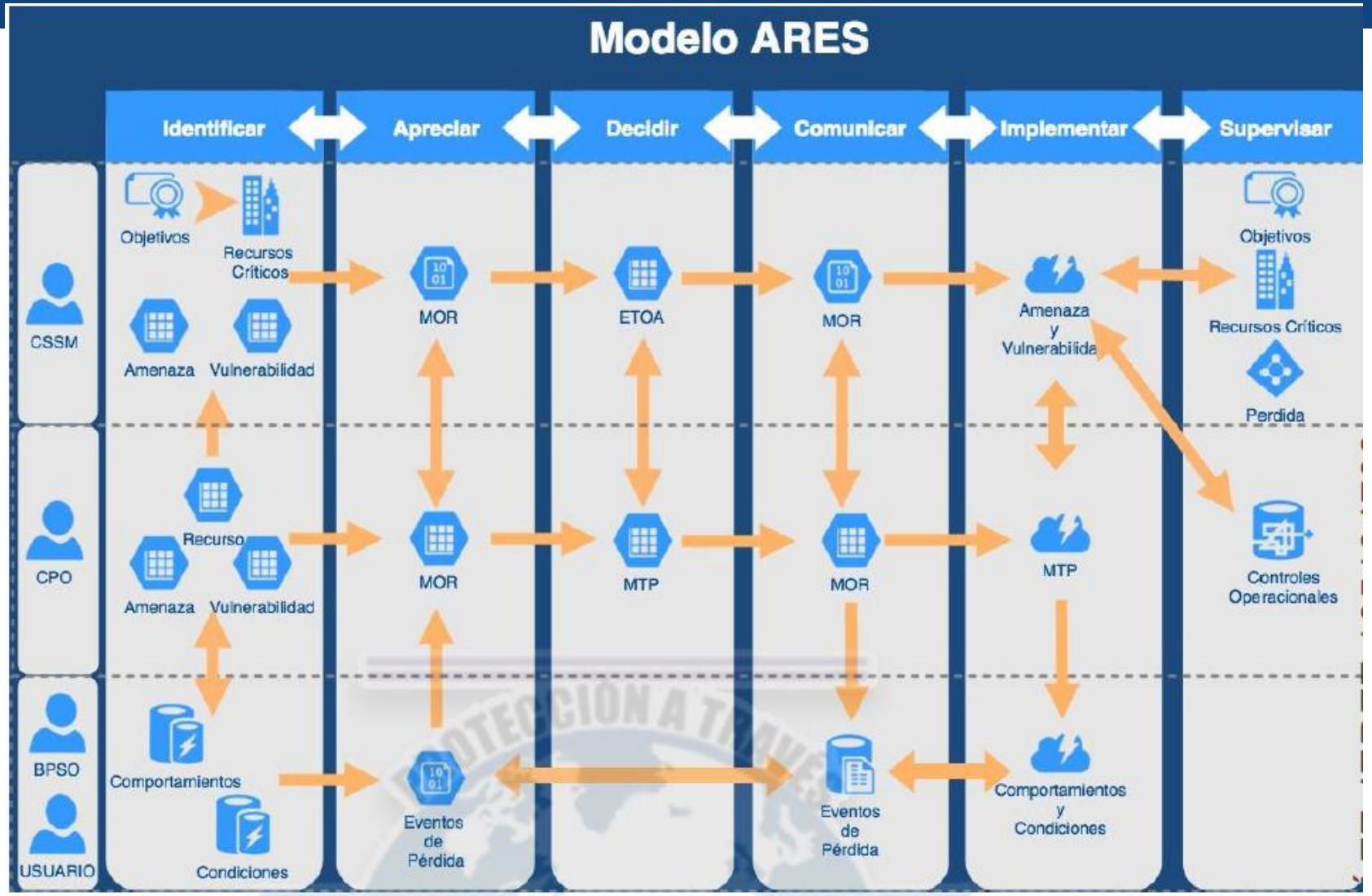
El Modelo ARES integra los principios de la gestión de riesgos en tres niveles —operativo, táctico y estratégico— asegurando que la protección se gestione de forma coherente en toda la organización.

- Nivel Operativo: Los oficiales básicos (BPSO) identifican vulnerabilidades, comunican condiciones inseguras y aplican correcciones según los procedimientos establecidos.
- Nivel Táctico: Los Oficiales CPO ejecutan el proceso completo del MOR: identifican, evalúan, deciden, comunican, implementan y supervisan los controles. Aplican la matriz MOR cualitativa, los principios CPTED, y equilibran controles de Métodos, Tecnología y Personas (MTP).
- Nivel Estratégico: Los gerentes de protección (CSSM) alinean los objetivos corporativos con los recursos críticos. Evalúan el riesgo mediante la matriz MOR cuantitativa, definen estrategias con la matriz ETOA, y justifican las inversiones en protección según pérdidas evitadas y cambios de criticidad.

El modelo ARES permite tomar decisiones analíticas, medibles y coordinadas a todos los niveles, convirtiéndose en un método integral de gestión de riesgos y rentabilidad organizacional.

"ARES transforma la seguridad en un proceso estratégico, donde cada nivel protege y mejora el desempeño de la organización."

Modelo ARES



PREGUNTAS DE AUTOEVALUACIÓN

Evolución de la Seguridad y Protección de Bienes

CPO©

Evolución de la Seguridad y Protección de Bienes

De la supervivencia a la profesión: la evolución de la protección

La historia de la protección es también la historia de la humanidad. Desde las primeras civilizaciones, el ser humano ha buscado defender sus recursos, bienes y personas frente a amenazas. A lo largo del tiempo, la protección ha pasado de ser una necesidad instintiva a convertirse en una profesión organizada y multifacética, con especialistas en distintas áreas. Comprender cómo ha evolucionado la seguridad privada nos permite valorar su importancia actual y anticipar los desafíos del futuro. La historia no solo muestra el pasado: revela las lecciones y tendencias que moldean el futuro de nuestra profesión.

”La protección no nació en la tecnología; nació con la humanidad.”

El Ciclo de la Historia

La protección: una necesidad tan antigua como la humanidad

Desde sus orígenes, el ser humano ha buscado proteger sus bienes, su vida y su entorno.

La protección privada no es una invención moderna: es una actividad que ha acompañado la historia, evolucionando hasta convertirse en una profesión estructurada y estratégica.

“Comprender el pasado nos enseña cómo proteger el futuro.”

El Ciclo de la Historia

Lecciones del pasado: tendencias que se repiten

El estudio histórico del control de pérdidas muestra patrones que aún persisten:

- Las iniciativas privadas siempre anteceden a las públicas.
- La protección crece junto al comercio y la industria.
- Los esfuerzos surgen después de una crisis o ataque.
- La defensa siempre va un paso detrás del delito.
- La protección suele nacer de la necesidad de ayuda mutua.

El Ciclo de la Historia

Orígenes: Periodos bíblicos y civilizaciones antiguas

La ley y la vigilancia nacen juntas

- El Código de Hammurabi (2000 a.C.) estableció las primeras leyes escritas.
- En Grecia (600–500 a.C.) surgieron los primeros guardias urbanos y protección de consejeros.
- El concepto de “protección ejecutiva” tiene su origen en esas tareas.

“Donde aparece la ley, nace la necesidad de protegerla.”

El Ciclo de la Historia

Roma: organización y estructura

Roma y el nacimiento de la seguridad organizada

- El Emperador Augusto creó los Pretorianos, primera fuerza de protección civil y estatal.
- Los Vigilios eran ciudadanos encargados de prevenir incendios y delitos.
- Con Justiniano surge el Corpus Juris Civilis, primer compendio legal sistemático.

El Ciclo de la Historia

Edad Media: comunidad y responsabilidad

Del Shire-Reeve al Constable: protección comunal

- En el período anglosajón aparece el Sheriff (Shire-Reeve) como autoridad de orden y justicia.
- Se desarrolla el sistema “tilthing”, donde grupos de 10 hombres juraban protegerse mutuamente.
- Nace la figura del Constable, precursor del jefe de policía local.

El Ciclo de la Historia

Era Moderna (1500–1900)

El nacimiento de la protección privada

- Surge la clase mercantil y con ella la primera policía privada para proteger el comercio.
- En 1829, Sir Robert Peel crea la policía moderna en Londres (Scotland Yard).
- Sus principios aún guían la profesión: disciplina, prevención, autocontrol, apariencia y relación con la comunidad.

“La ausencia de crimen es la mejor prueba de eficiencia.” — Sir Robert Peel

El Ciclo de la Historia

Expansión en América

El auge de la protección en Estados Unidos

- La expansión ferroviaria y la fiebre del oro generaron crimen y necesidad de vigilancia.
- Nacen las policías privadas de ferrocarril y los primeros vigilantes ciudadanos.
- A inicios del siglo XX, se crean cuerpos policiales estatales y el FBI (1932), marcando la profesionalización del sector.

El Ciclo de la Historia

Las guerras y la profesionalización

De la guerra a la industria: la protección moderna

- Las Guerras Mundiales impulsaron el desarrollo de la seguridad privada.
- El Departamento de Defensa de EE. UU. sistematizó la protección con manuales y estándares.
- El Manual de Protección Industrial (1952) se convirtió en la base de la seguridad moderna.

“Cada guerra deja una lección de prevención.”

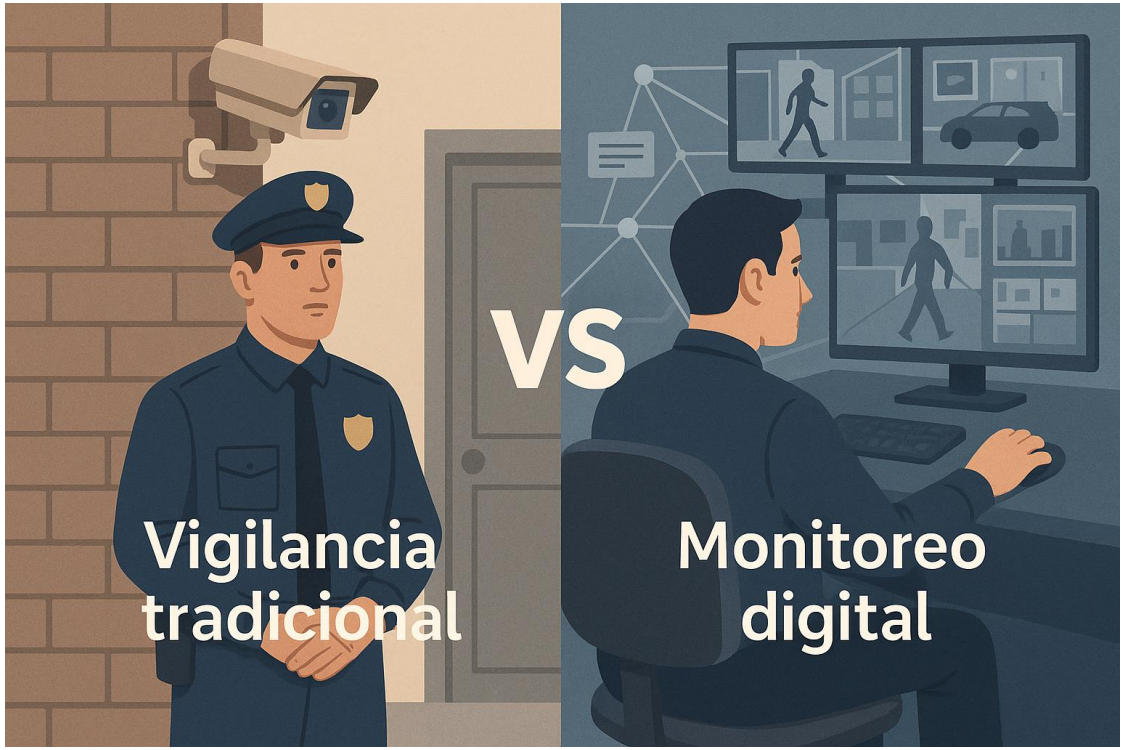
El Ciclo de la Historia

Hacia la era contemporánea

De la vigilancia física a la convergencia total

- Tras la Segunda Guerra Mundial, la protección se consolidó como una industria global.
- Hoy combina ciencia, tecnología y gestión estratégica, extendiendo su alcance a la ciberseguridad, protección de datos y control de pérdidas integral.

“La seguridad dejó de ser una reacción: hoy es una estrategia.”



Economía, tendencias de mercado y futuro de actividades de Protección

Economía, tendencias de mercado y futuro de actividades de Protección

La economía como motor del riesgo
Donde hay valor, hay amenaza

- A medida que los bienes y servicios adquieren valor, aumenta su atractivo para el crimen.
- El crecimiento del comercio minorista, los autoservicios y los canales digitales ha incrementado los riesgos de robo, fraude y sabotaje.
- Los delitos contemporáneos incluyen: Falsificación de productos y marcas. Robo de información y espionaje corporativo. Crímenes digitales: virus, desvío de fondos, robo de identidad.

“El delito se mueve al ritmo del mercado.”

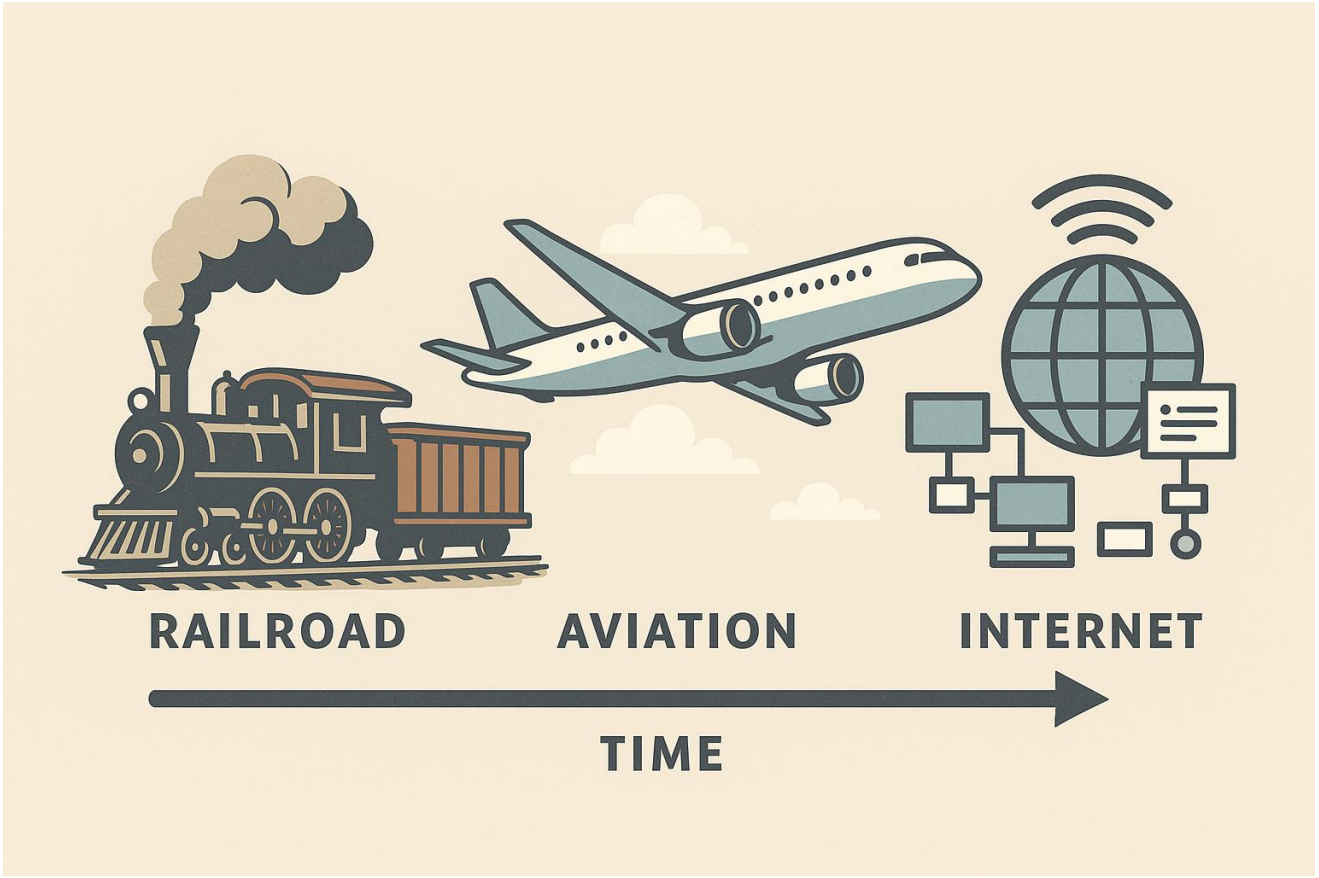
Economía, tendencias de mercado y futuro de actividades de Protección

Comercio y transporte: los primeros escenarios de protección

De los ferrocarriles al ciberespacio

- Desde el siglo XIX, el comercio ha impulsado la protección de recursos: Los ferrocarriles originaron cuerpos privados para defender vías y mercancías.
- En el siglo XX, el transporte aéreo introdujo nuevas amenazas: robos, terrorismo y secuestros, dando origen a los primeros programas de protección aeroportuaria (1974).
- Hoy, el frente de batalla está en el comercio electrónico y las telecomunicaciones, con delitos como la desinformación, el fraude digital y el robo de servicios.

“Cada nuevo canal de comercio crea un nuevo frente de riesgo.”



Economía, tendencias de mercado y futuro de actividades de Protección

Demografía y crimen

Las personas también definen la seguridad

Los cambios demográficos influyen directamente en los niveles de criminalidad. Durante la Revolución Industrial, la migración masiva y la urbanización desataron crisis sociales y aumento del delito.

Factores clave:

- Crecimiento poblacional acelerado.
- Choques culturales y pobreza urbana.
- Alcoholismo, desempleo y sobrepoblación.
- Ejemplo: Londres en 1850 y Nueva York en 1855 enfrentaron disturbios que llevaron a crear fuerzas policiales más organizadas.

“Donde cambia la sociedad, cambian también los riesgos.”

Economía, tendencias de mercado y futuro de actividades de Protección

Luchas sociales y terrorismo

Del conflicto de clases al extremismo global

La historia de la protección está marcada por los conflictos ideológicos y el terrorismo. Desde el Manifiesto Comunista (1848) hasta los atentados del 11 de septiembre de 2001, la violencia política y social ha transformado las estrategias de seguridad. Hitos relevantes:

- 1886: Disturbio de Haymarket (anarquismo).
- 1972: Secuestro de Patty Hearst (SLA).
- 1993–2001: Atentados en Nueva York y Washington (terrorismo islámico).
- 2015: Expansión del terrorismo global doméstico.

Factores que alimentan el extremismo: Desigualdad, cultura de guerra, manipulación religiosa, líderes carismáticos y pobreza estructural.

“Cada ideología extrema encuentra su reflejo en nuevas formas de violencia.”

Economía, tendencias de mercado y futuro de actividades de Protección

Relaciones laborales y profesionalización
Del conflicto obrero a la seguridad corporativa moderna

Los conflictos laborales fueron el origen de muchas prácticas modernas de seguridad. Antes, las empresas contrataban fuerzas privadas para romper huelgas; hoy, los equipos de seguridad especializados buscan prevenir daños y mediar conflictos. Estas experiencias dieron forma a:

- La planificación de emergencias.
- La protección del personal y las instalaciones.
- Los protocolos éticos y legales actuales en relaciones laborales.

“La seguridad laboral nació del conflicto, pero creció con la prevención.”

Administración de Riesgos y Seguros

El seguro: una herramienta dentro de la gestión de riesgos

Aunque el término “administración de riesgos” suele asociarse al sector asegurador, en realidad es una parte esencial del trabajo de protección integral.

El objetivo del profesional de seguridad no es solo endurecer el blanco (cerraduras, alarmas, barreras), sino aplicar los cinco métodos de administración del riesgo: evitar, reducir, transferir, aceptar y compartir.

El seguro es una forma de transferencia del riesgo, ya que ofrece compensación económica al asegurado tras una pérdida, basada en probabilidades y cálculos actuariales.

Administración de Riesgos y Seguros

TIPOS DE SEGUROS EN LA PROTECCIÓN
Instrumentos financieros para mitigar pérdidas

Las pólizas de seguro permiten proteger recursos, personas e información frente a distintos tipos de riesgo. Entre las más relevantes para la gestión de protección se incluyen:

1. Interrupción de negocios – Compensa pérdidas por suspensión operativa.
2. Secuestro y rapto – Cobertura ante extorsión o rescate.
3. Compensación laboral – Cubre accidentes o lesiones de empleados.
4. Incendios y robos – Protege activos físicos ante daños o sustracción.
5. Atracos y asaltos – Repara pérdidas en efectivo o mercancías.
6. Responsabilidad civil y profesional – Cubre daños a terceros por acción u omisión.
7. Fidelidad laboral – Protege frente a fraudes o deslealtad interna.

“El seguro no reemplaza la prevención, pero fortalece la resiliencia.”

La Ley

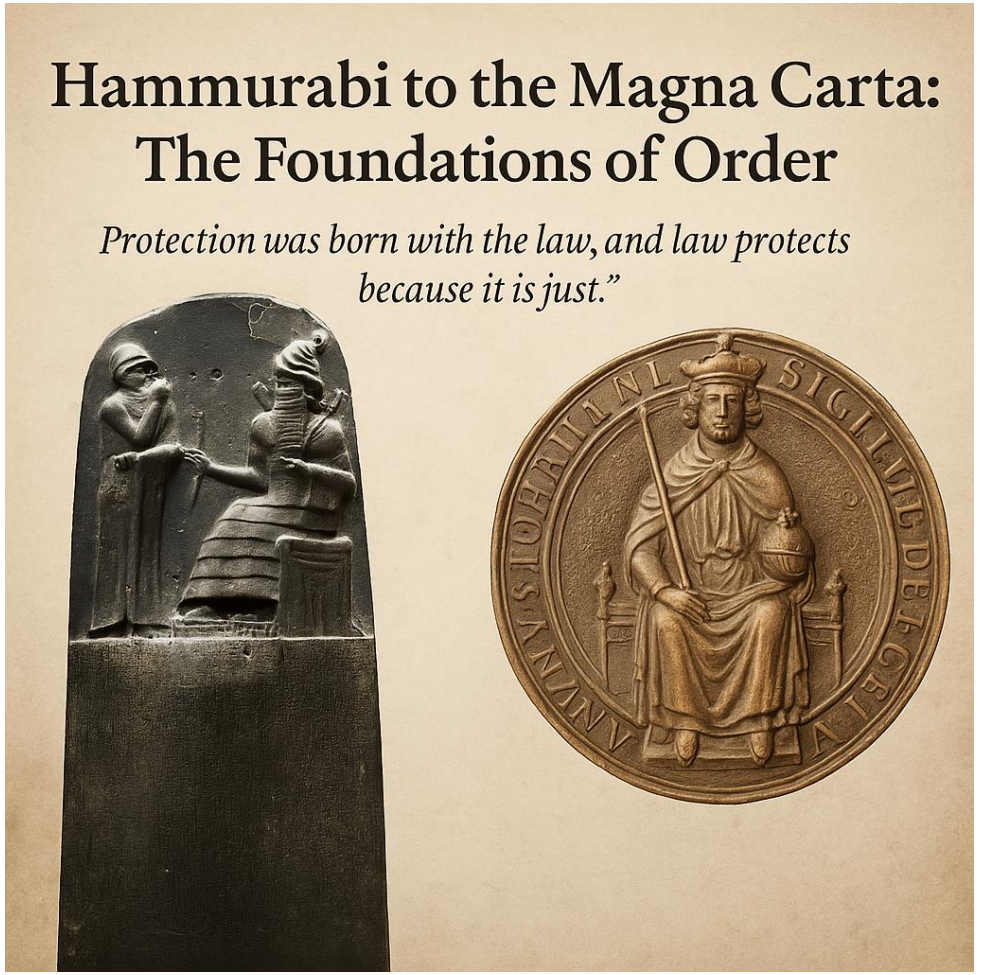
ORÍGENES Y EVOLUCIÓN DE LA LEY
De Hammurabi a la Carta Magna: los cimientos del orden

La ley surge como el primer sistema de control y justicia.

- El Código de Hammurabi (1792–1750 a.C.) estableció las primeras normas escritas, definiendo ofensas y castigos.
- La Carta Magna (1215) introdujo el principio del debido proceso, garantizando que toda persona sea tratada con justicia bajo reglas uniformes.

Estos hitos marcaron la base de la protección legal y moral, que luego inspiró el desarrollo del derecho moderno.

"La protección nació con la ley, y la ley protege porque es justa."



La Ley

EL PROFESIONAL DE PROTECCIÓN Y EL MARCO LEGAL

La ley como eje de la protección profesional

Los oficiales y gerentes de protección deben comprender y aplicar los principios legales que regulan su labor. Su responsabilidad incluye desarrollar políticas, evaluar riesgos y actuar dentro de la ley en temas de privacidad, propiedad y derechos humanos.

Las principales ramas del derecho aplicables son:

- Ley penal: delitos, robos, vandalismo, asaltos, violaciones.
- Ley civil: contratos, servicios, arrendamientos y relaciones entre personas.
- Ley administrativa: regulaciones de seguridad, salud, medio ambiente y telecomunicaciones.

“La protección sin ley se convierte en riesgo.”

La Ley

LEYES, CONTRATOS Y RESPONSABILIDAD

Negligencia, cumplimiento y responsabilidad legal

Los profesionales de la protección deben conocer las obligaciones legales derivadas de sus contratos y servicios:

- Seguridad privada y ejecutiva.
- Monitoreo y respuesta de alarmas.
- Investigaciones privadas y transporte de valores.

La negligencia ocurre cuando un servicio se ejecuta sin el debido cuidado y causa daño previsible. Para demostrarla se deben cumplir cinco condiciones:

1. Existencia del servicio.
2. Falla o error en su desarrollo.
3. Daño o lesión.
4. Que el daño fuera previsible.
5. Que derive directamente de la acción del acusado.

Además, las leyes administrativas y laborales regulan el cumplimiento de seguridad ocupacional (OSHA), relaciones laborales (NLRA), medio ambiente (EPA), aviación (FAA), energía nuclear (NRC), comunicaciones (FCC) y equidad de empleo (EEOC).

“Cumplir la ley no es opcional: es la base de toda protección legítima.”

Historia de las Empresas de Protección

EL NACIMIENTO DE LAS EMPRESAS DE PROTECCIÓN
De la vigilancia contratada a la industria global de la protección

Las agencias de protección privada surgieron como complemento a la seguridad pública, ofreciendo flexibilidad y especialización a empresas e individuos. La tercerización permite a los clientes adaptar recursos según sus necesidades y obtener personal capacitado sin mantener estructuras permanentes. Con el tiempo, las compañías dejaron atrás el concepto de “guardias” para dar paso al perfil profesional del Oficial de Protección (O.P.), con servicios que incluyen: Monitoreo y respuesta a alarmas. Transporte de valores y vehículos blindados. Protección personal ejecutiva (PPO). Investigación privada y análisis de riesgos.

- **“La seguridad dejó de ser un gasto para convertirse en una inversión estratégica.”**

Historia de las Empresas de Protección

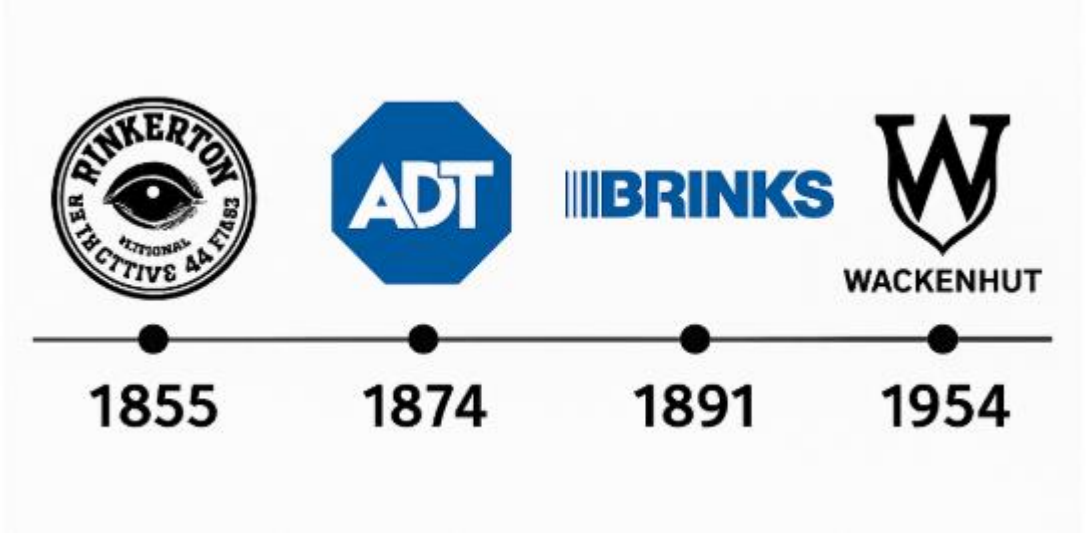
HITOS HISTÓRICOS DE LA INDUSTRIA

Pioneros y evolución de las empresas de protección

Los principales hitos de la historia moderna de la seguridad privada incluyen:

- 1855 – Allan Pinkerton funda la primera agencia de detectives (EE.UU.).
- 1858 – Edwin Holmes crea el primer sistema de supervisión y respuesta de alarmas.
- 1874 – ADT se consolida como líder mundial en alarmas, inventando el contacto magnético.
- 1891 – Brinks Armored inicia operaciones, convirtiéndose en la mayor empresa de transporte de valores.
- 1909 – William J. Burns dirige el precursor del FBI.
- 1954 – George Wackenhut funda la Wackenhut Corporation, referente en servicios integrales de protección.

“Cada época aportó una innovación; juntas crearon la industria moderna de la seguridad.”

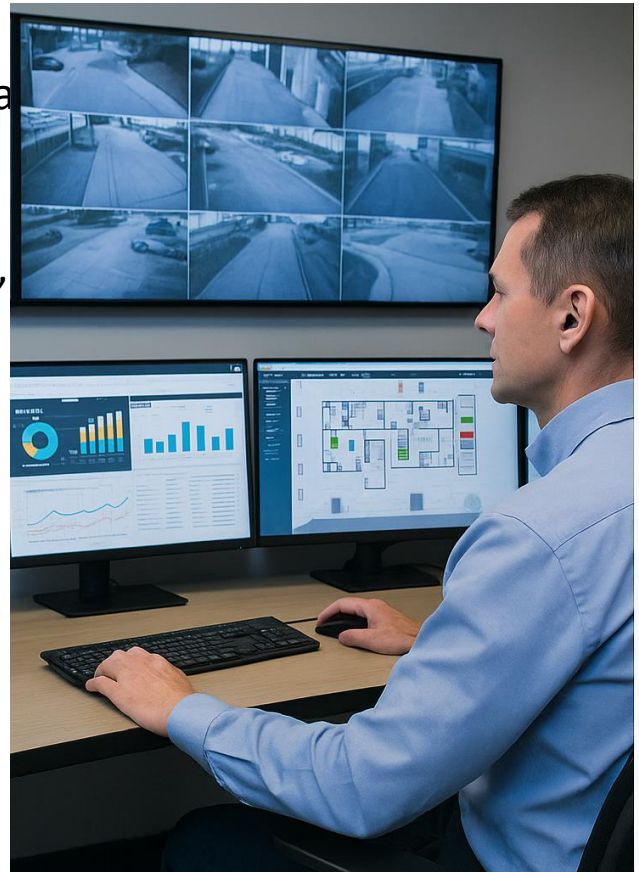


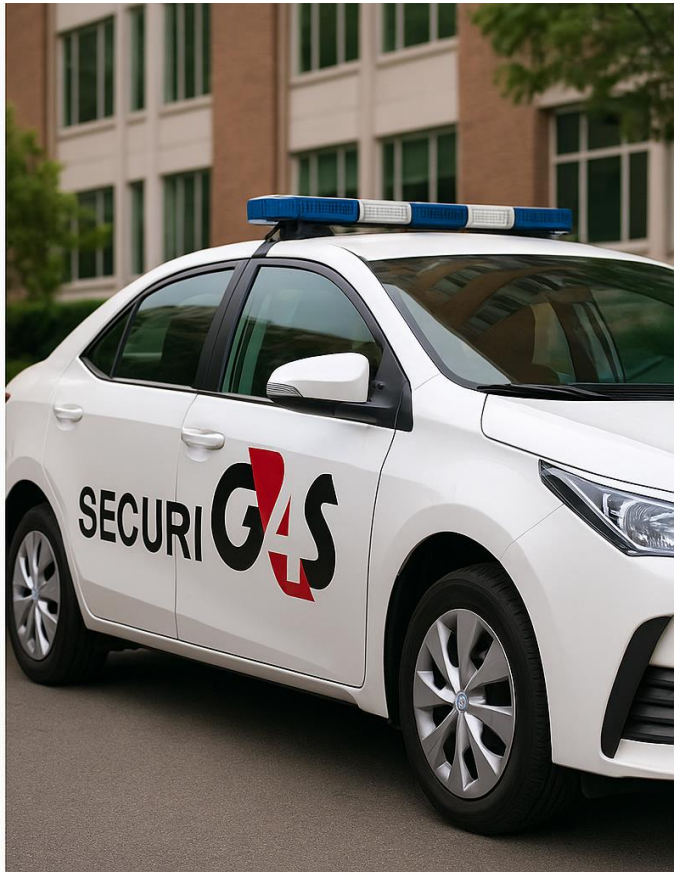
Historia de las Empresas de Protección

LA INDUSTRIA HOY
Un sector en expansión y transformación

Hoy, la industria de la protección es global, tecnológica y profesionalizada. Las empresas combinan inteligencia, ciberseguridad y servicios físicos, ofreciendo soluciones integrales en gestión de riesgos, protección ejecutiva y análisis de incidentes.
Las oportunidades de carrera se amplían en ventas, operaciones, atención al cliente, gestión humana y tecnología aplicada a la seguridad.

"El futuro de la protección pertenece a quienes integran personas, procesos y tecnología."





Trayectoria al Profesionalismo

EL CAMINO HACIA EL PROFESIONALISMO

De la práctica empírica a la profesión certificada

La industria de la protección ha recorrido un largo camino hacia su consolidación profesional. A mediados del siglo XX, comenzó un proceso de formalización y regulación que buscó elevar la calidad, la formación y la credibilidad de los servicios de seguridad privada. Hitos clave:

- 1955: Nace la ASIS International, primera organización global dedicada a la profesionalización de la seguridad industrial.
- 1971: El Reporte RAND revela que la industria de la protección era extensa pero irregular, marcando la necesidad de estandarización.
- 1975–1976: El Reporte del Grupo de Fuerzas en Protección Privada impulsa la creación de estándares mínimos de entrenamiento y licenciamiento.

“La profesionalización comienza cuando la experiencia se convierte en conocimiento compartido.”

Trayectoria al Profesionalismo

CONSOLIDACIÓN INTERNACIONAL

Certificaciones que transformaron la profesión

Los años 80 y 90 marcaron un antes y un después en la profesionalización de la seguridad:

- 1985: ASIS crea la certificación CPP, que establece un estándar global de competencia para los gerentes de seguridad.
- 1988: Se funda la IFPO, dedicada a elevar el estatus profesional de los oficiales de protección públicos y privados.
- 2006: Nace IFPO Sudamérica, promoviendo la formación y certificación regional.
- 2016: Se lanza IFPO en Español, extendiendo los programas de capacitación a todo el mundo hispanohablante.

“La seguridad dejó de ser oficio para convertirse en profesión.”

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

IFPO
FUNDACIÓN INTERNACIONAL PARA OFICIALES DE PROTECCIÓN
PROTECCIÓN A TRAVÉS DEL CONOCIMIENTO

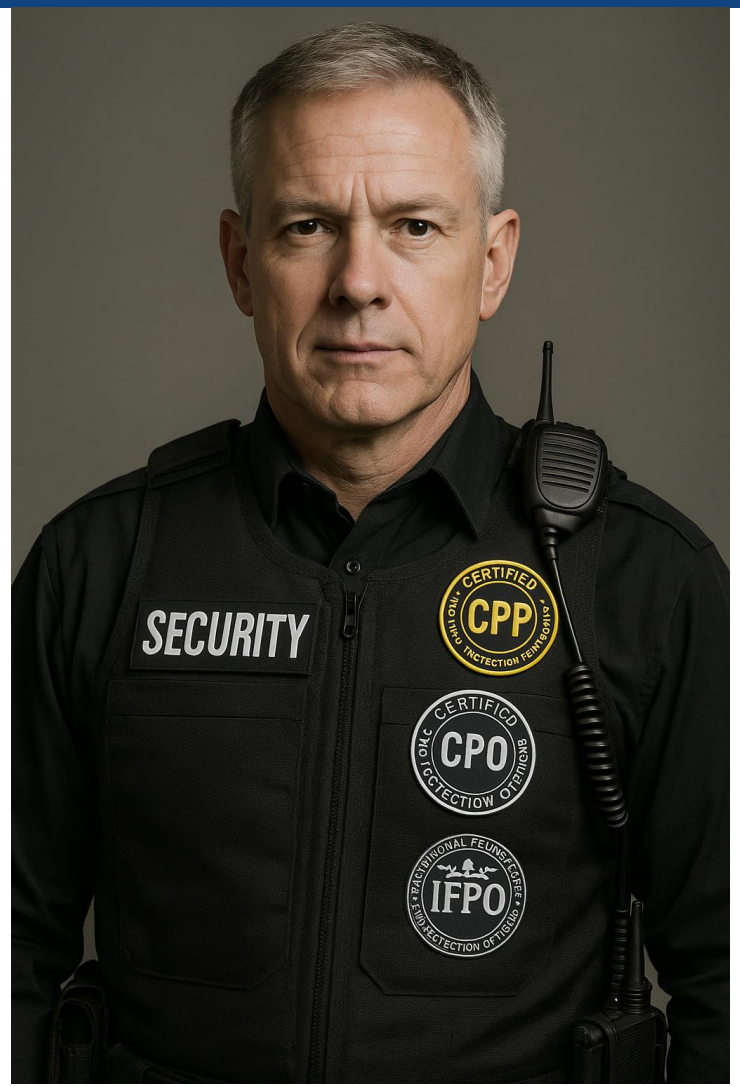
Trayectoria al Profesionalismo

EL PROFESIONAL DE PROTECCIÓN HOY
Competencia, ética y formación continua

El profesional moderno de protección combina formación técnica, ética y liderazgo.

Las certificaciones internacionales (CPP, CPO, CSSM, etc.) garantizan estándares de excelencia, impulsando una cultura de aprendizaje permanente, investigación y compromiso con la comunidad.

“Ser profesional en protección no es tener un cargo, es sostener un estándar.”



INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS
KNOWLEDGE TO PROTECT

Carreras Contemporáneas en la Protección de Recursos

EL NUEVO ECOSISTEMA DE LA PROTECCIÓN

Carreras modernas en la protección de recursos

La industria de la protección ofrece múltiples trayectorias profesionales, adaptadas a distintos entornos y niveles de especialización. Desde la vigilancia física hasta la operación tecnológica, cada rol aporta valor a la seguridad integral de personas, información, propiedades e imagen. Principales áreas:

- Puestos fijos y control de accesos.
- Patrullaje e inteligencia operativa.
- Control de pérdidas y auditoría.
- Operaciones de monitoreo y respuesta.
- Investigación privada y análisis forense.

“Cada rol es una pieza clave en el ecosistema de la seguridad moderna.”

Carreras Contemporáneas en la Protección de Recursos

ROLES OPERATIVOS

Del terreno al control: los primeros niveles de acción

- Oficial de puesto fijo: trabaja en accesos, aeropuertos, hospitales, museos o eventos, garantizando control y prevención.
- Oficial de patrulla: observa, reporta y responde. Actúa como agente de inteligencia, consultor legal y primera línea de respuesta ante emergencias o delitos.
- Agente de control de pérdidas: combina investigación, vigilancia e interrogatorio, con oportunidades de crecimiento dentro de la industria.

“El profesionalismo comienza en el terreno, pero se construye con conocimiento.”

Carreras Contemporáneas en la Protección de Recursos

ROLES TECNOLÓGICOS Y DE MONITOREO

La central de alarmas: cerebro de la protección moderna

El operador de central o despachador monitorea sistemas de alarmas, CCTV y control de accesos. Debe comprender los distintos tipos de alarmas:

- Intrusión: detección de accesos no autorizados.
- Incendio: detección temprana de humo o calor.
- Emergencia / pánico: activadas por personas en peligro.
- Procesos: supervisan variables críticas (temperatura, presión, energía).

Una respuesta rápida y efectiva es esencial; la central es el centro de comando, control y comunicaciones.

Carreras Contemporáneas en la Protección de Recursos

ROLES DE SUPERVISIÓN Y ANÁLISIS
Del control a la inteligencia corporativa

- Inspectores y auditores: verifican comportamientos, condiciones y cumplimiento de procedimientos.
- Investigadores privados: trabajan para empresas o individuos, realizando investigaciones criminales, encubiertas o de fraude.

Estos roles requieren análisis, ética y autonomía profesional.

“La evolución del oficial de protección es su paso del resguardo a la inteligencia.”

PREGUNTAS DE AUTOEVALUACIÓN

Administración de Riesgos Empresariales de Seguridad

CPO©

Introducción a la Gestión de Riesgos

El riesgo: navegar entre el progreso y la incertidumbre

El término riesgo proviene del latín risicare, que significa “navegar entre riscos o peligros”.

Hoy, en una sociedad globalizada, las organizaciones enfrentan esa misma travesía: más bienestar, pero también más amenazas.

El sociólogo Ulrich Beck planteó que cada avance tecnológico o económico genera, al mismo tiempo, nuevas formas de riesgo: ecológico, industrial, financiero, digital.

El riesgo ya no proviene de la naturaleza, sino de las acciones y decisiones humanas.

La gestión de riesgos busca equilibrar tres objetivos esenciales de toda organización: Supervivencia – Crecimiento - Rentabilidad.

Pero históricamente, los riesgos se han administrado de forma aislada o en silos, lo que ha limitado la colaboración y la visión integral.

Hoy, el desafío es romper esa fragmentación e integrar personas, procesos e información bajo una visión convergente y estratégica del riesgo.

“Gestionar riesgos no es evitar el peligro, es aprender a navegarlo.”

OBJETIVO DEL CAPÍTULO

Describir conceptos y teorías sobre riesgos y su administración,
proponer un modelo completo para gestión técnica de riesgos y
demostrar su aplicación práctica a diferentes campos de seguridad y protección.

Necesidad de Modelos de Gestión Integrados

De los sistemas aislados a la gestión integral

Toda organización necesita un sistema de gestión que integre todos sus procesos bajo un mismo enfoque.

Estos sistemas se basan en un ciclo continuo de mejora: Planificar → Ejecutar → Verificar → Aprender (Actuar-Mejorar).

Los modelos de excelencia (ISO, EFQM, entre otros) permiten a las empresas medir su madurez y avanzar hacia la prevención, eficiencia y sostenibilidad.

Sin embargo, muchos aún operan de forma fragmentada, gestionando la calidad, la seguridad, la salud o la protección como áreas separadas.

La verdadera excelencia surge al adoptar una visión convergente, donde calidad, seguridad, salud, ambiente, información y continuidad de negocio se integran en una cultura común de prevención y mejora continua.

“No se trata de tener muchos sistemas, sino un solo propósito: proteger y mejorar continuamente.”

Estándares ISO aplicados a Protección

Principales normas ISO aplicadas a la seguridad y protección

Las normas ISO definen las mejores prácticas internacionales para gestión, control y mejora continua. Entre las más relevantes:

Norma	Enfoque principal	Aplicación en protección
ISO 9001	Calidad	Estandariza procesos y mejora continua.
ISO 14001	Medio ambiente	Control de impactos ambientales.
ISO 18788	Operaciones de seguridad privada	Define principios éticos y marcos operativos.
ISO 22399 / 22301	Continuidad de negocio	Asegura operaciones frente a eventos disruptivos.
ISO 26000	Responsabilidad social	Fortalece reputación y sostenibilidad.
ISO 27001	Seguridad de la información	Protege datos y activos digitales.
ISO 31000	Gestión del riesgo	Eje metodológico de toda protección.
ISO 45001	Seguridad y salud ocupacional	Previene incidentes y mejora el bienestar.

“Cada norma es un pilar; juntas forman el edificio de la protección integral.”

Estándares ISO aplicados a Protección

Gestión integral = eficiencia, coherencia y resultados

Integrar las normas ISO en un único sistema de gestión aporta ventajas clave:

1. Enfoque en resultados: Políticas y objetivos alineados. Coordinación consciente entre áreas. Medición de productividad y rentabilidad de las acciones preventivas.
2. Ahorro de recursos: Un solo sistema documental y comité. Menos auditorías, más eficiencia. Optimización del tiempo directivo y operativo.
3. Oportunidades de mercado: Demuestra cumplimiento y compromiso internacional. Mejora relaciones con clientes, proveedores y socios. Fortalece reputación institucional y confianza.

“Un solo sistema, múltiples beneficios: eficiencia, coherencia y reputación.”

Estándares ISO aplicados a Protección

ARES: la convergencia de todos los sistemas ISO

El modelo ARES (Administrar Rentabilidad, Entorno y Seguridad) resume los criterios esenciales para cumplir con cualquier estándar ISO aplicable a la protección.

Los 7 criterios base del modelo ARES:

1. Conocer la organización
2. Compromiso de la Dirección
3. Gestión de Riesgos
4. Planificación
5. Implementación Operacional
6. Seguimiento y Evaluación
7. Revisión, Mantenimiento y Mejora

Este enfoque interdisciplinario e integral permite armonizar los requisitos de calidad, seguridad, ambiente, salud, información y continuidad bajo un solo sistema convergente.

"ARES es el puente entre las normas ISO y la realidad operativa de la protección."

Administración de Riesgos Empresariales

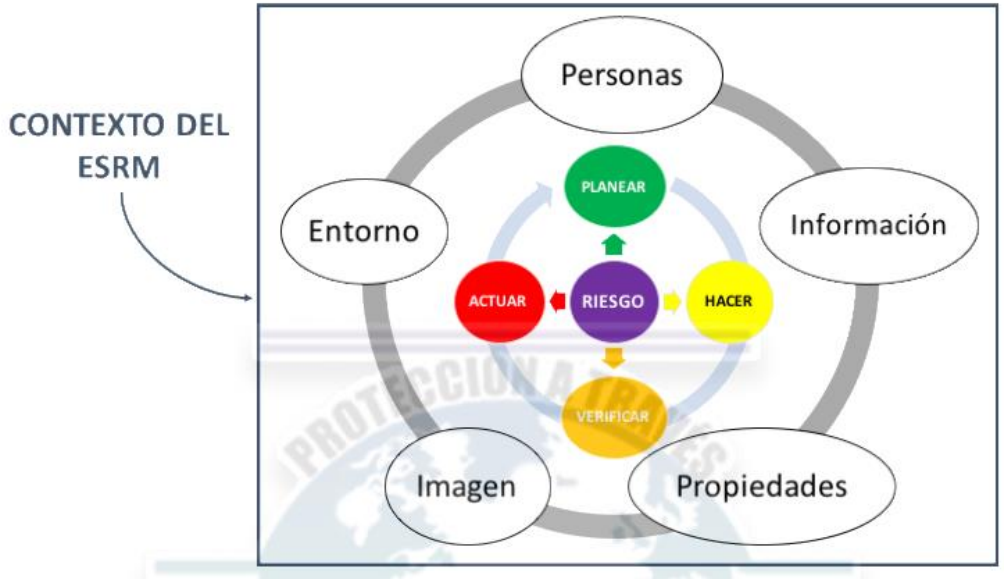
Del miedo al riesgo, a la oportunidad de gestión

Durante décadas, la administración de riesgos se ha enfocado solo en evitar pérdidas.

Sin embargo, la visión moderna del Enterprise Risk Management (ERM) entiende que cada amenaza también puede ocultar una oportunidad.

El riesgo no solo implica “lo malo que puede pasar”, sino también la posibilidad de mejorar, innovar o crecer si se lo gestiona correctamente.

La Sociedad de Administración de Riesgos (RIMS) define el ERM como: **“La cultura, procesos y herramientas para identificar oportunidades estratégicas y reducir la incertidumbre”.**



“El riesgo no es un enemigo a eliminar, sino una oportunidad a comprender.”

Administración de Riesgos Empresariales

ARES: un modelo para la gestión empresarial convergente

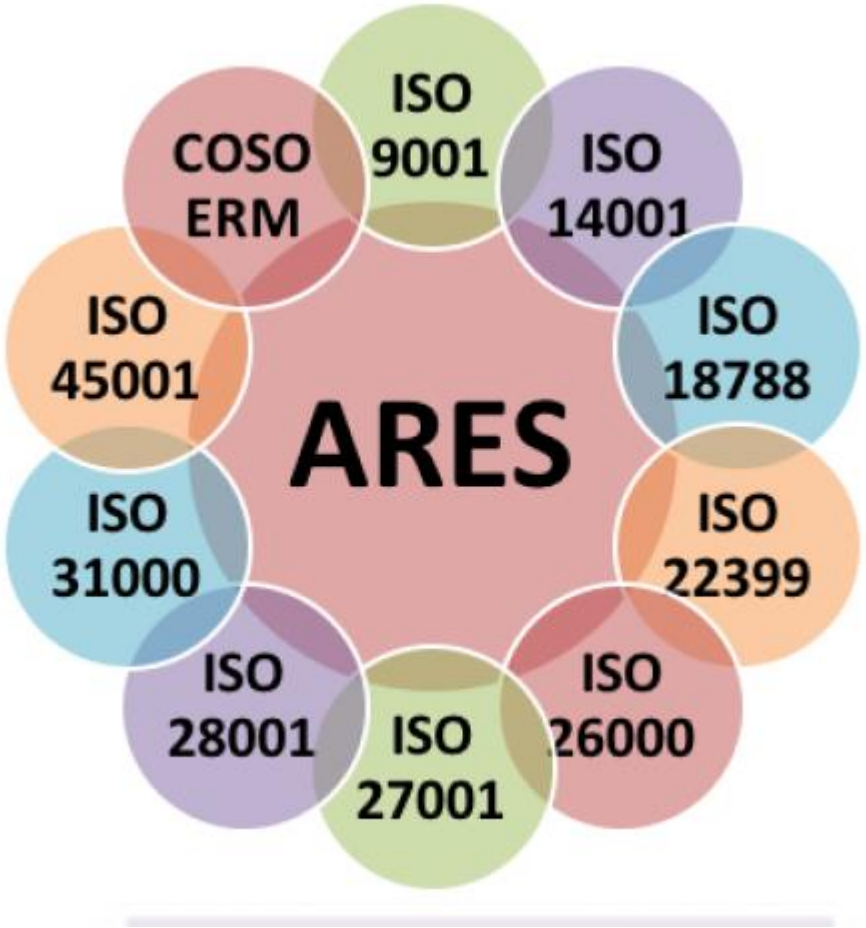
El Modelo ARES (Administrar Rentabilidad, Entorno y Seguridad) nació en 2008 como una propuesta académica que integró la visión del ESRM (Enterprise Security Risk Management) con los sistemas de gestión ISO y los modelos de calidad (QSSHE).

Su meta es alinear la protección de personas, información, propiedades, imagen y entorno con los objetivos estratégicos de la organización.

ARES se basa en:

- Integración: seguridad como parte del negocio.
- Coordinación estratégica-táctica-operativa.
- Comunicación y alineamiento entre stakeholders.
- Optimización del control de riesgos y recursos.

“ARES no reemplaza los sistemas existentes: los conecta.”



Administración de Riesgos Empresariales

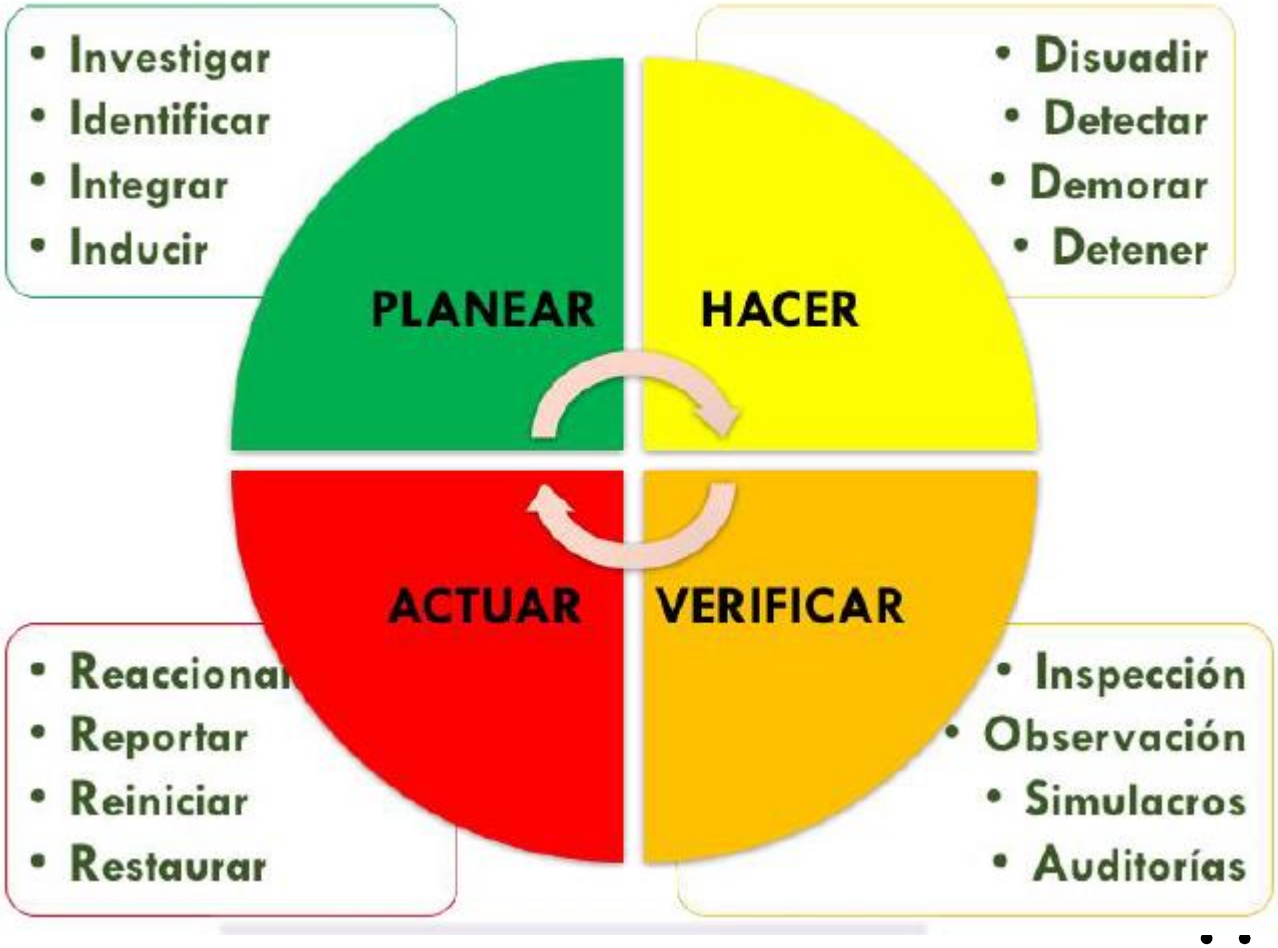
Un modelo Integrado, Integral, Multidisciplinario, Participativo y Equilibrado

1. Integrado: Alinea la gestión de riesgos con los objetivos organizacionales, integrándose al día a día de todos los procesos.
2. Integral: Protege simultáneamente personas, información, propiedades, imagen y entorno.
3. Multidisciplinario: Une saberes de administración, seguridad, salud, ambiente y psicología organizacional.
4. Participativo: Todos los miembros de la organización participan —desde la alta dirección hasta el personal operativo— fomentando una cultura de seguridad.
5. Equilibrado: Visualiza los bienes protegidos como una esfera con múltiples dimensiones, buscando armonía entre todas ellas.

Administración de Riesgos Empresariales

ARES: gestión viva y continua
ARES se implementa en cuatro fases dinámicas, aplicando la lógica del ciclo de mejora continua Planear → Hacer → Verificar → Actuar:

“ARES convierte la prevención en una práctica cotidiana.”



Administración de Riesgos Empresariales

ARES: el puente entre la protección y la estrategia empresarial

El modelo ARES transforma la administración de riesgos en una forma de vida organizacional. Sus ventajas clave:

- Integra seguridad y calidad como motores de productividad.
- Usa métodos medibles, verificables y económicamente justificables.
- Identifica peligros y oportunidades de mejora sistemáticamente.
- Protege de forma convergente los 5 pilares de valor: personas, información, propiedades, imagen y entorno.
- Fomenta una cultura organizacional basada en la mejora continua y la conciencia preventiva.

“ARES no solo gestiona riesgos, desarrolla cultura y rentabilidad.”

Fases para Implementar el Modelo ARES

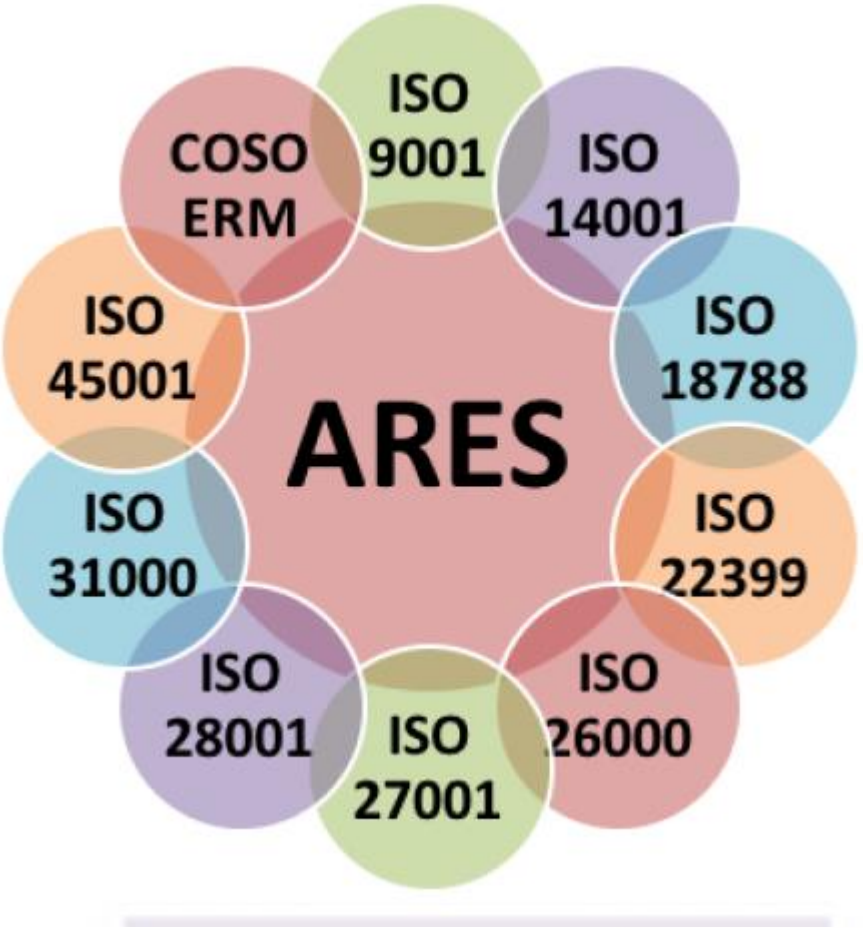
CPO©

Introducción al Modelo ARES

Implementar un modelo de administración de riesgos empresariales (ARES)

- Integrar Prevención, Mitigación y Respuesta
- Enfocado en QSSHE: Calidad, Seguridad, Salud, Ambiente, Protección, Información y Continuidad
- Basado en un espiral de mejora continua (PDCA)

Objetivo: Reducir pérdidas, controlar riesgos y fortalecer resiliencia organizacional



Las 7 fases del Modelo ARES

1. Conocer la organización
2. Políticas y procedimientos
3. Gestión de riesgos
4. Planificación
5. Implementación y operación
6. Chequeo y evaluación
7. Revisión, mantenimiento y mejora

Estas fases conforman un ciclo virtuoso, que garantiza sostenibilidad y madurez del sistema de gestión.

Fase 1: Conocer la Organización

Fase 1: Conocer la organización

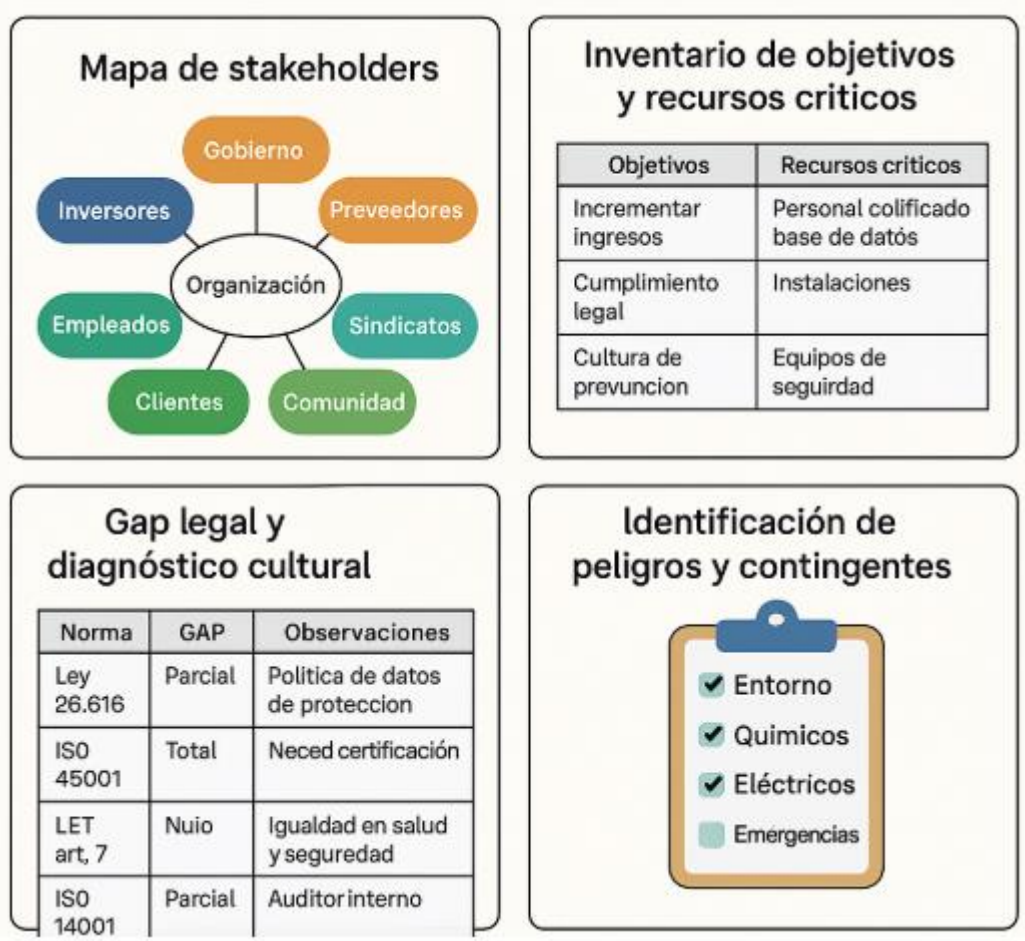
- Contexto macro (PESTEL) (factores Políticos, Económicos, Sociales, Tecnológicos, Ecológicos y Legales) del país y la industria y micro (misión, visión, objetivos, stakeholders)
- Identificar recursos críticos: Personas, Información, Propiedades, Imagen, Entorno
- Diagnóstico de cultura organizacional y madurez QSSHE

No se puede proteger lo que no se conoce; se debe "vivir la organización".

Fase 1: Conocer la Organización

Herramientas de la fase 1

- Mapa de stakeholders
- Inventario de objetivos y recursos críticos
- Gap legal y diagnóstico cultural
- Identificación de peligros y contingentes



Fase 2: Políticas y Procedimientos

Compromiso de la dirección

- Responsabilidad y liderazgo visibles
- Definir el riesgo tolerable
- Asignar un Chief Risk Officer (CRO)Comunicación interna y externa continua

La dirección es la responsable final del sistema ARES.

Ilustración 18: Pasos para iniciar el proceso

Fase 2: Políticas y Procedimientos

Política ARES (QSSHE)

Política unificada para Calidad, Seguridad, Salud, Ambiente, Protección, Información y Continuidad

Cuatro compromisos:

1. Mejora continua
2. Cumplimiento legal
3. Evaluación de riesgos tolerables
4. Comunicación efectiva

Fase 2: Políticas y Procedimientos

Procedimientos y estructura documental

- Documentar el “cómo, para que, quién, cuándo y resultado esperado”
- Mínimo 66 políticas y procedimientos obligatorios agrupados en 10 bloques
- Manual único ARES con trazabilidad total

8. PROGRAMA DE INVESTIGACIONES

- Política de Investigaciones Preventivas y Reconstructivas
- Procedimiento de Investigaciones Preventivas
- Procedimiento de Inspecciones Rutinarias de la operación
- Procedimiento de Investigaciones Reconstructivas de Incidentes y Accidentes
- Procedimiento de Levantamiento de acciones preventivas
- Procedimiento de Estadísticas de acciones preventivas
- Procedimiento de Estadísticas de pérdidas

9. PROGRAMA DE EMERGENCIAS

- Política de Planificación y Manejo de Emergencias, Crisis y Continuidad de Negocio
- Plan de emergencia, manejo de crisis y continuidad de negocio
- Procedimiento para Convenios de Apoyo de Fuerza Pública
- Procedimiento para Convenios de Ayuda Mutua
- Procedimiento de Recolección de información primaria
- Procedimiento de Red de comunicación
- Instrucciones Generales para el Manejo Emergencias
- Instrucciones específicas por Emergencia
- Instrucciones específicas para Evacuación
- Instrucciones específicas para manejo inmediato de Secuestro / Extorsión

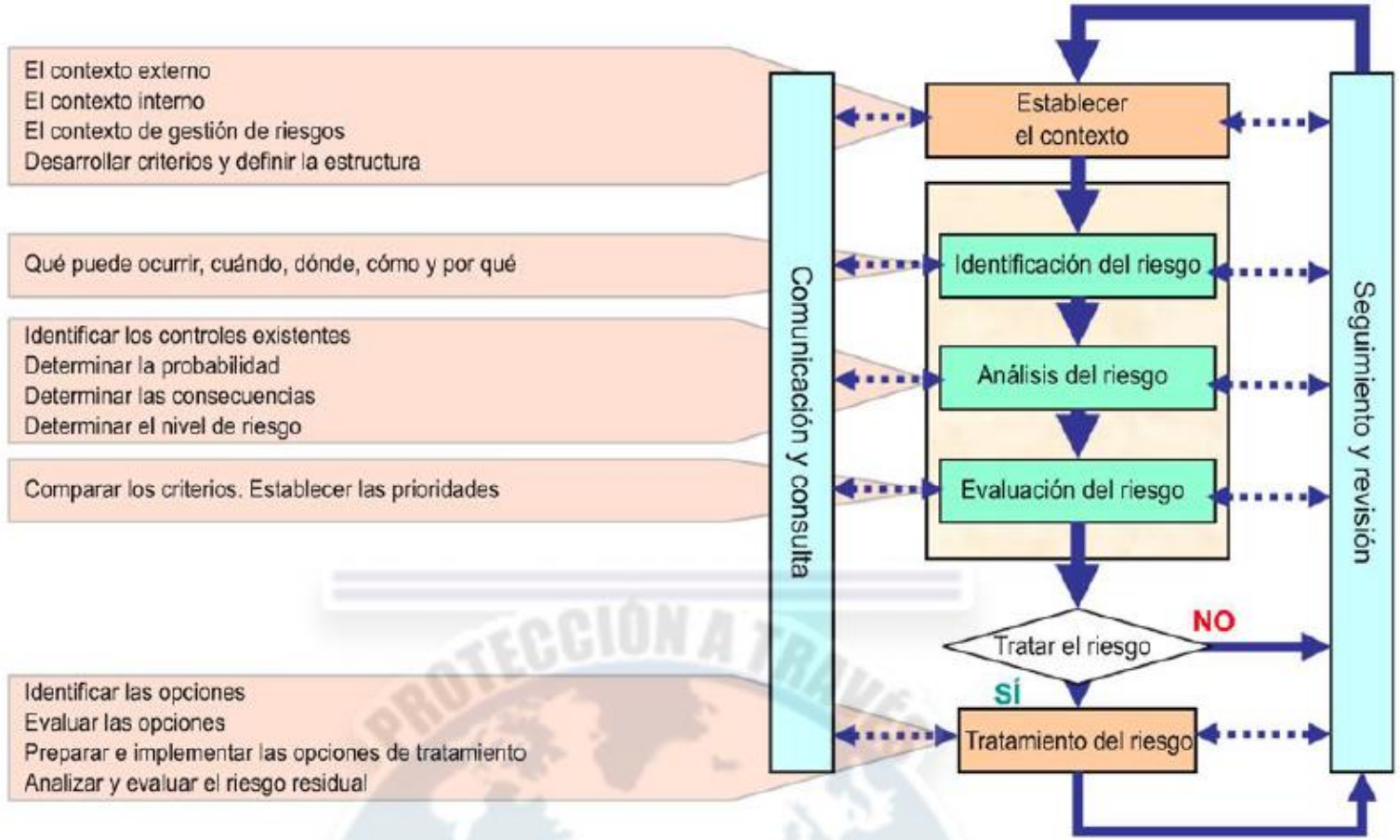
10. PROGRAMA DE COMUNICACIÓN, FORMACIÓN E INFORMACIÓN

- Política de Comunicación, Formación e Información
- Procedimiento de Inducción a Personal de Protección
- Procedimiento de Inducción a Personal en general

Fase 3: Gestión de Riesgos

Filosofía de gestión de riesgos

- Enfoque proactivo, no reactivo
- Basado en ISO 31000
- Evaluar tanto amenazas como oportunidades
- Adaptar el sistema a cambios del entorno

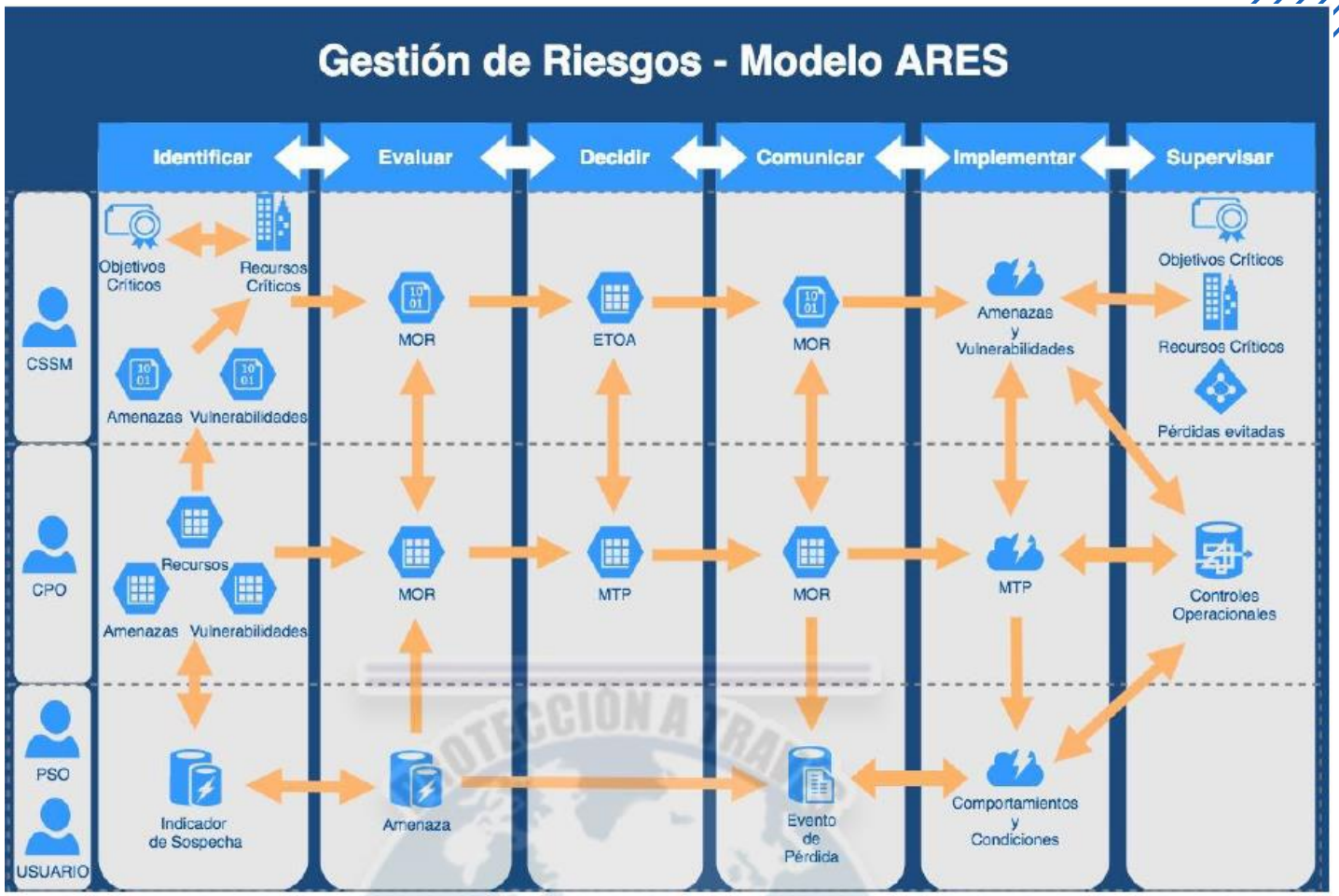


Fase 3: Gestión de Riesgos

Seis fases del proceso de gestión

1. Identificar peligros, aspectos y factores de riesgo
2. Analizar y evaluar riesgos
3. Decidir medidas de control
4. Comunicar decisiones
5. Implementar contramedidas
6. Supervisar resultados

Relacionado con el ciclo PDCA.



Fase 3: Gestión de Riesgos

Identificar Pérdidas potenciales

Identificar potenciales eventos de pérdida (peligros, aspectos y factores de riesgo)

Identificar el proceso, instalación o bien que se estudiará.

Enfocarse en recursos críticos, considerar eventos históricos e índices de gestión.

Caracterizamos su importancia para la organización en términos de necesidad, Disponibilidad, Integridad y Confidencialidad.

Carver + Shock considera: Criticalidad - Accesibilidad física al bien – Recuperabilidad (recuperar o reemplazar al bien) - Vulnerabilidades generales - Efectos de una pérdida total - Reconocibilidad (facilidad de identificarlo como blanco) - Shock para la organización

MATRIZ IDENTIFICACIÓN EVENTOS DE PERDIDAS
(Identificar recursos, amenazas y vulnerabilidades)

	PERSONAS	INFORMACIÓN	PROPIEDADES	IMAGEN	ENTORNO
P ráctica s					
E rrores					
R obo					
D esperdicio					
I ncidentes					
D años					
A ccidentes					

Fase 3: Gestión de Riesgos

Evaluación de Riesgos

Cada uno de los eventos de pérdida identificados en el paso anterior debe medirse en términos de su probabilidad e impacto. Este es un proceso cualitativo / cuantitativo.

- Debe basarse en estrategia técnica de muestreo
- Debe usar equipos certificados y calibrados
- Debe ser realizada por técnicos profesionales con las competencias adecuadas
- Incluye medición ambiental y biológica
- Debe enfocarse en objetivos críticos de protección y en grupos o áreas vulnerables

Fase 3: Gestión de Riesgos

Método Cualitativo

C - Criticalidad
A - Accesibilidad
R - Recuperabilidad
V – Vulnerabilidad
E - Efecto
R - Reconocibilidad
S - Shock

Se asigna una probabilidad medida en porcentaje de que ocurra cada evento de pérdida, factores que determinan probabilidad son:

- Nivel actual de seguridad y protección
- Vulnerabilidades existentes
- Intención del Intruso
- Utilidad para el Intruso
- Situación General del área

Probabilidad

A – Inminente.
B – Probable.
C – Posible.
D – Remoto.

Factores que determinan impacto

- Presupuesto
- Opinión pública
- Operaciones de la empresa
- Moral del personal
- Sistema general de seguridad y protección

Impacto

I – Extremo.
II – Alto
III – Medio
IV – Común

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 recursos II	1	2	3	4
	Medio Puede causar daño menor, daño a la propiedad o degradación al uso eficiente de recursos. III	2	3	4	5
	Común Presenta amenaza mínima a salud, protección personal, a la, propiedad, o uso eficiente de recursos. IV	3	4	5	5

Fase 3: Gestión de Riesgos

Método Cuantitativo
Entre los más conocidos podemos mencionar el Modelo EASI para seguridad física de
instalaciones, o los modelos RULA, NIOSH, OWAS para estudios ergonométricos.

Para **estimar las vulnerabilidades** se puede utilizar los elementos de medición aportados por el
modelo EASI, midiendo la probabilidad de vulnerabilidad, interrupción y detección, mediante
sencillas fórmulas matemáticas:

Las amenazas y vulnerabilidades deben ser estimadas cuantitativamente.
Este estudio tiene tres fines:

1. Caracterizar la amenaza
2. Identificar el estado actual de la seguridad y Protección
3. Especificar los perfiles de “eventos de pérdidas”

Fase 3: Gestión de Riesgos

R = P x K

R = Riesgo; P = Probabilidad; K = Criticidad

PdR = Prt * PrR

PrT = Probabilidad tiempo de respuesta; PrR = Probabilidad de recursos de Respuesta

Si Trt ≥ TR => PrT = 1 (100%); Si rR ≥ rA => PrR = 1 (100%)

Trt = Tiempo de retardo; TR = Tiempo respuesta; rR = Recursos respuesta; rA = Recursos Amenaza

P = PA x PV

PA = Probabilidad de amenaza; PV = Probabilidad de vulnerabilidad

PV = 1 – Pi

Pi = Probabilidad de Interrupción

Pi = Pdt * Pdr

Pdt = Probabilidad Detección; Pdr = Probabilidad Detención

Pdt =1 – (Pndt1 * Pndt2 * … Pndtn) ; Pdt =1-(1-Pdt1 * 1-Pdt2 * … 1-Pdtn)

Pndt(n) = Probabilidad NO detección c/ elemento; Pdt(n) = Probabilidad detección c/ elemento

Pdr = Pdc * PdR

Pdc = Probabilidad de comunicación; PdR = Probabilidad de Respuesta

Fase 3: Gestión de Riesgos

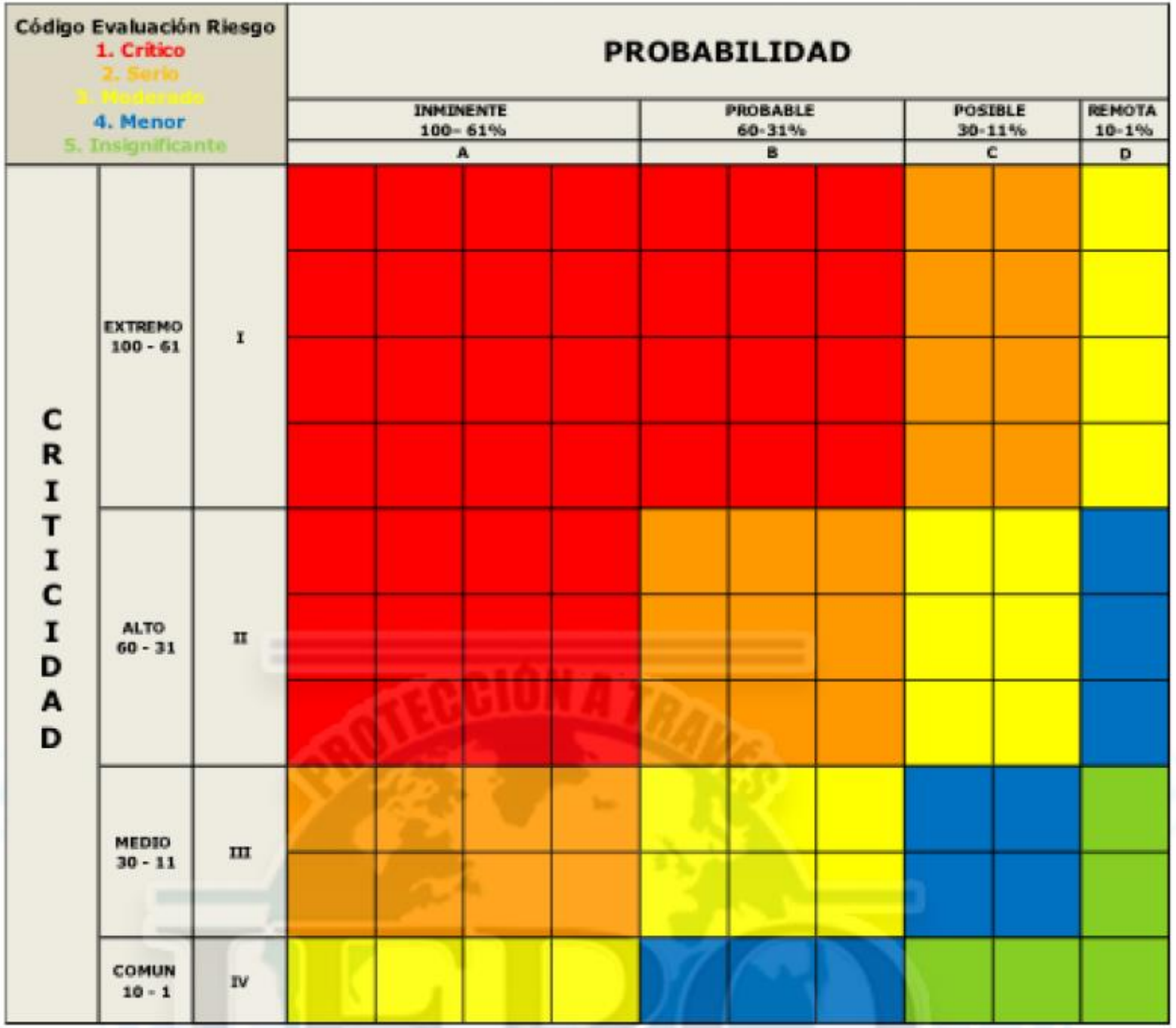
El reporte asociado a la matriz cuantitativa de riesgos muestra numérica y gráficamente los eventos de pérdida que poseen mayor riesgo, cuáles se repiten o están interrelacionados.

- El impacto y probabilidad debe ser estimado cuantitativamente en base a los datos obtenidos y la criticidad es calculada en base al mayor riesgo posible dividido entre el riesgo tolerable modificado por la experiencia operacional.

- Impacto previsible que se darían en el caso de acaecer el evento de pérdida, medido en unidad de moneda corriente $.

- Probabilidad de que el evento de pérdida ocurra, corregida por la exposición al riesgo a que se ven sometidos los bienes en cuanto a su frecuencia. La probabilidad se mide en %
- La criticidad se mide en relación con el valor de riesgo tolerable previamente definido en % del valor de riesgo tolerable.

REPORTE MATRIZ OPERACIONAL DE RIESGO CUANTITATIVA



Fase 3: Gestión de Riesgos

Decisión sobre Medidas de Control
Estimar la efectividad de los controles y contramedidas existentes actualmente:

- Cumplimiento técnico legal
- Control de Ingeniería
- Control en conducta del hombre
- Control en gestión administrativa

- Recomendar siempre evitar todo riesgo innecesario o que difícilmente pueda ser manejado.
- Los riesgos que no se puedan evitar deben ser evaluados a profundidad.
- La recomendación de asumir, distribuir o transferir debe estar acompañada de un análisis financiero detallado.

En primer lugar debemos **definir la estrategia general** prevista para la administración del riesgo; las opciones frente al riesgo puro son cuatro:

1. Evitar
2. Transferir
3. Optimizar
4. Aceptar

Fase 3: Gestión de Riesgos

		PROBABILIDAD			
		Inminente A	Probable B	Posible C	Remota D
IMPACTO	Extremo I	Evitar	Evitar Transferir	Transferir Optimizar	Transferir Optimizar
	Alto II	Evitar Transferir	Transferir Optimizar	Optimizar	Optimizar
	Medio. III	Transferir Optimizar	Optimizar	Optimizar	Optimizar Aceptar
	Común IV	Optimizar	Optimizar	Optimizar Aceptar	Aceptar

Fase 3: Gestión de Riesgos

Comunicar las Decisiones

Realizando sesiones de sociabilización a todas las partes interesadas podemos retroalimentar el sistema.

Es importante aclarar que las normas deben ser sociabilizadas para poder ser utilizadas; esto implica un proceso continuo de retroalimentación.

Fase 3: Gestión de Riesgos

Implementar Contramedidas

Trabajo técnico donde se busca equilibrar la relación costo / beneficio de las contramedidas y los riesgos valorados.

Las contramedidas son de tres tipos: Métodos, Tecnología y Personal, y deben asignarse en cada uno de los 12 subprocesos de protección:

1. Las soluciones de Métodos (Ej Procedimientos) generalmente tienen el menor costo y mayor eficiencia, más aún si son preventivas.
2. La Tecnología tiene la mayor fiabilidad, aunque la inversión inicial puede ser alta, el retorno a largo plazo es también mejor.
3. Asignar Personal posee costos elevados y dificultad de implementación, especialmente si es encargado de reacción.

El objetivo de un sistema de Gestión Integrada de Riesgos es prevenir - reduciendo la probabilidad de ocurrencia de un determinado riesgo, como también mitigar el impacto en caso de que dicho riesgo llegue a materializarse y finalmente responder reduciendo las pérdidas ocasionadas mediante actuaciones frente a cambios previsibles y actuaciones frente a cambios imprevistos.

Fase 3: Gestión de Riesgos

Supervisar Resultados

Una vez implementadas las contramedidas, se debe hacer seguimiento sobre su efecto en el riesgo calculado originalmente, siendo resultados posibles:

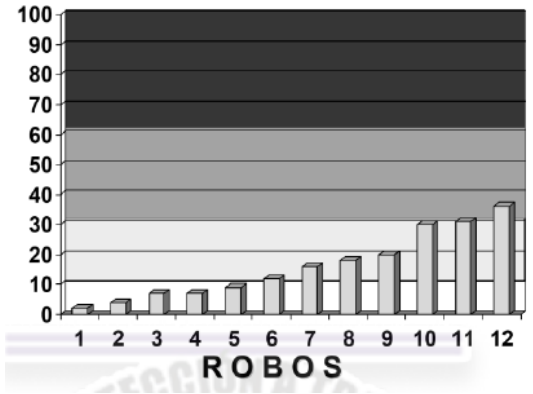
- El riesgo disminuyó: En cuyo caso debe retomarse el proceso desde el paso 2 (Análisis de Riesgo) para medirlo nuevamente y decidir estrategias de administrar ese riesgo residual (transfiriéndolo, reduciéndolo, distribuyéndolo o aceptándolo).

- El riesgo no disminuyó: En cuyo caso debe retomarse el proceso desde el paso 1 (Estudio de Seguridad), ya que probablemente no se identificó adecuadamente el peligro o las vulnerabilidades

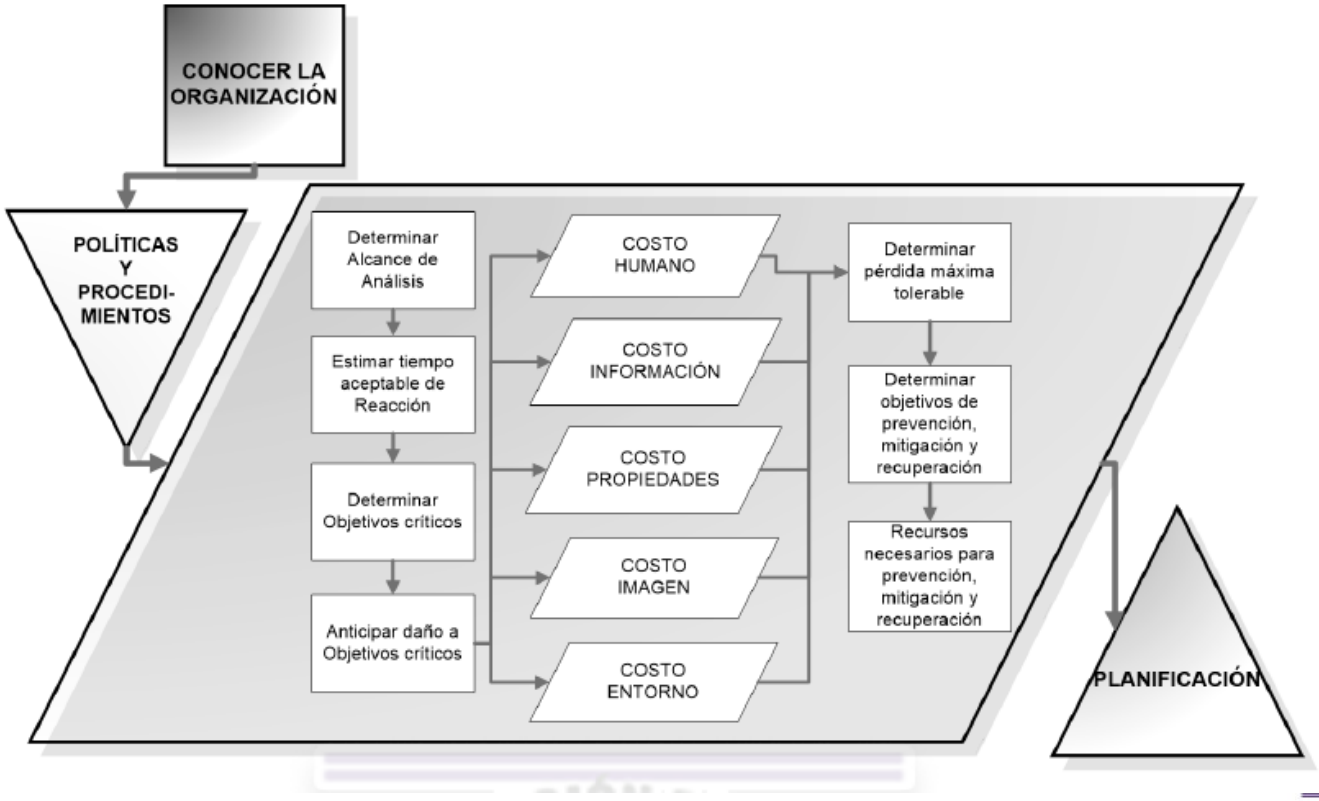
Lo que no se mide no se puede administrar y se pierde en el tiempo.
El seguimiento y mejora continua de las contramedidas debe ser evaluado por su efectividad

Fase 3: Gestión de Riesgos

Los registros históricos de riesgos deberán ser contrastados y Monitoreados.



También se debe tener presente el Análisis Económico del Riesgo



Fase 4: Planificación

Planificar es medir

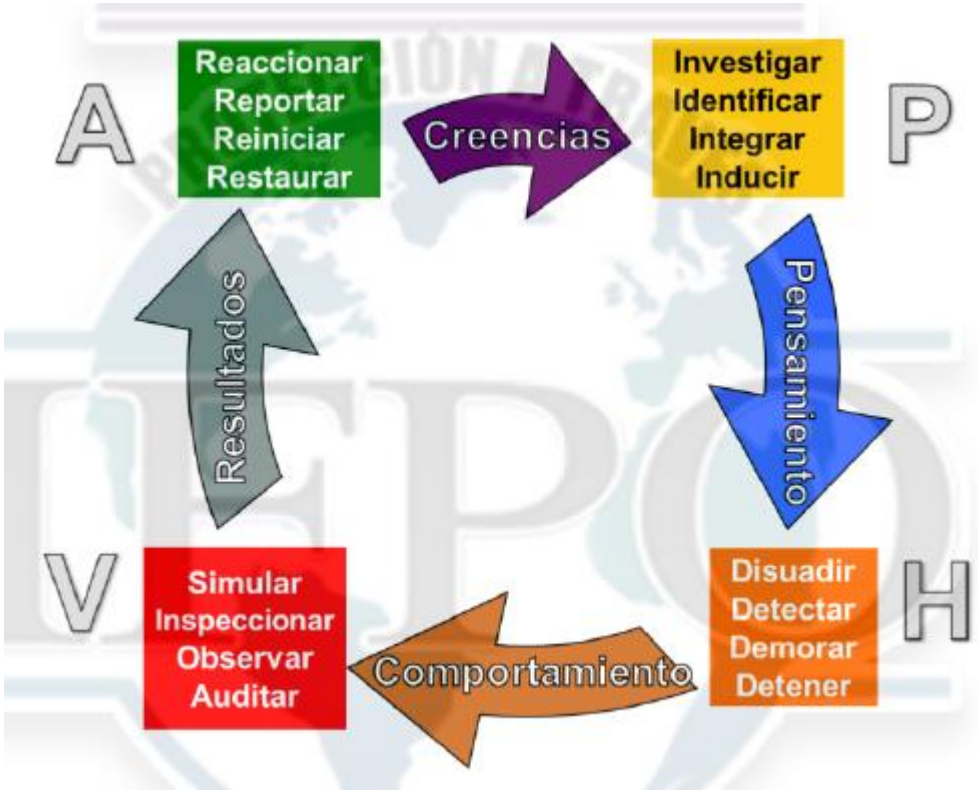
- “No se puede administrar lo que no se puede medir”
- Definir indicadores de gestión SMART
- Alinear objetivos con metas QSSHE
- Establecer planes de acción e indicadores de desempeño

Indicadores de gestión ARES

- Financieros (14)
- Administrativos (6)
- Técnicos (14)
- Procesos operativos (12)
- Talento humano (5)

Fase 5: Implementación Operacional

Para su implementación operacional el modelo ARES sigue el esquema de la mejora continua popularizado por las normas y estándares ISO:



Fase 5: Implementación Operacional

Implementación de la gestión se realiza a 3 niveles:

- ESTRATÉGICO: Proceso detallado, involucra investigación de datos disponibles, uso de diagramas y herramientas de análisis y pruebas formales o seguimiento de largo alcance de los peligros asociados con la operación evaluar los riesgos.
- TÁCTICO: Aplicación del proceso de seis pasos;
- OPERATIVO: Un análisis continuo muchas veces realizado de manera oral o mental “algo rápido”;

Fase 5: Implementación Operacional

Nivel Operativo

Es aplicado por todos en la organización para su trabajo diario, es compromiso de todos:

1. Identificar indicadores de sospecha.
2. Reportar potenciales amenazas.
3. Actuar de acuerdo a lo que permite su labor y las circunstancias

El rol operativo del oficial de seguridad debe enfocarse en la prevención

Fase 5: Implementación Operacional

Preguntas fundamentales e indicadores de sospecha

CONDICIONES	ACTOS
¿Qué es eso? • Cosas no corresponden	**¿Qué tiene él/ella/ellos?** • Personas no tienen lo que deberían
¿Cómo hace eso? • Cosas no hacen lo que deberían	**¿Cómo hace él/ella/ellos?** • Personas haciendo lo que no corresponde
¿Quién tiene eso? • Cosas sin su custodio legítimo	**¿Quién es él/ella/ellos?** • Personas no son lo que deberían
¿Cuándo es eso? • Cosas fuera de tiempo	**¿Cuándo es él/ella/ellos?** • Personas fuera de turno
¿Dónde está eso? • Cosas fuera de su lugar	**Dónde está él/ella/ello?** • Personas no están donde deberían

Fase 5: Implementación Operacional

Antes de actuar es importante entender la fase en que podría estar desarrollándose un potencial ataque:

Fase 5: Implementación Operacional

Nivel Táctico

Es aplicado por los miembros del equipo de Supervisión y Gerencia Media, personas que idealmente poseen al menos la certificación CPO, y estarán capacitados para llevar a cabo el proceso de mejora en todas sus fases.

Fase 5: Implementación Operacional

Nivel Estratégico

La era de la seguridad de Barreras, Candados y Guardias (Seguridad Reactiva) ha terminado.
El objetivo actual del sistema de Protección es mejorar nuestras capacidades de:

1. PREVENCIÓN
2. MITIGACIÓN
3. SUPERVISIÓN
4. RESPUESTA

La implementación estratégica debe ser desarrollada por gerentes de protección con las competencias del Certificado en Supervisión y Gerencia de Protección – CSSM.

Fase 6: Chequeo y Evaluación

La evaluación continua se ejecuta mediante tres procesos:

- Monitoreo continuo del Sistema de Gestión.
- Manejo de No Conformidades y de Acciones Preventivas o Correctivas
- Inspecciones y Auditorías

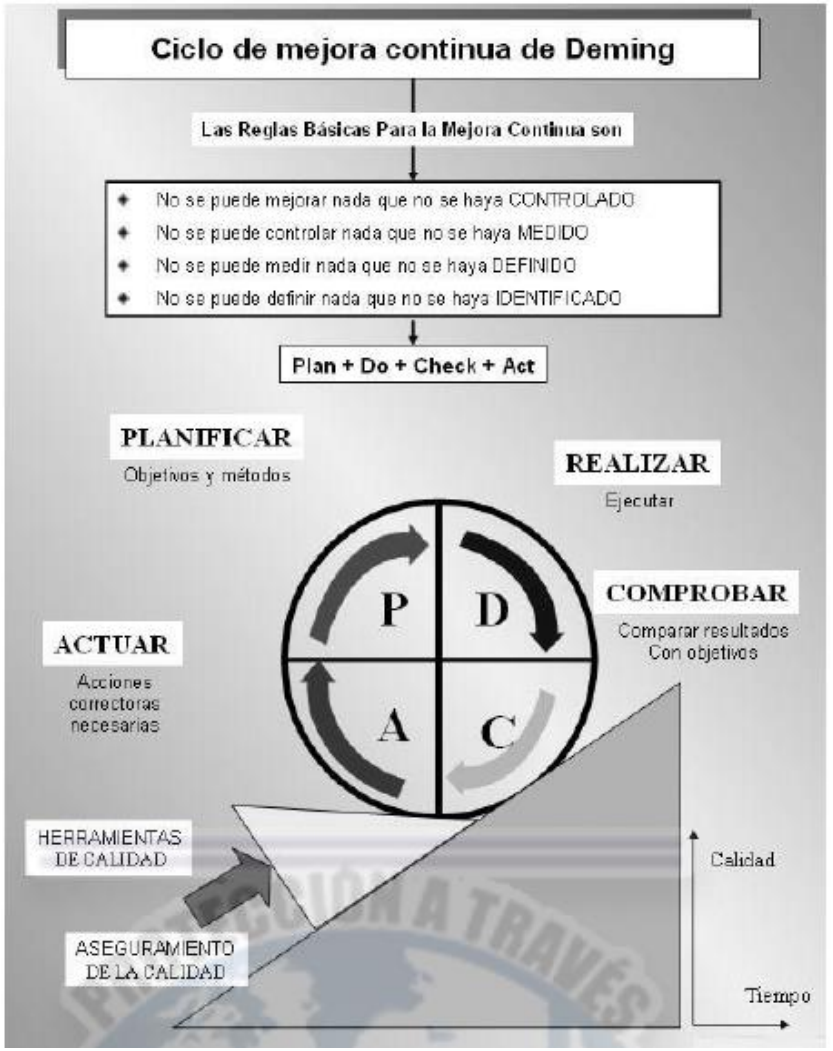
Beneficios de la supervisión ARES

- Uso eficiente de recursos
- Identificación de áreas críticas
- Intervención inmediata
- Gestión proactiva y basada en datos

Fase 7: Revisión, Mantenimiento y Mejora

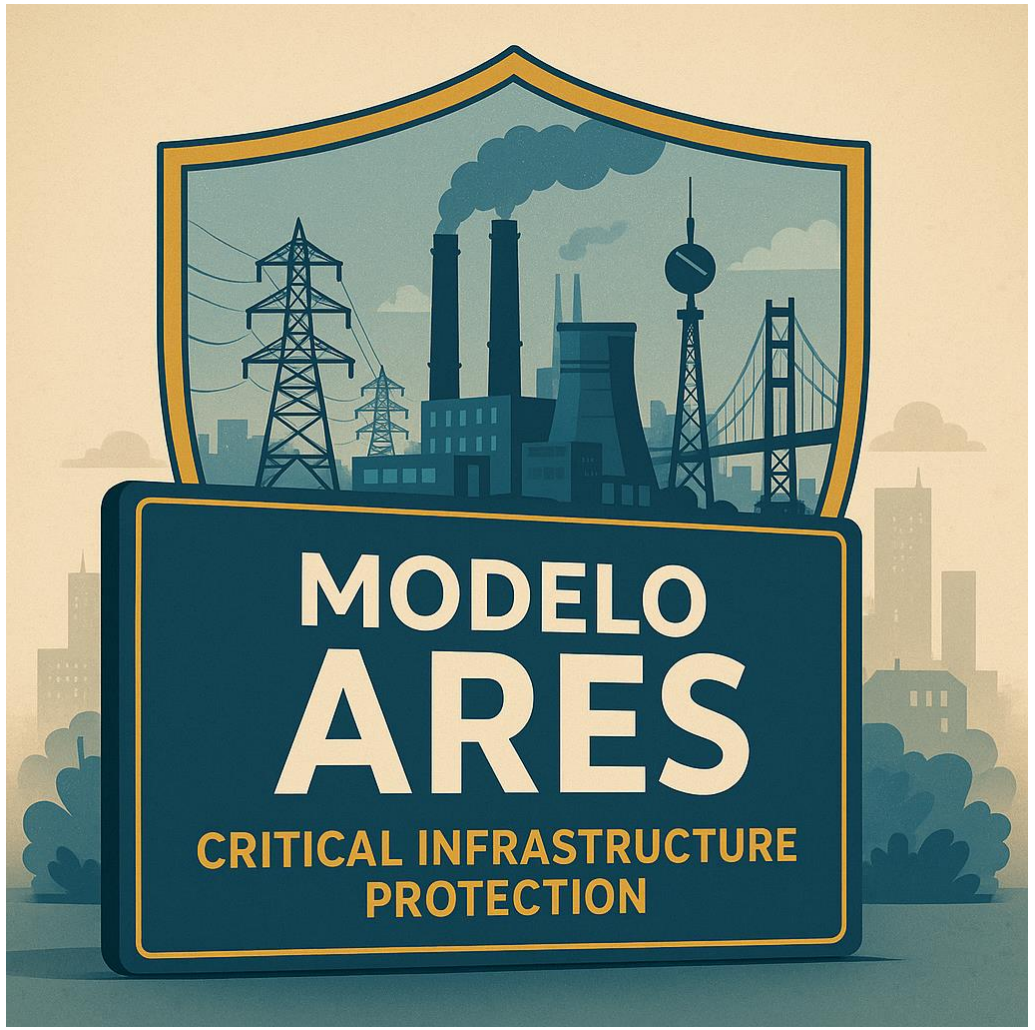
Revisión y mejora continua

- Revisar política, objetivos y resultados
- Incorporar lecciones aprendidas
- Benchmarking con mejores prácticas
- Actualizar procesos y capacitar continuamente



Beneficios del Modelo ARES

- Identificar y manejar los riesgos cruzados de la empresa
- Alinear el riesgo tolerado y la estrategia.
- Reducir sorpresas y pérdidas operativas
- Mejorar las decisiones de respuesta a los riesgos
- Recursos



PREGUNTAS DE AUTOEVALUACIÓN