



Criminología Empresarial: Fundamentos de una gestión de seguridad corporativa

Business Criminology: Fundamentals of Corporate Security Management

* David León Díaz | Universidad de Ixtlahuaca | México.

Recibido: 2025/22/01 | Aceptado: 2025/23/03 | Publicado: 2025/05/21

Resumen

La criminología moderna genera conocimientos en prevención y seguridad para la mejora e implementación de protocolos, planes o políticas de seguridad corporativa. La cultura de seguridad es un punto muy importante de todos aquellos que procuran un bienestar laboral, al respeto y al apego de los programas normativos; así como a los controles de seguridad, gestionando y percibiendo los riesgos que nos ayudan a prevenir acciones que afecten la integridad de las personas y de las organizaciones, de esta manera se elimina el abuso de confianza ante las debilidades identificadas, fomentando hábitos y prácticas de seguridad tomando en cuenta factores sociales, económicos y tecnológicos. La toma de decisiones en una Gestión de Seguridad Corporativa está fundamentada con la identificación de riesgos, una protección física, la administración investigaciones, prevención de pérdidas y capital humano de manera fructífera para la prevención del delito y de aquello que afecte a la mejora continua de la organización.

Palabras clave: Patrimonio, Riesgo, Tecnología, Pérdida, Investigación, Mejora continua, Prevención, Seguridad.

Abstract

Modern criminology generates knowledge in prevention and security for the improvement and implementation of corporate security protocols, plans or policies. The safety culture is a very important point for all those who seek well-being at work, respect and adherence to regulatory programs; as well as security controls, managing and perceiving the risks that help us prevent actions that affect the integrity of people and organizations, in this way the abuse of trust is eliminated in the face of identified weaknesses, promoting security habits and practices taking into account social, economic and technological factors. Decision-making in Corporate Security Management is based on the identification of risks, physical protection, administration, investigations, loss prevention and human capital in a fruitful way for the prevention of crime and that which affects the continuous improvement of the organization.

Keywords: Heritage, Risk, Technology, Loss, Research, Continuous improvement, Prevention, Security.



Cómo citar este artículo:

León Díaz, D., R. (2025). Criminología Empresarial: Fundamentos de una gestión de seguridad corporativa. *Revista Criminología y Ciencias Forenses: Ciencia Justicia y Sociedad*, 4 (7), 44-61

* Instructor y capacitador de capital humano, cursos en prevención del delito, gestión de riesgos, protección de activos, seguridad e-commerce y logística, seguridad de la información, protección civil y Diplomado en Seguridad Patrimonial y Prevención de Pérdidas. Correo electrónico: davidleondiaz510@gmail.com. orcid.org/0009-0008-4341-2378

1. Introducción

Una de las tantas necesidades que tiene toda organización pública o privada, es proteger todo producto o servicio que emplea como desarrollo económico, de imagen, infraestructura, humano, social y entre otros. Lo que ha llevado a distintos profesionales a crear, desarrollar y aplicar programas de seguridad y prevención del delito para mantener un desarrollo organizacional y una mejora continua; para ello, se requieren fundamentos básicos a ejecutar en materia de protección física, mejora de la rentabilidad económica, optimización de planes de seguridad en tecnología, identificación de riesgos e investigación en seguridad.

Para los profesionales en Seguridad Patrimonial, es necesario conocer puntos base y clave para poder desarrollar un plan de seguridad como lo es; la gestión de riesgos en donde se identifica, analiza y evalúa de manera multidisciplinar el riesgo al cual nos enfrentamos.

A lo anterior es importante conocer físicamente el espacio en donde se oferta el producto o servicio, y en donde cada colaborador desempeñando cada una de sus actividades, por lo que se implementan medidas físicas de seguridad al patrimonio, buscando generar un entorno físico más seguro y eliminando la oportunidad del delito.

Al dar seguimiento a las incidencias detectadas por Seguridad, es necesario realizar una investigación clara y precisa, para poder conocer la génesis del delito o en su defecto el *modus operandi* de la incidencia con el objetivo primordial de prevenir otros siniestros.

El objetivo primordial de una Gestión de Seguridad en las organizaciones públicas y privadas es; la seguridad y prevención, el generar planes de seguridad con ventajas estratégicas para el control y reducción de delitos y conductas inapropiadas que afectan los activos de alto valor, donde el primordial es la vida humana. Así mismo se podrá llegar a una mejora continua, donde se plasmarán las áreas de oportunidad y desarrollo continuo en Seguridad.

2. Desarrollo

La Criminología del siglo XXI ha creado un papel fundamental en temas de Seguridad y Prevención del delito en empresas de servicios financieros, tecnológicos, manufactura, comunicación, transporte y logística, entre otros y a esto se deriva una rama llamada *Criminología Corporativa*. Para esto, debemos entender los fundamentos básicos a desarrollar en Seguridad y Prevención.

2.1 Seguridad Patrimonial

Según los profesionales en seguridad en Latinoamérica, describen que Seguridad Patrimonial es el conjunto de medidas de protección que una empresa toma para protegerse contra los riesgos y amenazas que puedan afectarla. Para ello, éstas organizaciones, bajo el liderazgo de un director de seguridad, analizan sus «vulnerabilidades» y desarrollan planes de seguridad. El programa está diseñado para proteger la propiedad, los activos y los empleados de la empresa (Revista de Seguridad 360, 2024).

La seguridad empresarial igual que la mayoría de las disciplinas, también ha evolucionado al punto que en los actuales tiempos se maneja como un “sistema de gestión”, el cual está conformado por el conjunto coherente de principios, políticas, objetivos, estrategias, normas y procedimientos de seguridad, así como de lineamientos y directrices que permitan la administración sistemática y efectiva de los planes y programas que tienen como fin la preservación de los recursos y actividades de las empresas (Díaz, 2020).

En algunas organizaciones el departamento de seguridad y prevención, adquiere servicios de consultoría en Seguridad Patrimonial para encontrar aquellas vulnerabilidades que han afectado el progreso organizacional, por otro lado, el capital humano que tienen contratado de manera interna aporta conocimientos en prevención del delito basado en el giro de la organización, papel que hoy en día está siendo ejecutado por Criminólogos.

2.2 Gestión de Riesgos

La norma ISO 31000 define la Gestión de Riesgos como todas aquellas acciones coordinadas para dirigir y controlar los riesgos a los que puedan estar abocadas las organizaciones. La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión. Para entender la parte esencial de la norma se desprenden los siguientes términos:

- **Riesgo:** efecto de la incertidumbre sobre los objetivos.
- **Efecto:** es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.
- **Parte interesada:** persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- **Fuente de riesgo:** elemento que, por sí solo o en combinación con otros, tiene el potencial de generar.
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias.
Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias. Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.
- **Consecuencia:** resultado de un evento que afecta a los objetivos. Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos. Las consecuencias se pueden expresar de manera cualitativa o cuantitativa. Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.
- **Probabilidad:** posibilidad de que algo suceda.
En la terminología de gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).
- **Control:** medida que mantiene y/o modifica un riesgo.
Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.
Los controles no siempre pueden producir el efecto de modificación previsto o asumido (Normalización, 2018).

2.2. Metodología de identificación de riesgo

La identificación de riesgos está sustentada y basada en distintas metodologías que quiera aplicar el responsable de seguridad y el equipo multidisciplinar, para ello se presenta una que es de gran importancia y que es aplicada en la actualidad por los responsables de seguridad en las

organizaciones privadas, como lo mencionó el Lic. en Crim. Arturo Villuendas en su conferencia “Gestión de Riesgos en la Seguridad Patrimonial” en el XIII Congreso Internacional de Criminología, en la Universidad de Ixtlahuaca CUI, donde mencionaba que toda gestión de riesgos tiene una metodología, para ello se menciona el:

2.2.1 Método Mosler

El método Mosler tiene por objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación y materialización de un riesgo, con la finalidad de que la información obtenida, nos permita calcular la clase y dimensión de riesgo. El método es de tipo secuencial y cada fase del mismo se apoya en los datos obtenidos en las fases que le preceden (CIVITTAS, 2012).

Así mismo el consultor en Seguridad Integral, Francisco Sandoval González Fuentes describe el método Mosler de la siguiente manera:

- **Definición del riesgo:** Esta fase tiene por objeto, la identificación del riesgo, delimitando su objeto y alcance, para diferenciarlo de otros riesgos.
- **Análisis del riesgo:** En esta fase se procederá al cálculo de criterios que posteriormente nos darán la evolución del riesgo.
- **Criterio de función:** Las consecuencias negativas o daños pueden alterar o afectar de forma diferente la actividad:
 - Muy gravemente 5
 - Gravemente 4
 - Medianamente 3
 - Levemente 2
 - Muy levemente 1
- **Criterio de sustitución:** Dificultad para ser sustituidos los bienes o productos:
 - Muy difícilmente 5
 - Difícilmente 4
 - Sin muchas dificultades 3
 - Fácilmente 2
 - Muy fácilmente 1

- **Criterio de Profundidad:** Perturbación y efectos psicológicos que podrían producirse en la imagen:
 - Perturbaciones muy graves 5
 - Perturbaciones graves 4
 - Perturbaciones limitadas 3
 - Perturbaciones leves 2
 - Perturbaciones muy leves 1
- **Criterio de extensión.** El alcance de los daños o pérdidas a nivel territorial:
 - Alcance internacional 5
 - Carácter nacional 4
 - Carácter regional 3
 - Carácter local 2
 - Carácter individual 1
- **Criterio de agresión.** La probabilidad de que el riesgo se manifieste:
 - Muy alta 5
 - Alta 4
 - Normal 3
 - Baja 2
 - Muy baja 1
- **Criterio de vulnerabilidad.** Probabilidad de que realmente se produzcan daños o pérdidas:
 - Muy alta 5
 - Alta 4
 - Normal 3
 - Baja 2
 - Muy baja 1
- **Evaluación del riesgo.** Tiene por objeto cuantificar el riesgo considerado (ER).
 - Cálculo del carácter del riesgo “C”: $\text{Calculo} = I + D$
 $I = \text{Importancia del suceso} = \text{Función (F)} \times \text{Sustitución (S)}$
 $D = \text{Daños ocasionados} = \text{Profundidad (P)} \times \text{Extensión (E)}$
 - Cálculo de la probabilidad “Pb”.

$Pb = \text{Agresión (A)} \times \text{Vulnerabilidad (V)}$

- Cuantificación del riesgo considerado “ER”.

$ER = \text{Carácter (C)} \times \text{Probabilidad (Pb)}$

$ER = C \times Pb$

(Fuentes, 2022).

- **Cálculo de la clase de riesgo.**

Valor de ER	Clase de Riesgo
2 a 250	Muy Bajo
251 a 500	Pequeño
501 a 750	Normal
751 a 1000	Grande
1001 a 1250	Elevado

(Fuentes, Ciencias de la Seguridad y Forenses, 2024)

El resultado de un análisis de riesgos que se aplique con cualquier método; identifica, evalúa y analiza cada vulnerabilidad detectada, refiriendo las debilidades que aquejan a los planes o programas de seguridad y prevención.

2.3 Investigaciones

Para las investigaciones en seguridad, el criminólogo es el profesional responsable de conducir la integración, detección, comprobación y resolución exitosa de situaciones relativas a la falta de honradez de clientes, empleados o proveedores, por ejemplo:

- Pre empleo
- Antecedentes de potenciales clientes o socios
- Robo (interno o externo)
- Intrusiones a las instalaciones

La investigación empresarial es un proceso de adquisición de información detallada de todas las áreas de negocio para maximizar las ventas y los beneficios de la organización. Este estudio ayuda a las empresas a determinar qué productos y servicios son los más rentables o los más demandados. Puede afirmarse como la adquisición de información o conocimientos con fines profesionales o comerciales para determinar las oportunidades y objetivos de un negocio. La investigación para negocios se puede utilizar para cualquier cosa. En general, cuando la gente habla del término, significa hacer preguntas para saber en qué se puede gastar el dinero para aumentar las ventas, los beneficios o la cuota de mercado. Tal investigación es crítica para tomar decisiones sabias e informadas (Díaz, 2020, p. 42-43).

Dentro de las investigaciones de seguridad, existen errores de lo más común, por ello se menciona de la siguiente manera:

- **Conflictos de interés en la apertura, cierre, aceleración o retraso de investigaciones:** Si el investigador tiene alguna relación con las personas involucradas en la investigación, los testigos o las personas que emiten el informe, o si busca algún beneficio personal, su imparcialidad se verá afectada.
- **Parcialidad en la selección de personas entrevistadas para influir en los resultados:** Si el investigador tiene conclusiones anticipadas, solo entrevistará a aquellos que apoyen su hipótesis, lo que afectará la objetividad de la investigación.
- **La manipulación, destrucción o fabricación de pruebas o información:** Podría llevar a la acusación y posible condena de una persona equivocada, o incluso a la absolución de alguien responsable de un incidente. Es esencial que se tomen medidas para garantizar la integridad y la precisión de la información recopilada, con el fin de promover la justicia y evitar cualquier error que pueda poner en peligro el resultado de la investigación.
- **Recursos de amenazas o promesas y mentiras durante entrevistas pueden dañar la investigación y la credibilidad del investigador:** Es fundamental que los investigadores tengan las habilidades necesarias para llevar a cabo entrevistas éticas y efectivas, sin recurrir a tácticas engañosas.
- **Compromiso de información confidencial de la investigación:** Toda investigación es confidencial y solo debe compartirse con las partes interesadas y los tomadores de

decisiones. No se deben compartir detalles con otras personas ni utilizarlos para presentaciones fuera del entorno de la empresa.

- **La ausencia de un informe de investigación:** Un informe bien escrito no solo es importante para clarificar los procesos llevados a cabo, sino también para presentar los hallazgos y conclusiones de manera clara y concisa. De esta forma, se facilita la comprensión y se fomenta una toma de decisiones informada y efectiva.
- **Uso de técnicas de investigación no comprobadas científicamente:** algunas técnicas pueden ser orientativas, pero no son una confirmación de responsabilidad, como la grafología o algunas técnicas de interpretación del lenguaje corporal.

¿Cuáles son los objetivos de un informe de investigación?

Los objetivos de un informe de investigación pueden variar según el tipo y el propósito de la investigación en sí. Sin embargo, algunos objetivos clave a considerar al redactar un informe de investigación pueden incluir:

1. **Ofrecer información sobre los objetivos, alcance y criterios de la investigación:** El informe debe proporcionar un contexto claro sobre el propósito y enfoque de la investigación, facilitando su comprensión y aplicabilidad.
2. **Presentar información sobre los descubrimientos y conclusiones de la investigación:** Los resultados obtenidos deben ser presentados de manera clara y concisa, permitiendo a los lectores comprender los hallazgos y su relevancia.
3. **Establecer una base para determinar posibles acciones disciplinarias:** Si la investigación revela irregularidades o violaciones, el informe puede ser utilizado como base para tomar decisiones sobre acciones disciplinarias por parte de la alta dirección y los encargados de tomar decisiones.
4. **Identificar acciones correctivas necesarias para atenuar riesgos significativos:** Si la investigación tiene como objetivo identificar riesgos y áreas de mejora, el informe debe señalar las acciones correctivas necesarias para abordar estos problemas.
5. **Servir como fundamento para identificar oportunidades de mejora en el sistema de gestión de riesgos:** Si es pertinente y forma parte de los objetivos de la investigación, el informe puede ser utilizado para mejorar los procesos y sistemas de gestión de riesgos de la organización.

6. **Proporcionar un registro de la investigación realizada:** El informe debe servir como un documento histórico que detalle el proceso y los resultados de la investigación, permitiendo futuras consultas y seguimiento (José Luis Prieto, 2025).

El criminólogo adquiere un papel fundamental en los procesos administrativos de una investigación, ya que dentro de sus bases criminológicas comprenderá el origen del delito.

2.4 Prevención de Pérdidas

En 2022 José Luis Prieto Montes menciona, para proteger los ingresos económicos, desarrollar venta al por menor, contar con una estrategia operativa, margen de ganancia sobre inversiones, gastos y pérdidas **en los activos de las organizaciones, es necesario entender que es Prevención de Pérdidas:**

- Medidas que toman las empresas para ayudar a proteger sus ingresos.
- Mejorar la rentabilidad de la organización con estrategias de seguridad.
- Mejora continua de la organización con los activos ofrecidos al cliente.

A lo anterior, es importante aplicar las buenas prácticas en Prevención de Pérdidas. Para ello en 2021 la Revista de Loss Prevention Solutions se pueden describir:

- **Análisis:** historial de las mermas, cambios en las mermas.
- **Cumplimiento:** auditorías, visitas de seguridad a tienda, observaciones de inventario físico, capacitación.
- **Inventario físico:** las prácticas adecuadas sean seguidas para obtener los resultados más precisos.
- **Componentes base:** entrevistas generales, diagnóstico de merma, auditorías, mystery shops.
- **Investigaciones:** rentabilidad y salud de la organización.
- **Líneas de abuso:** centros de atención a clientes, buzón de quejas.
- **Excepciones:** la capacidad de detectar actividades fraudulentas a tiempo.
- **Políticas y procedimientos:** buenas prácticas de inventario, atención a clientes, merma y seguridad.

El mantener y mejorar la rentabilidad que dejan los activos de la organización, derivan de la aplicación de un programa de seguridad y prevención que aborda y entiende:

- **Tipos de retail:** tiendas físicas, tiendas online, sistema híbrido.
- **Tipos de pérdida:** natural, intencional, accidental.
- **Tipos de merma:** natural, administrativo, daños, robo interno o externo.
- **Causas de la merma:** interna, externa, proveedor o administrativa.
- **Técnicas de gestión del inventario:** al recibir el activo, al exhibir en piso de venta, a entregar en cajas y la salida del activo (Díaz, Cofradía Criminológica, 2023).

El desarrollo, la aplicación y evaluación de un inventario se basa en la calidad que este tiene, para ello se describe lo siguiente:

- **Tiempo y forma:** bajo volumen, solo se pide lo necesario.
- **Análisis A-B-C;** A: alto valor, con baja frecuencia de ventas y niveles de existencias más bajos, B: artículos de valor y frecuencia de ventas moderadas, C: son de bajo valor, con alta frecuencia de ventas y relativamente altos en existencias.
- **Revisión periódica de stock:** revisión manual o automática para identificar existencias considerando pronósticos de venta.
- **Nivel predeterminado de existencias:** hay un stock definido ¿Si se llega a un nivel mínimo se pide más Producto?
- **Fisrt- IN y Fist- OUT:** Primeras entradas - primeras salidas, stock más antiguo se vende primero, es importante en los productos perecederos.
- **Auditoria básica:** Es cotejar lo teórico contra lo real, inventario físico, conteos dirigidos o conteos cíclicos (Montes, 2022, p. 24).

2.5 Seguridad Física

Limitar el número de entradas al edificio, pasar por puestos de control de seguridad con agentes de seguridad o dispositivos de bloqueo, son algunas partes del diseño de seguridad física de un edificio. **El diseño físico puede crear o ampliar una esfera de influencia. Los usuarios**

desarrollan entonces un sentido de control territorial, mientras que los posibles infractores, al percibir este control, se sienten desanimados.

El desarrollo de una protección física para el patrimonio se deriva de un sistema de seguridad que comienza con una definición del problema a resolver y la determinación de las metas y objetivos del sistema. Las principales etapas son diseño, análisis e implementación. Dentro de la fase de diseño, el equipo y las medidas de seguridad específicas se dividen en cuatro grupos, de acuerdo a la función (disuasión, detección, demora y respuesta) (**Asis Internacional, 2012**).

ASIS International en 2019, define la seguridad física como: la parte de la seguridad relacionada con las medidas físicas destinadas a proteger a las personas; para evitar el acceso no autorizado a los equipos, instalaciones, materiales y documentos; y para protegerlos contra un incidente de seguridad. Las medidas de desempeño de las funciones del Seguridad Física son:

- **Detección:** Probabilidad de detección, tiempo para comunicar y evaluar, frecuencia de alarmas no deseadas.
- **Demora:** Tiempo para vencer los obstáculos.
- **Respuesta:** Probabilidad de comunicación precisa a las fuerzas de respuesta, tiempo para comunicar, probabilidad desplegarse hacia la ubicación del adversario, tiempo para desplegarse y efectividad de la fuerza de respuesta.

Es necesario entender que los protocolos de protección física que el departamento de seguridad patrimonial desarrolla, debe contar con aplicación tecnológica, humana, periférica y estructural, la cual ayudará a la optimización de la operación. Para ello se entiende que los componentes de seguridad física se despliegan de la siguiente manera:

- **Humanos:** Guardias de seguridad, analistas de inteligencia, monitorista de alarmas, CCTV y GPS.
- **Electrónicos:** Sensores de alarmas, cámaras, rastreador GPS, detectores de humo PCI, control de accesos.
- **Periféricos:** Seguridad Ciudadana, Protección Civil, Seguridad e Higiene.
- **Estructurales:** Bardas, calles, estructura metálica, ventanas.

2.6 Teoría de Prevención del Crimen a través del diseño ambiental (CPTED)

El diseño de seguridad física se refiere a cualquier estructura que se pueda construir o instalar para disuadir, impedir o detener un ataque. Actualmente distintas organizaciones implementan medidas drásticas en seguridad física a sus unidades de negocio con el objetivo de eliminar la oportunidad del delito.

El diseño apropiado y el uso eficiente de la construcción del entorno, pueden conducir a una reducción en la oportunidad, el miedo y la incidencia de los delitos de extraño a extraño, así como en la mejora de la calidad de vida (dónde y cómo vivimos, del trabajo y la diversión).

CPTED es el diseño o rediseño de un lugar para reducir la oportunidad del delito y del temor al delito a través de medios naturales, mecánicos y de procedimientos. CPTED es una teoría de la prevención de la delincuencia basada en la criminología ambiental, es decir, la proposición de que el diseño cuidadosamente pensado de lugares tales como edificios, parques, estacionamientos y otras estructuras en los alrededores, pueden mejorar la calidad de vida, disuadiendo las oportunidades para el delito y reduciendo el miedo al delito. Como tal, también es compatible con una mejora de la seguridad y de protección de los activos, y una mayor conciencia de seguridad de la organización y/o instalación donde se implementa.

Para el profesional de la seguridad, el CPTED es un conjunto de herramientas de gestión orientadas a lo siguiente:

- **Lugares:** Entornos físicos (tales como edificios, oficinas, estacionamientos, parques y espacios públicos, edificios de apartamentos multifamiliares, almacenes, escuelas, casas de culto y centros comerciales) pueden ser diseñados para producir efectos en el comportamiento, que reduzcan la oportunidad para ciertos tipos de delitos y para el temor a esos crímenes.
- **Comportamiento:** Algunos lugares parecen crear, promover o permitir la actividad criminal o los comportamientos insurrectos mientras que otros entornos provocan conductas respetuosas y obedientes de la ley.
- **Diseño y uso del espacio:** El rediseño de un espacio o un uso eficiente de él puede fomentar un comportamiento deseable y desalentar la delincuencia y las conductas indeseadas (Lawrence J. Fennelly, CPTED and Traditional Security Countermeasures, 2018, p. 3-5).

El CPTED aborda el diseño del espacio físico para apoyar a los usuarios legítimos a los que está destinado el espacio, y minimizar el comportamiento previsible de los delincuentes. Tim Crowe refinó las ideas de Newman y clasificó las soluciones del CPTED como sigue:

- **Medidas mecánicas:** También conocidas como medidas de endurecimiento, las medidas mecánicas incluyen el hardware de seguridad física y la tecnología (tales como cerraduras, cámaras de seguridad en ventanas, cercas y salidas, sistemas de control, detección de intrusos, video vigilancia y barreras).
- **Medidas humanas y organizacionales:** Estas incluyen la vigilancia entre los vecinos de la cuadra, vigilancia entre los vecinos del barrio, patrullas y puestos de seguridad, patrullas policiales, conserjes, botones de vestíbulos y cualquier persona o grupo que actúe como guardián con la capacidad de observar, informar e intervenir.
- **Medidas naturales:** Las medidas naturales del CPTED emplean una buena planificación del espacio para reducir los conflictos de los habitantes teniendo en cuenta los patrones de circulación compatibles. Las medidas naturales incluyen el tener una entrada al edificio bien definida y organización de jardines, patios y porches para tener una visión sin obstáculos (Lawrence J. Fennelly, CPTED and Traditional Security Countermeasures, 2018, pág. 6-7).

En 2012 Asis Internacional menciona, las medidas naturales proporcionan una orientación específica para el uso del espacio, e incluye paisajismo arquitectónico, cunetas, bermas, bolardos, jardineras, fosos y acciones de mejoramiento de la visibilidad, tales como iluminación y recorte de arbustos o árboles. Aun cuando es suministrada por un equipo mecánico (lámparas), la iluminación es clasificada como un componente de vigilancia natural.

Estas medidas se aplican con varios conceptos en mente:

- **Control de acceso natural:** La idea es emplear barreras tanto reales como simbólicas incluyendo puertas, cercas y arbustos para definir y limitar el acceso a un edificio u otro espacio. Por ejemplo, para disuadir a los ladrones de entrar por las ventanas más bajas, uno podría plantar arbustos densos y espinosos cerca de las ventanas o instalar dispositivos de bloqueo de ventanas o un sistema de alarmas.
- **Vigilancia natural:** Aumentar la visibilidad de los ocupantes y los observadores casuales aumenta la detección de intrusos o de malas conductas en una instalación. Por ejemplo, si

una cerca de madera alta bloquea la visibilidad de una plataforma de descarga, esa falta de visibilidad puede invitar a los ladrones.

- **Refuerzo territorial natural:** Este es el proceso de establecer un sentido de propiedad, responsabilidad y rendición de cuentas de los propietarios, administradores u ocupantes para aumentar la vigilancia e identificar los intrusos. Por ejemplo, el uso de pequeños bordes de arbustos a lo largo de las aceras en un complejo de apartamentos, marca un territorio de apartamentos individuales y desalienta a los intrusos que intenten atravesarlos. Además, las personas prestan más atención y defienden un espacio en particular si se sienten psicológicamente dueños de ese espacio.
- **Gestión y mantenimiento:** Para que los espacios luzcan bien cuidados y libres de delincuencia, deben ser mantenidos. La teoría de “ventanas rotas” sugiere que dejar las ventanas rotas u otros signos de decaimiento (por ejemplo, grafiti, basura o muebles abandonados) sin supervisión o no reparados pueden conducir a la impresión de abandono e incrementar las oportunidades de delitos, ya que no se observa ningún guardián. Un vehículo aparcado demasiado tiempo con un vidrio roto puede muy pronto tener otro más.
- **Apoyo a la actividad legítima:** Algunos lugares son difíciles de proteger por la naturaleza de su ubicación u otras características geográficas. En tales casos, el apoyo a la actividad legítima es esencial. Un foco de delincuencia podría ser erradicado si la policía instalara allí una subestación o el personal de mantenimiento se trasladará para ocupar ese espacio, proporcionando el apoyo a las actividades legítimas. (Lawrence J. Fennelly, CPTED and Traditional Security Countermeasures, 2018, pág. 36-37).

Por el contrario, el uso de mallas metálicas que permitan una visibilidad del área, sin obstrucciones, por trabajadores o transeúntes puede desalentar a los ladrones. Ventanas, mirillas, espejos y otra característica del diseño que mejore la visibilidad se encuentran dentro de la vigilancia natural.

2.7 Prevención Situacional del Crimen

La prevención situacional del crimen se desarrolló a finales de los años setenta y principios de los ochenta en Gran Bretaña. Aunque influenciada por el CPTED y los conceptos de espacio defendible, la prevención del situacional procuraba reducir las oportunidades delictivas en todos los contextos, no sólo en edificios y otros espacios.

En sus inicios, la prevención situacional consistía en una serie de medidas específicas dirigidas a reducir la oportunidad del delito, por ejemplo, eliminando o desviando los potenciales delincuentes de las áreas objetivo. Actualmente, la prevención situacional del crimen incluye estrategias para reducir los motivos y las oportunidades, tales como reglas de fijación de límites y estimulando la conciencia de los potenciales delincuentes. Tales estrategias de prevención social se unen a esta nueva generación de CPTED que está emergiendo.

Asis Internacional en 2012, menciona que los cuatro enfoques de la prevención situacional del crimen frecuentemente se logran así:

- **Incrementando el esfuerzo:** medidas de endurecimiento del objetivo, las cuales aumentan el esfuerzo mediante la creación de barreras físicas, tales como cerraduras, cámaras, puertas de acero, cercas y cristal inastillable.
- **Incrementando el riesgo:** detección de entrada y salida, lo que aumenta el riesgo mediante el control de quién entra y sale de un área de vigilancia formal y mecánica con sistemas de CCTV vigilancia a través de empleados, conserjes y oficiales de seguridad.
- **Disminuyendo los beneficios esperados:** retiro de objetivos, tales como una política de no-efectivo (no-cash), depósito directo de cheques y retiro temporal de las radios de los vehículos, denegar al delincuente los beneficios, por ejemplo, a través de colocación de plantas en los muros vulnerables a los grafitis, kits de explosión de tinta en bolsas de dinero de bancos y números de identificación del personal (PIN) para tarjetas de crédito y radios de vehículos.
- **Eliminando las excusas:** establecer reglas y límites que eliminen la ambigüedad que permita a las personas cometer delitos y excusar sus actos aduciendo ignorancia o incomprensión, estimular la conciencia, a través de declaraciones contra el robo, exceso de velocidad, tabaquismo, consumo de drogas, botar basura, etc.

3. Metodología

La presente investigación que se realizó es de tipo cualitativo. Utilizó la recolección y análisis de los datos para afinar los fundamentos básicos que se requieren para una Gestión de Seguridad Corporativa.

Para la interpretación de los fundamentos básicos en Seguridad Corporativa se utilizó el método hermeneúutico para el análisis de textos, investigaciones, artículos, cursos y diplomados desarrollados por profesionales en temas de Seguridad y Prevención en empresas públicas y privadas.

El punto medular de la criminología es la prevención, para ello en una Gestión de Seguridad Corporativa versa en: la mitigación de cada uno de los riesgos identificados, trabajo que se realiza de manera multidisciplinar, con programas normativos y/o estándares de seguridad, metodologías de identificación y análisis de riesgos para llegar al punto de la creación y aplicación de controles de seguridad, donde su objetivo principal es; identificar, controlar, mitigar y prevenir el fenómeno delictivo, riesgo que afecta a toda organización en particular.

4. Conclusión

El conocer claramente, los términos de gremio dentro de la seguridad patrimonial permitirán que los criminólogos corporativos realicen una correcta diferenciación de términos que parecen significar lo mismo o los que ya están actualizados para distintas organizaciones nacionales e internacionales en materia de seguridad.

La mejora continua, está reflejada en la correcta implementación de programas de seguridad en la organización, esto derivado de terminología aplicada correcta desde una identificación de riesgos, y que se es visualizada en la mitigación de riesgos pues el diferenciar las necesidades en la seguridad con las comodidades genera una aceptación multidisciplinaria para la prevención de lo identificado.

En el siglo XXI el trabajo del criminólogo corporativo está derivado del trabajo de otros criminólogos que buscaron cambiar el rumbo del campo laboral y demostrar que se extiende a otras áreas, teniendo como punto medular la seguridad y prevención de todo aquello que genere conductas de riesgo, principalmente las delictivas.

El criminólogo desempeña sus actividades preventivas y de mitigación en organizaciones privadas y públicas, dejando como base prioritaria el análisis y la evaluación de una identificación de riesgos de manera multidisciplinar y en cada giro empresarial viendo a un criminólogo como una necesidad organizacional y su protección física.

La metodología es uno de los principales sustentos de un criminólogo corporativo, pues es aquella que le ayuda a determinar los controles operacionales de seguridad, los controles preventivos y los de mitigación para la organización en la que se esté desempeñando de manera laboral.

Fuentes de consulta

- Asis Internacional. (2012). Protección de Activos: Seguridad Física. En A. Internacional, *Protección de Activos: Seguridad Física* (p.p. 39-40). Estados Unidos de América: Asis Internacional.
- CIVITTAS. (08 de Diciembre de 2012). *CIVITTAS Empresa de Seguridad Privada*. Obtenido de <https://www.civittas.com/analisis-de-riesgos-el-metodo-mosler/>
- Díaz, D. L. (2020). En *Identificación y Mitigación de Riesgos en Empresas del Estado de México* (págs. 42-43). Ixtlahuaca: Universidad de Ixtlahuaca.
- Díaz, D. L. (20 de Abril de 2023). Cofradía Criminológica. 10. Ciudad de México.
- Díaz, D. L. (01 de 04 de 2024). Prevención de Pérdidas. Tlalpan, Ciudad de México, México.
- Fuentes, F. J. (21 de Enero de 2022). *Ciencias de la Seguridad y Forenses*. Recuperado el 16 de 01 de 2024, de Ciencias de la Seguridad y Forenses: <http://www.pryseseguridad.com/2013/05/ejemplo-de-un-analisis-de-riesgos.html>
- Fuentes, F. J. (16 de 01 de 2024). *Ciencias de la Seguridad y Forenses*. Obtenido de <http://www.pryseseguridad.com/2013/05/ejemplo-de-un-analisis-de-riesgos.html>
- Prieto, C. P. (16 de Enero de 2025). *Criminología Corporativa*. Obtenido de <https://criminologiacorporativa.com/art%C3%ADculos/f/objetivos-del-informe-de-investigaci%C3%B3n-corporativa>
- Lawrence J. Fennelly, M. A. (2018). *CPTED and Traditional Security Countermeasures*. Boca Raton, Florida: Taylor & Francis Group, LLC.
- Montes, J. L. (01 de Enero de 2022). Diplomado en Seguridad Patrimonial y Prevención de Pérdidas. Ciudad de México.
- Normalización, O. I. (2018). *Online Browsing Platform (OBP)*. Obtenido de <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>
- Revista de Seguridad 360. (18 de 06 de 2024). ¿Qué es seguridad patrimonial? Base Latinoamerica, Latinoamerica.
- Solutions, lpinnovations. (04 de 04 de 2021). *Solutions, lpinnovations*. Obtenido de www.lpinnovations.com