OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

UNIDAD I

RIESGOS, CONCEPTOS CLAVE E HISTORIA

Manual del Alumno — Resumen Fiel al Manual Oficial CPO®-IFPO v6.0

Certified Protection Officer (CPO®) - IFPO

Con recuadros de adaptación a la Ley 21.659 y DS 209 — República de Chile

2026

TABLA DE CONTENIDOS

CAPÍTULO 1 — CONCEPTOS CLAVE 3

Introducción 3

Conceptos Asociados a Riesgo 4

El Proceso de la Gestión de Riesgos (ISO 31000) 5

Tratamiento de Riesgos (ETOA) 6

Control de Pérdidas (Teoría WAECUP y Categorías PERDIDA) 6

El Entorno de Control 7

Prevención del Delito mediante el Diseño del Entorno (CPTED) 7

Otros Conceptos Clave (Mando y Autoridad) 8

Conclusión, Referencias y Preguntas de Auto Estudio 9

CAPÍTULO 2 — MANEJO OPERACIONAL DEL RIESGO (MOR) 11

Introducción 11

Matriz de Evaluación de Riesgo (Matriz MOR) 11

Las Seis Fases del Proceso MOR 13

MOR y Modelo ARES 13

Conclusión, Referencias y Preguntas de Auto-Estudio 14

CAPÍTULO 3 — ADMINISTRACIÓN DE RIESGOS EMPRESARIALES DE SEGURIDAD 16

Introducción a la Gestión de Riesgos 16

Compartamentalización de Riesgos 16

Necesidad de Modelos de Gestión Integrados 17

Estándares ISO Aplicados a Protección 17

Origen del Modelo ARES 17

Características Fundamentales del Modelo ARES 18

Implementación Operacional (Niveles Operativo, Táctico, Estratégico) 19

Administración de Riesgos y Seguros 20

Conclusión y Referencias 20

CAPÍTULO 4 — EVOLUCIÓN DE LA SEGURIDAD Y PROTECCIÓN DE BIENES 22
Introducción y El Ciclo de la Historia 22
Periodos Bíblicos y Desarrollo en Tiempos de Guerra 22
Periodo Anglosajón y Periodo Moderno (1500-1900) 23
Los Inicios en Estados Unidos y la II Guerra Mundial 23
Economía, Tendencias de Mercado y Terrorismo 24
Historia de las Empresas de Protección 25
Trayectoria al Profesionalismo y Carreras Contemporáneas 25
Referencias y Preguntas de Auto Estudio 26
ANEXO — SÍNTESIS DE ADAPTACIÓN A CHILE (Ley 21.659 y DS 209) 27

Nota metodológica: Este manual constituye un RESUMEN del contenido oficial del Manual de Capacitación "Oficial Certificado de Protección CPO© Versión 6.0" (IFPO Hispanoamérica, 2021), estructurado siguiendo fielmente sus cuatro capítulos originales. Cada sección conserva los conceptos, terminología y modelos propios de IFPO, e incorpora recuadros de adaptación práctica a la legislación chilena vigente (Ley 21.659 y Decreto Supremo 209 de 2024).

CAPÍTULO 1 — CONCEPTOS CLAVE

Introducción

Los RECURSOS que protegemos son "bienes" materiales o intangibles que siempre tienen valor para su propietario; si son robados, perdidos, destruidos o dañados, alguna organización o individuo sufrirá una pérdida. Los recursos a proteger tienen cuatro clasificaciones básicas, en orden de prioridad:

- PERSONAS: Capital humano — trabajadores, contratistas, clientes, visitantes, la comunidad.
- INFORMACIÓN: Capital intelectual — información propietaria, datos confidenciales, planes.
- PROPIEDADES: Capital financiero — muebles e inmuebles con características físicas.
- IMAGEN: Capital comercial — reputación pública frente a clientes y posicionamiento del negocio.

Estas cuatro categorías dan origen a los subsistemas de control de pérdidas que estructuran las doce unidades completas del programa CPO®, y que en esta Unidad I se estudian desde su fundamento conceptual.

> **CL Adaptación a Chile**
> La Ley 21.659 exige que todo Plan de Seguridad Privada identifique explícitamente los recursos críticos a proteger (personas, información, propiedades e imagen) como parte del Estudio de Seguridad presentado ante la Subsecretaría de Prevención del Delito (SPD), replicando esta misma lógica de clasificación de recursos del modelo IFPO.

Conceptos Asociados a Riesgo

El RIESGO se define como "incertidumbre" frente a la consecución de objetivos; es la consecuencia probable de eventos de pérdida generados por fuentes de riesgo.

CONCEPTO	DEFINICIÓN (Manual IFPO)
Fuente de Riesgo	Factor (tangible o intangible) con potencial de crear incertidumbre en la consecución de objetivos. Requiere de un peligro o amenaza activado por vulnerabilidades.
Vulnerabilidad	Comportamientos y condiciones que se desvían de la norma ("sub-estándar"). Se habla de "factores de riesgo" en riesgos dinámicos y de "vulnerabilidades" en riesgo puro.
Peligro	Hace referencia a una situación.

Amenaza	Individuo o grupo de personas con elementos de capacidad e intención que lo califican para causar pérdida en los recursos.
Perfil del Evento de Pérdida	Se construye al establecer la relación unívoca entre una amenaza y sus vulnerabilidades correspondientes.
Riesgo Puro / Riesgo de Seguridad	Probabilidad de que una amenaza tome ventaja de las vulnerabilidades del recurso y esto cause un impacto (consecuencia negativa o pérdida).

El impacto puede estimarse de manera cualitativa (SEVERIDAD) o cuantificarse, por ejemplo, en términos monetarios (CRITICALIDAD).

El Proceso de la Gestión de Riesgos

El proceso usado por IFPO para gestionar los riesgos puros sigue un ciclo continuo de seis pasos interrelacionados, plenamente alineado con la norma ISO 31000:

Paso 1 — Identificar: Mediante un estudio de seguridad se asocian los recursos con sus fuentes de riesgo: pasos de la operación, recursos críticos, amenazas y vulnerabilidades, y posibles eventos de pérdida.

Paso 2 — Evaluar: Se asigna el evento a una de las siete categorías de pérdida; se estima probabilidad e impacto; se comparan los riesgos usando el Código de Evaluación de Riesgo (CER/RAC) para priorizarlos.

Paso 3 — Decidir: Se prioriza comenzando por el riesgo más serio y se escoge la estrategia de tratamiento (ETOA), seleccionando las medidas de control de pérdidas.

Paso 4 — Comunicar: Se reporta el resultado del análisis, se consulta a las partes interesadas y se comunican los acuerdos logrados.

Paso 5 — Implementar: Se ejecutan las medidas de control mediante métodos (políticas, procedimientos), tecnología (ingeniería, seguridad física, EPP) y personal.

Paso 6 — Supervisar: Se evalúa la ejecución del plan, se verifica la efectividad de las contramedidas y se hace seguimiento de actos, condiciones y cambios del escenario.

CL Adaptación a Chile

El DS 209 exige que el Estudio de Seguridad de toda entidad obligada documente un ciclo equivalente de identificación, evaluación y tratamiento de riesgos, replicando el estándar ISO 31000 que aquí describe IFPO — por lo que dominar este proceso de 6 pasos es directamente aplicable a la elaboración de planes exigidos por la SPD.

Tratamiento de Riesgos

IFPO organiza los cuatro métodos para tratar riesgos según el acrónimo ETOA:

- **E — Evitar: Eliminar completamente el riesgo cambiando de actividad o trasladando el bien a un escenario más favorable.**
- **T — Transferir: Compartir el impacto de las pérdidas mediante seguros, asociación financiera o subcontratación.**
- **O — Optimizar: Aprovechar el riesgo en busca de oportunidades, controlando exposición, vulnerabilidades o consecuencias.**
- **A — Aceptar: Decisión informada de aceptar el riesgo cuando éste se encuentra dentro de límites tolerables.**

No se puede asegurar que un riesgo sea evitado totalmente mediante medidas de protección; la prevención absoluta resulta impráctica cuando es demasiado costosa o inhabilita la función del recurso protegido.

Control de Pérdidas

Según la teoría WAECUP (Bottom y Kostanoski), las pérdidas pueden tener múltiples orígenes. IFPO estandariza siete categorías de riesgo mediante el acrónimo PERDIDA:

- **P — Prácticas no profesionales / no éticas — fraude, ocultación, conflictos de interés, crimen de cuello blanco.**
- **E — Error en la planeación o ejecución.**
- **R — Robo y diversos comportamientos criminales.**
- **D — Desperdicio y desorden de recursos, tiempo, materiales, mano de obra y espacio.**
- **I — Incidentes y desviaciones de normas que aparentemente no causan daño.**
- **D — Desastres naturales e intencionales, incluye sabotaje.**
- **A — Accidentes y enfermedades laborales que causan lesión o compensaciones laborales.**
-

El Entorno de Control

El control de pérdidas se ejecuta mediante un ciclo de cuatro fases —Planear, Hacer, Verificar, Actuar—, alineado a la mejora continua ISO. La fase PLANEAR identifica potenciales eventos de pérdida e integra medidas de control; la fase HACER despliega actividades de disuasión, demora, detección y detención de agresores; la fase VERIFICAR involucra simulacros, inspecciones y auditorías; y la fase ACTUAR mide la capacidad de reacción, reporte, recuperación y reinicio de operaciones tras un incidente.

Prevención del Delito mediante el Diseño del Entorno — CPTED

El CPTED (Crime Prevention Through Environmental Design), acuñado por el Dr. C. Ray Jeffrey en 1971, es una teoría de control de pérdidas basada en influenciar apropiadamente el entorno físico. Incluye seis fundamentos:

1. Defensa en Profundidad: Círculos concéntricos de contramedidas en perímetro, estructura y recurso.

2. Territorialidad: Marcación de límites y líneas de propiedad bien establecidas (señalética, percepción de pertenencia).

3. Vigilancia: Natural (áreas despejadas), electrónica (CCTV) u organizada (patrullajes de personal de protección o fuerza pública).

4. Control de Accesos: Seis pasos: validar identidad, confirmar derecho de acceso, registrar, inspeccionar propiedades, entregar información y restricciones, permitir el acceso.

5. Refuerzos Positivos: Esfuerzo por alejar a las personas de actividades criminales, involucrándolas en actividades legítimas.

6. Mantenimiento: El desorden y la suciedad causan pérdidas; la reparación y el orden continuo disuaden el crimen.

> **CL Adaptación a Chile**
> CPTED es hoy exigido implícitamente en Chile a través de ordenanzas municipales de seguridad urbana y es una de las herramientas más recomendadas por Carabineros de Chile en sus programas de prevención situacional. Para instalaciones críticas (mineras, portuarias, retail), aplicar los 6 fundamentos CPTED reduce directamente el riesgo evaluado en el Estudio de Seguridad exigido por el DS 209.

Otros Conceptos Clave

Todo oficial de protección debe comprender los siguientes conceptos de mando y autoridad:

Delegación de Autoridad: Un superior delega autoridad a subordinados para repartir la carga de trabajo; la responsabilidad no puede ser delegada totalmente.

Administración por Excepción: En situaciones de emergencia o delicadas, es recomendable que el superior inmediato asuma nuevamente el control.

Cadena de Mando: Las comunicaciones deben circular hacia arriba, hacia abajo u horizontalmente, siempre a través de una jerarquía organizada; nunca debe romperse.

Unidad de Mando: Ningún subordinado debe reportar o seguir órdenes de más de un superior, para evitar confusión.

Extensión del Control: Número de subordinados que un superior puede supervisar adecuadamente: relación recomendada 1:3 para trabajos de alta responsabilidad y 1:12 para trabajos operativos rutinarios.

Conclusión del Capítulo 1

Los oficiales de protección deben estar familiarizados con estos conceptos y estándares de la profesión; esta es la diferencia entre el empirismo y la verdadera profesionalización. El control de pérdidas consiste en establecer un entorno que refuerce el cumplimiento de restricciones, disminuyendo la probabilidad y el impacto de las pérdidas mediante la modificación de amenazas y vulnerabilidades.

Referencias a Consultar

- Norma ANSI/ASIS SPC.1-2009 — Resiliencia organizacional, sistemas de gestión de la seguridad, preparación y continuidad.
- International Foundation for Protection Officers (IFPO). Certified in Security Supervision and Management (CSSM).
- International Organization for Standardization (ISO). The new ISO 31000 keeps risk management simple.
- Maggio, E. J. (2009). Private security in the 21st century: Concepts and applications.

Preguntas de Auto Estudio — Capítulo 1

1. ¿Cuáles son las cuatro clasificaciones de recursos a proteger según IFPO? Ordénelas por prioridad.

2. Defina, con sus propias palabras, la diferencia entre "peligro" y "amenaza".

3. Enumere los seis pasos del proceso de gestión de riesgos y explique brevemente cada uno.

4. ¿Qué significa el acrónimo ETOA? Desarrolle cada componente con un ejemplo propio.

5. ¿Qué representa el acrónimo PERDIDA en la teoría de Control de Pérdidas?

6. Enumere y explique los seis fundamentos del CPTED.

7. Explique la diferencia entre "cadena de mando" y "unidad de mando".

CAPÍTULO 2 — MANEJO OPERACIONAL DEL RIESGO (MOR)

Introducción

El Manejo Operacional del Riesgo (MOR) es una metodología originalmente desarrollada y usada en planeamiento y operaciones militares, igual de efectiva en operaciones de protección cotidianas. El proceso MOR subsiste en tres niveles: Inmediato (revisión mental rápida), Deliberado (aplicación del proceso de pasos para gestionar riesgos) y En Profundidad (proceso estratégico con evaluación completa, investigación de datos, diagramas y pruebas formales).

El MOR incorpora cuatro principios:

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

Matriz de Evaluación de Riesgo (Matriz MOR)

La Matriz MOR provee un marco consistente para múltiples aplicaciones, combinando el IMPACTO DE PÉRDIDA (medición de la peor consecuencia creíble) con la PROBABILIDAD DE PÉRDIDA (grado de lo probable que un evento ocurra).

NIVEL DE IMPACTO	DESCRIPCIÓN
I — Extremo	Puede causar muerte, pérdida de una instalación/recursos o daño grave.
II — Alto	Puede causar daño severo, enfermedad, daño a la propiedad o degradación del uso de recursos.
III — Medio	Puede causar daño menor, daño a la propiedad o degradación menor del uso de recursos.
IV — Común	Presenta amenaza mínima a la protección personal, salud, propiedad o uso de recursos.

NIVEL DE PROBABILIDAD	DESCRIPCIÓN
A — Inminente	Ocurrencia inmediata o en corto plazo; se espera que ocurra frecuentemente.
B — Probable	Probablemente ocurrirá alguna vez a un individuo, o frecuentemente a una organización.
C — Posible	Puede ocurrir con el tiempo; razonable esperar que suceda alguna vez.
D — Remota	Improbable que ocurra.

MATRIZ MOR — Código de Evaluación de Riesgo (CER)

IMPACTO \ PROBABILIDAD	A — Inminente	B — Probable	C — Posible	D — Remota
I — Extremo	1	1	2	3
II — Alto	1	2	3	4
III — Medio	2	3	4	5
IV — Común	3	4	5	5

CER	SIGNIFICADO
1	Riesgo Crítico
2	Riesgo Serio
3	Riesgo Moderado
4	Riesgo Menor
5	Riesgo Insignificante

El Código de Evaluación de Riesgo (CER, o RAC en inglés) se deriva de la matriz MOR y permite priorizar los riesgos identificados de manera consistente entre distintas aplicaciones y equipos.

Las Seis Fases del Proceso MOR

El programa MOR consta de seis fases y dieciocho pasos:

Fase 1: Identificar: Asociar recursos con sus fuentes de riesgo: pasos de la operación, amenazas, vulnerabilidades y posibles eventos de pérdida.

Fase 2: Evaluar: Asignar a una de las siete categorías de pérdida; estimar probabilidad e impacto; comparar usando el CER.

Fase 3: Decidir: Priorizar desde el riesgo más serio; escoger estrategia (ETOA); seleccionar medidas de control.

Fase 4: Comunicar: Reportar resultados, consultar a partes interesadas, comunicar acuerdos logrados.

Fase 5: Implementar: Ejecutar medidas de control mediante métodos, tecnología y personal.

Fase 6: Supervisar: Evaluar la ejecución del plan, verificar efectividad de contramedidas, dar seguimiento a cambios del escenario.

MOR y Modelo ARES

El modelo para Administración de Riesgos Empresariales de Seguridad (ARES) integra las herramientas MOR en tres niveles organizacionales:

Nivel Operativo: Los oficiales de protección física (PSO) identifican continuamente amenazas y vulnerabilidades que pueden generar pérdida, y potenciales eventos de pérdida en su turno diario.

Nivel Táctico: Supervisores y mandos medios consolidan la información operativa, ajustan contramedidas y coordinan recursos entre turnos y áreas.

Nivel Estratégico: Proceso detallado que involucra investigación de datos disponibles, diagramas, herramientas de análisis y seguimiento de largo alcance de los peligros asociados a la operación completa.

> **CL Adaptación a Chile**
> La Matriz MOR es una herramienta directamente utilizable por guardias y supervisores OS10 en Chile para documentar novedades y evaluar incidentes de forma estandarizada, aportando evidencia objetiva y trazable en caso de fiscalización por la SPD o de un procedimiento judicial derivado del uso de la fuerza (Art. Ley 21.659).

Conclusión del Capítulo 2

El programa MOR fue desarrollado para maximizar la efectividad operacional, minimizando el riesgo de heridas o muerte de personas y la devaluación o pérdida de propiedad e información. Esta metodología es aplicable en procesos de análisis y toma de decisiones inmediatas, tanto a nivel operativo como táctico y estratégico.

Referencias a Consultar

- United States Navy (1989). Operational Risk Management (ORM) Methodology.
- IFPO Hispanoamérica (2021). Manual de Capacitación CPO© Versión 6.0, Capítulo 2.

Preguntas de Auto-Estudio — Capítulo 2

1. ¿En qué consiste el Código de Evaluación de Riesgos (CER) de la matriz MOR?

2. Explique con un ejemplo cómo se integraría un programa MOR dentro de un programa de gestión de riesgos organizacional.

3. ¿En qué consiste una Matriz de Evaluación de Riesgos (MER)? Seleccione la alternativa correcta y justifique.

4. Aplique la matriz MOR a un escenario con Impacto II y Probabilidad B. ¿Qué nivel de CER obtiene y qué significa?

5. Describa los tres niveles en que se integra el modelo ARES con las herramientas MOR.

CAPÍTULO 3 — ADMINISTRACIÓN DE RIESGOS EMPRESARIALES DE SEGURIDAD

Introducción a la Gestión de Riesgos

En muchos idiomas modernos, las palabras que significan "riesgo" comparten la misma raíz latina risicare, que en la antigüedad hacía referencia a la capacidad de navegar alrededor de riscos, arrecifes o rocas. El sociólogo alemán Ulrich Beck plantea que, a medida que la modernidad avanza, la producción social de riqueza va acompañada sistemáticamente por la producción social de riesgo: hoy los principales peligros ya no provienen solo de la naturaleza, sino de decisiones y negligencias humanas.

La Administración de Riesgos Empresariales (Enterprise Risk Management) ha sido definida por la Risk and Insurance Management Society (RIMS) como la cultura, procesos y herramientas para identificar oportunidades estratégicas y reducir la incertidumbre.

Compartimentalización de Riesgos

Tradicionalmente las organizaciones abordan cada tipo de riesgo (financiero, operacional, de seguridad, tecnológico) de forma aislada y por departamentos independientes, sin una política formal de gestión de riesgo integrada. Este enfoque compartimentado impide ver las interdependencias entre riesgos: cuando un riesgo se materializa en un área, puede incrementar el impacto de riesgos en otras áreas de la organización.

Necesidad de Modelos de Gestión Integrados

Frente a la compartimentalización, surge la necesidad de modelos integrados que entiendan estas interdependencias, haciendo la mitigación de riesgos más efectiva y capaz de generar ahorros al abarcar múltiples sectores del negocio simultáneamente.

Estándares ISO Aplicados a Protección

Para la gestión de riesgos, el modelo ARES utiliza los lineamientos de la norma ISO 31000, y las herramientas del método de Matrices Operacionales de Riesgo (MOR) desarrollado por la Armada de los Estados Unidos en 1989. La siguiente tabla resume el cambio de paradigma que representa un modelo integrado como ARES frente al análisis tradicional de riesgos:

ENFOQUE	CARACTERÍSTICAS
Análisis tradicional	Se enfoca en crímenes y controles internos; cada función es independiente; no existe política formal de gestión de riesgo.
Modelo ARES	Se enfoca en la identificación, medición y control integral de riesgos; está integrado en todas las operaciones y líneas de negocio; cuenta con política de gestión de riesgo formal y claramente entendida.

Origen del Modelo ARES

El Modelo para la Administración de Riesgos Empresariales de Seguridad (ARES) fue desarrollado inicialmente en el año 2008 como tesis de postgrado, y ha sido actualizado constantemente por IFPO Hispanoamérica. Define el camino para implementar operacionalmente el Enterprise Security Risk Management (ESRM), integrando la protección de Personas, Información, Propiedades, Imagen y Entorno a modelos ya existentes de Calidad, Seguridad, Salud y Ambiente (QSSHE).

Características Fundamentales del Modelo ARES

El modelo ARES se orienta a administrar el contexto de control que puede afectar a las organizaciones, bajo un enfoque de mejora continua (Planear-Hacer-Verificar-Actuar) y cuatro características esenciales:

Integrado: Se alinea a los objetivos organizacionales; la administración de riesgos forma parte del Sistema de Gestión de la Organización, no una acción aislada, sino un proceso continuo.

Integral: Enfoca sus esfuerzos en procesos organizados para proteger Personas, Información, Propiedades e Imagen de forma conjunta.

Multidisciplinario: Integra planeación estratégica, teoría de procesos, sistemas de gestión de calidad, indicadores de gestión y continuidad de negocio.

Participativo: Busca cumplir las expectativas de todas las partes interesadas ("stakeholders") que requieren entender el espectro completo de riesgos.

El sistema integral de protección ARES está ordenado para manejar doce subsistemas, correspondientes a las doce unidades completas del programa CPO®: (1) Gestión de Riesgos, (2) Roles del Personal de Protección, (3) Personas, (4) Información, (5) Propiedades, (6) Imagen, (7) Entorno de Cumplimiento, (8) Manejo de Emergencias, (9) Investigaciones, (10) Protección de Recursos Críticos, (11) Consideraciones Legales, y (12) Uso de la Fuerza.

Implementación Operacional

El modelo ARES ejecuta la gestión de riesgos en seis fases a tres niveles de la organización de seguridad:

Nivel Operativo: El usuario y el oficial de protección física identifican continuamente amenazas y vulnerabilidades en su labor diaria.

Nivel Táctico: Supervisores consolidan hallazgos, ajustan contramedidas y coordinan la respuesta entre distintas áreas o turnos.

Nivel Estratégico: Proceso detallado que involucra investigación de datos disponibles, diagramas, herramientas de análisis formal y seguimiento de largo alcance de los peligros asociados a toda la operación.

Administración de Riesgos y Seguros

El seguro es una opción de TRANSFERENCIA de riesgos: proporciona al asegurado compensación financiera tras la ocurrencia de la pérdida, conducida por probabilidad de eventos según tablas actuariales. Los profesionales de protección no deben limitarse a "endurecer el blanco" (cerraduras, barreras, alarmas), sino utilizar los cinco métodos completos de administración de riesgos. Tipos de seguro relevantes incluyen: interrupción de negocios, secuestro y rapto, compensación laboral, incendio, robo, atracos, responsabilidad civil, desempeño profesional y fidelidad.

CL Adaptación a Chile

En Chile, muchas empresas obligadas por la Ley 21.659 combinan la contratación de seguros de responsabilidad civil con la implementación de un Plan de Seguridad certificado, siguiendo exactamente la lógica ARES: transferencia de riesgo residual (seguro) + gestión activa del riesgo (plan operativo, guardias capacitados, tecnología).

Conclusión del Capítulo 3

Los beneficios de la administración de riesgos empresariales solo se optimizan con un enfoque integral de la empresa, integrado de tres maneras: centralizando los reportes de riesgo, ligando el crecimiento con el riesgo y rendimiento, y racionalizando los recursos. Los tres principales beneficios de la administración de riesgos empresarial son: alinear estratégicamente al negocio, incrementar la eficiencia de recursos y lograr mejores reportes del riesgo.

Referencias a Consultar

- Estándar ANSI/ASIS SPC.1-2009 — Resiliencia organizacional.
- IFPO Hispanoamérica (2021). Manual de Capacitación CPO© v6.0, Capítulo 3.
- ISO (2018). The new ISO 31000 keeps risk management simple.
- Brown, S., & Blackmon, K. (2001). Operations management: Policy, practice and performance improvement.

CAPÍTULO 4 — EVOLUCIÓN DE LA SEGURIDAD Y PROTECCIÓN DE BIENES

Introducción y El Ciclo de la Historia

La historia es ilustrativa: señala tendencias, muestra cómo eran las cosas y da indicios de cómo posiblemente serán en el futuro. Es también un laboratorio de la teoría, ya que exhibe soluciones planteadas en su momento y el resultado que obtuvieron. Existe una fuerte relación entre el desarrollo de la industria y el comercio, y sus necesidades de protección; la demografía juega un papel dominante en el control del crimen, y los esfuerzos de protección suelen ir un paso atrás de los últimos métodos del ataque criminal.

Periodos Bíblicos y Desarrollo en Tiempos de Guerra

La más antigua evidencia de ley escrita aparece alrededor del año 2.000 A.C., cuando Hammurabi, Rey de Babilonia, recopiló un código legal estableciendo obligaciones y derechos de los ciudadanos. En el Imperio Griego (600-500 A.C.) se implementó un sistema de guardias para vigilar accesos y sitios clave, incluida la protección de consejeros — la evidencia más antigua de protección a ejecutivos.

Imperio Romano

El emperador Augusto (63-14 A.C.) formó una unidad militar para proteger a los civiles de Roma: los Pretorianos, considerados la primera fuerza policial pese a ser de origen militar. Posteriormente se formaron los Cohors (mantención de la paz) y los Vigilios (control de incendios y colaboración en el control del crimen). El emperador Justiniano resumió el conjunto de leyes en el "Hábeas Juris Civilis" (Cuerpo Civil Legal).

Periodo Anglosajón y Periodo Moderno (1500-1900)

En la Edad Media se estableció la figura del Sheriff (originalmente Shire-reeve). Con la conquista Normanda de Inglaterra (1066) surgieron el feudalismo, el gobierno centralizado y la reorganización de la Iglesia; también nació la policía comunal ("tilthing"), grupos de diez hombres liderados por un "Constable". En 1600 surge una nueva clase social —los mercaderes— y con ella la primera policía privada, dedicada a preservar sus actividades comerciales.

Los Inicios en Estados Unidos y la II Guerra Mundial

En 1850, Allan Pinkerton, inmigrante escocés, fundó la Pinkerton National Detective Agency, hito fundacional de la seguridad privada moderna. Otros hitos históricos relevantes:

- **1855: Consolidación de la Agencia Pinkerton en investigación privada.**
- **1858: Edwin Holmes crea la primera central de supervisión y respuesta de alarmas.**
- **1874: Fundación de ADT (American District Telegraph), luego la mayor compañía de alarmas del mundo.**

- **1891: Se crea Brinks Armored, la mayor compañía de vehículos blindados del mundo.**
- **1909: William J. Burns lidera el "Departamento de Investigación", precursor del FBI.**
- **1954: George Wackenhut funda la Wackenhut Corporation.**

Economía, Tendencias de Mercado y Terrorismo

Existe una fuerte relación entre comercio, canales de transporte, demografía y necesidades de protección. Durante los años 80 y 90 se documentaron episodios de terrorismo de distinto signo ideológico en Estados Unidos, y una serie de atentados de fundamentalismo islámico marcaron el cambio de siglo:

- **1993: Atentado con explosivos en el World Trade Center.**
- **1995: Atentado con bomba en el edificio federal Murrah, Oklahoma.**
- **2001: Ataques del 11 de septiembre al World Trade Center y el Pentágono.**
- **2015: Atentados de células terroristas en ciudades de Europa, Asia y Norteamérica.**

El manual identifica factores que explican el crecimiento de estos grupos: el choque entre lo viejo y lo nuevo, las luchas de clase, la demografía juvenil desempleada, y una prolongada cultura de guerra en ciertas regiones del mundo.

Historia de las Empresas de Protección

Los servicios de protección tercerizados han desempeñado un papel importante en la seguridad pública y privada, ofreciendo flexibilidad al cliente. Además del servicio estándar de oficiales de protección, existen servicios especializados como respuesta y monitoreo de alarmas, vehículos blindados, protección personal (PPO) e investigación privada.

Trayectoria al Profesionalismo y Carreras Contemporáneas

La industria de protección ha evolucionado significativamente en los últimos 150 años: el candado y las llaves tradicionales han sido reemplazados por sofisticados sistemas electrónicos, perímetros de alta protección y CCTV, junto con profesionales cada vez mejor capacitados. Existen hoy oportunidades de carrera en ventas, atención al cliente y gerencia de recursos humanos dentro de la industria de protección, además del rol operativo de oficial de protección propiamente tal.

> **CL Adaptación a Chile**
> La Ley 21.659 (2019-2021) y su reglamento DS 209 (2024) representan, salvando las distancias, el mismo salto de "empirismo a profesionalización" que describe IFPO para la industria estadounidense desde 1850: formación obligatoria certificada, registro estatal de guardias, códigos de conducta vinculantes y fiscalización activa por Carabineros y la Subsecretaría de Prevención del Delito.

Referencias a Consultar

- IFPO Hispanoamérica (2021). Manual de Capacitación CPO© v6.0, Capítulo 4.
- Maggio, E. J. (2009). Private security in the 21st century: Concepts and applications.

Preguntas de Auto Estudio — Capítulo 4

1. Enumere tres fuerzas de control usadas en la Antigua Roma y describa la función de cada una.

2. Describa el evento significativo asociado a los años 1215, 1066 y 1855.

3. Enumere tres innovaciones atribuidas a Allan Pinkerton.

4. Enumere tres razones por las que, según el manual, el terrorismo de grupos fundamentalistas creció en ciertas décadas.

5. ¿Qué relación existe entre demografía, comercio y necesidades de protección a lo largo de la historia?

ANEXO — SÍNTESIS DE ADAPTACIÓN A CHILE

Este anexo resume los puntos de conexión directa entre los cuatro capítulos de la Unidad I y el marco legal chileno vigente, para facilitar su aplicación práctica por parte de los estudiantes de OTEC MSEREY.

CAPÍTULO	CONEXIÓN CON LA NORMATIVA CHILENA
Cap. 1 — Conceptos Clave	El Estudio de Seguridad exigido por el DS 209 replica la clasificación de recursos (Personas, Información, Propiedades, Imagen) y el ciclo de gestión de riesgos ISO 31000 descrito por IFPO.
Cap. 2 — MOR	La Matriz MOR (CER/Impacto/Probabilidad) es aplicable directamente a la documentación de novedades y evaluación de incidentes por guardias OS10, aportando trazabilidad ante fiscalización de la SPD.
Cap. 3 — ARES	El enfoque integrado (Personas-Información-Propiedades-Imagen) del modelo ARES es el mismo enfoque que exige un Plan de Seguridad certificado bajo la Ley 21.659 para entidades con múltiples sucursales.
Cap. 4 — Historia	La transición de la seguridad empírica a la profesionalizada (Pinkerton, 1850) es análoga a la transición chilena marcada por la Ley 21.659 (2019-2021) y el DS 209 (2024).

MANUAL DEL ALUMNO — UNIDAD I (RESUMEN FIEL AL MANUAL OFICIAL)

Basado en: Manual de Capacitación Oficial Certificado de Protección CPO© v6.0 — IFPO Hispanoamérica (2021)

Adaptado y resumido por OTEC MSEREY para estudiantes de Certificación CPO®-IFPO