Revista
EL MUNDO CAMBIÓ

EDICIÓN 18
2026

LO QUE APRENDÍ DE CHERNOBYL: EL SILENCIO COMO RIESGO ESTRATÉGICO EN LA GESTIÓN DE CRISIS

Ing. Erick Sarante
República dominicana

EL MUNDO CAMBIO

2 de mayo de 2026

Revista
El Mundo Cambió

Titulares

LO QUE APRENDÍ DE CHERNOBYL: EL SILENCIO COMO RIESGO ESTRATÉGICO EN LA GESTIÓN DE CRISIS
Ing. Erick Sarante

11

INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD FÍSICA AGROINDUSTRIAL: EL CAMBIO QUE LATINOAMÉRICA NO PUEDE IGNORAR
Juan Carlos Mejía Alarcón

16

DISEÑO DE LA SEGURIDAD PERIMETRAL EN INSTALACIONES MODERNAS
Javier Nery Rojas B., MBA, CPP

19

TRUST BUT VERIFY CUANDO SUENA EL PRIMER DISPARO, YA PERDISTE, EL ERROR QUE NADIE QUIERE ADMITIR.
Eduardo E. Hurtado – MBA, CPP

22

DIMENSIÓN DE LA SEGURIDAD MULTIDIMENSIONAL Y SU INTERVENCIÓN EN EL DELITO COMPLEJO
Oleskyenio Flórez Rincón PhD

29

EL NUEVO MAPA DEL CRIMEN: CRIMINOLOGÍA CORPORATIVA Y LAS AMENAZAS INVISIBLES DEL SIGLO XXI
Carlos Eduardo Valenzuela Oviedo

35

¿CORTINA DE HUMO?
General. (R) Juan Carlos Buitrago Arias

42

GENERACIÓN ASISTIDA: EL PRECIO INVISIBLE DE PENSAR MENOS EN LA ERA DE MÁS INFORMACIÓN
Mariana Tovar Mora

45

Hasta

46% Dto.

Para comprarle Samsung a Mamá

Brilla · CELYA · Addi · 0% · Entrega y estreno

BARRANQUILLA
CC Buenavista 1
Piso 2 Local 219
CC Villa Country
Piso 1 Isla zona Común
Pasillo Central
CC Portal del Prado
Isla Área comun 16
Viva Centro Comercial
Isla 222
CC Parque Alegra
Piso 1 Isla 1-118A
SOLEDAD
CC Plaza del Sol
Local 267 - 268

BOGOTÁ
CC Plaza de las Américas
Local 1716
CC Gran Estación
Isla 1 - 103
CC Gran Estación
Isla diagonal a101

CALI
CC Llanogrande
Palmira, Valle
Burbuja 702 frente a
Ron Viejo de Caldas
CC Único 1
Burbuja 933

CARTAGENA
CC Mall Plaza el Castillo
Local 110 - 111 piso 1
CC Mall Plaza el Castillo
Isla
CC Plaza Bocagrande
Piso 1 Isla 1-32
TURBACO
CC Plaza 90
Isla 13

SANTA MARTA
CC Ocean Mall
2° piso local 61 y 62
CC Buena Vista
Isla 137

VALLEDUPAR
CC Mayales Plaza
Local 236 a Isla #6
CC Guatapuri
1° piso al lado de la
plazoleta de Juan valdez

VISA · Mastercard · American Express · Diners Club · PSE · Davivienda · Bancolombia · Banco de Bogotá

NUESTRO EQUIPO

administracion@revistaelmundocambio.com

+57 300 6412376

EXCELENCIA

OBSERVATORIO DE DERECHOS HUMANOS

El Observatorio Interamericano de DDHH & Desarrollo Sostenible,
En representación de la
Oficina Interamericana para la Paz y el Desarrollo Sostenible,
El nodo global de Observatorios de DDHH, La Federación Internacional para los DDHH y el Movimiento Mundial para los DDHH,

Acredita a:

EL MUNDO CAMBIO

Como

EMPRESA DEFENSORA Y PROMOTORA DE LOS DDHH

Dando fé del cumplimiento de los objetivos 5, 10, y 16 del pacto global para el Desarrollo sostenible.

ODS RECONOCIMIENTO A LAS BUENAS PRACTICAS

030248

Jean Francois Thomas Schmidt
WHRDC Representative for Switzerland

CR. (RA) Juan Carlos Perez Espitia
Comisionado Evaluador

Concord California - EEUU Febrero 26 2026.
eeuu@oippds.org - www.oippds.org
RES: O800131/0019 / 2026

Expedido y registrado bajo licencia Internacional : Convenio OIPPDS/023456/ESP. Impreso en Costa Rica. Todos los derechos reservados ®

Revista

EL MUNDO CAMBIÓ

Editorial:

La presente edición de Revista El Mundo Cambió reúne una serie de análisis estratégicos que reflejan la evolución de la seguridad, el riesgo y las dinámicas del crimen en un entorno cada vez más complejo, interconectado y desafiante. A través de distintas miradas —operativas, académicas y corporativas—, esta edición pone en evidencia una realidad ineludible: los riesgos del siglo XXI ya no pueden entenderse desde enfoques tradicionales, fragmentados o reactivos.

Abrimos esta edición con “Lo que aprendí de Chernobyl: el silencio como riesgo estratégico en la gestión de crisis”, del **Ing. Erick Sarante**, quien nos invita a mirar más allá del accidente nuclear para entender una falla estructural mucho más profunda: la incapacidad de gestionar la información en contextos críticos. El autor plantea que el verdadero riesgo no fue únicamente técnico, sino comunicacional, dejando una lección vigente sobre la importancia de la transparencia, la señalización temprana y la toma de decisiones en entornos de alta incertidumbre.

En segundo lugar, “Inteligencia artificial en la seguridad física agroindustrial: el cambio que Latinoamérica no puede ignorar”, de **Juan Carlos Mejía Alarcón**, aborda una brecha crítica en el sector agroindustrial. El autor expone cómo, a pesar del avance tecnológico en producción, la seguridad física sigue anclada en modelos obsoletos, y plantea a la inteligencia artificial como un multiplicador de eficiencia, anticipación y control en entornos operacionales complejos.

A continuación, “Diseño de la seguridad perimetral en instalaciones modernas”, de **Javier Nery Rojas B., MBA, CPP**, desarrolla un enfoque técnico y estructurado sobre la protección física desde el perímetro. El autor resalta la importancia de integrar barreras, control de accesos y vigilancia como un sistema cohesionado, donde cada elemento cumple una función dentro de una arquitectura de seguridad más amplia.

Seguidamente, “Trust but verify: cuando suena el primer disparo, ya perdiste, el error que nadie quiere admitir”, de **Eduardo E. Hurtado, MBA, CPP**, presenta una reflexión contundente sobre la seguridad de dignatarios y la gestión del riesgo en escenarios críticos. El autor desmonta la falsa percepción de éxito basada en la reacción, y plantea que la verdadera efectividad radica en la prevención, la anticipación y la verificación constante de los sistemas de seguridad.

En esta misma línea estratégica, “Dimensión de la seguridad multidimensional y su intervención en el delito complejo”, del PhD **Oleskyenio Flórez Rincón**, propone un cambio de paradigma en la forma de entender la criminalidad contemporánea. El autor expone cómo el delito ha evolucionado hacia estructuras sistémicas e interconectadas, lo que exige respuestas integradas, inteligencia convergente y una ruptura con la fragmentación institucional tradicional.

Posteriormente, “El nuevo mapa del crimen: criminología corporativa y las amenazas invisibles del siglo XXI”, de **Carlos Eduardo Valenzuela Oviedo**, traslada el análisis al interior de las organizaciones. A través de la criminología corporativa, el autor revela cómo las amenazas más críticas ya no son externas, sino internas, impulsadas por factores psicológicos, culturales y tecnológicos que requieren un enfoque preventivo y estratégico.

En “¿Cortina de humo?”, el **General (R) Juan Carlos Buitrago Arias** expone con claridad la magnitud del comercio ilícito de tabaco en la región, desmontando la idea de que se trata de un fenómeno menor. El autor evidencia cómo estas economías ilegales se articulan con estructuras criminales más amplias, adaptándose constantemente y desafiando las capacidades institucionales de control y respuesta.

Finalmente, cerramos esta edición con “Generación asistida: el precio invisible de pensar menos en la era de más información”, de **Mariana Tovar Mora**, quien aporta una mirada fresca y reflexiva desde el ámbito académico. La autora analiza el impacto de la inteligencia artificial en el aprendizaje, advirtiendo sobre los riesgos de dependencia tecnológica y la posible pérdida de habilidades críticas, al tiempo que plantea la necesidad de un uso consciente y estratégico de estas herramientas.

Esta edición nos deja una conclusión clara: los desafíos actuales —ya sean en seguridad, crimen, tecnología o educación— no pueden abordarse con las lógicas del pasado. La anticipación, la integración de capacidades, la gestión inteligente de la información y el fortalecimiento del pensamiento crítico se consolidan como pilares fundamentales para enfrentar un entorno donde lo visible ya no siempre es lo más peligroso.

ING. CARLOS ROJAS

www.pph.com.co

PPH

Seguridad Privada

PPH ofrece servicios integrales de **seguridad privada,** incluyendo **vigilancia fija y móvil**, escoltas, **medios tecnológicos**, asesoría y **más...**

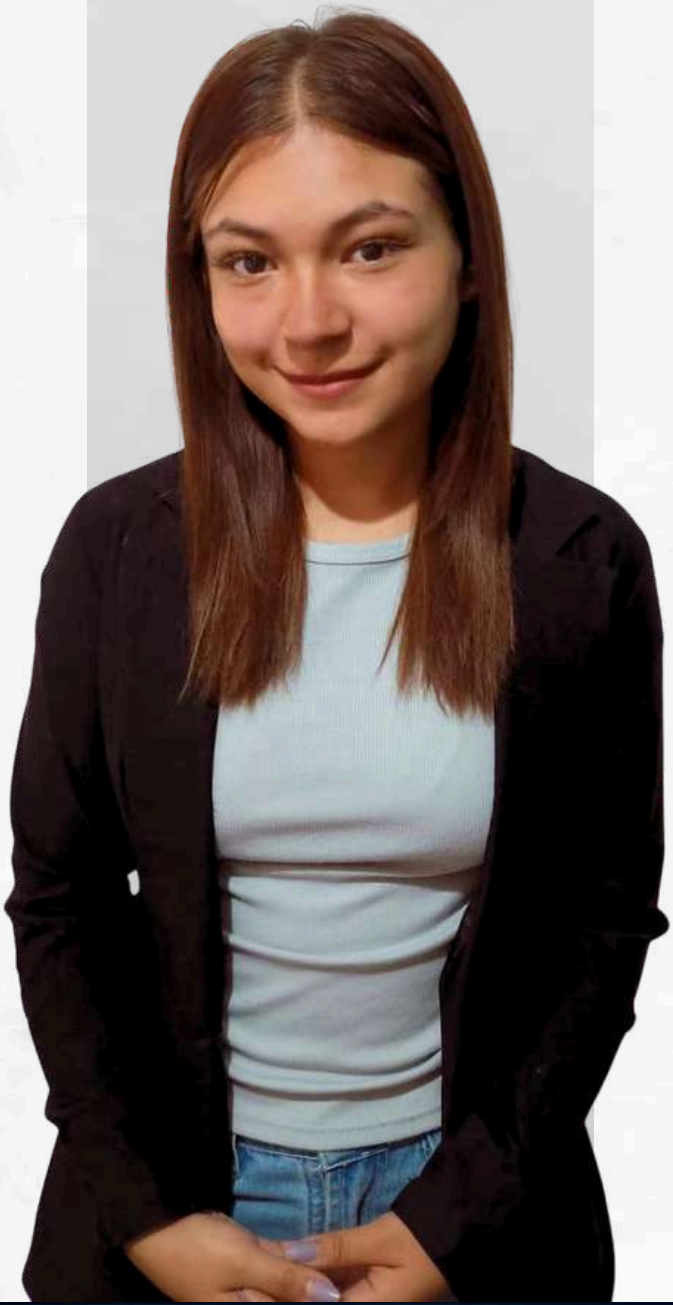
Calle 143 #46-09
Bogotá, Colombia

601 744 25 10

director.comercial@pph.com.co

PROFESIONAL DE LA SEMANA

MARIANA TOVAR MORA



Mariana Tovar Mora es una joven académica colombiana con una sólida proyección en el campo de la gestión de la información y el análisis crítico de los entornos digitales contemporáneos. Nacida en 2007 en Bogotá, actualmente cursa estudios en Archivística y Ciencias de la Información Digital en la Universidad Distrital Francisco José de Caldas, donde ha orientado su formación hacia la comprensión integral del papel de la información en la sociedad actual.

Su enfoque académico trasciende lo técnico, incorporando una visión analítica que reconoce la información como un elemento esencial en la construcción de memoria colectiva, identidad social y pensamiento crítico. Este perfil se ha fortalecido mediante su interés en el pensamiento histórico, lo que le permite interpretar los fenómenos contemporáneos con una perspectiva contextualizada y reflexiva.

Mariana ha desarrollado un interés particular en los impactos sociales de la transformación tecnológica, especialmente en relación con el acceso masivo a la información y el uso creciente de herramientas como la inteligencia artificial. Su trabajo se orienta a examinar cómo estas dinámicas están redefiniendo los procesos de aprendizaje, la toma de decisiones y la forma en que las nuevas generaciones interactúan con el conocimiento.

Con una clara vocación hacia la reflexión y la generación de conciencia, Mariana busca contribuir al desarrollo de una sociedad más crítica y preparada frente a los desafíos del entorno digital. Su propósito no se limita al ámbito profesional, sino que se proyecta hacia la construcción de un impacto significativo, promoviendo el uso responsable de la tecnología y el fortalecimiento de capacidades analíticas en contextos de alta complejidad informativa.

En síntesis, representa una nueva generación de profesionales que entienden que el verdadero valor del conocimiento no reside únicamente en su acceso, sino en la capacidad de interpretarlo, cuestionarlo y transformarlo en herramientas para el desarrollo social.

ESTE 2026 TIENE PARA TI

PREMIOS A LA EXCELENCIA PROFESIONAL

CATEGORIAS A LAS CUALES TE PUEDES POSTULAR

- Profesional Destacado del Año 2026
- Empresa Revelación en Seguridad del Año
- Liderazgo Estratégico en Seguridad Corporativa
- Innovación en Gestión de Riesgos
- Excelencia en Seguridad Logística y Cadena de Suministro
- Transformación Digital en Seguridad
- Cultura Organizacional en Seguridad
- Gestión Integral de Crisis y Continuidad

¿COMO TE POSTULAS?

Envía tu **hoja de vida al correo,** especificando la categoría a la que aplicas. Además, **completa el formulario** de inscripción.

VIERNES 28 AGOSTO

CORFERIAS
BOGOTA - COLOMBIA

POSTULATE

administracion@revistaelmundocambio.com

CONTACTOS

+57 3007317523

EL MUNDO CAMBIO

ESS+ FERIA INTERNACIONAL DE SEGURIDAD

EN MARCO DE LA **FERIA INTERNACIONAL** DE SEGURIDAD Y RIESGO 2026

EL MUNDO CAMBIO

El **VI Encuentro Mundial de Líderes de Seguridad y Riesgos**, organizado por la **Revista El Mundo Cambió**, cuenta con el respaldo de **importantes aliados estratégicos** que creen en la transformación del sector:

ASIS INTERNATIONAL® Bogotá Chapter

ESS+ FERIA INTERNACIONAL DE SEGURIDAD

PR HUMANA SOLUCIONES

Universidad Militar Nueva Granada

MUNDO HELP

WORLD UAV FEDERATION COLOMBIA

Este gran espacio internacional reunirá a líderes, expertos y organizaciones comprometidas con la seguridad, el riesgo y la innovación.

¿Quieres ser patrocinador oficial de este gran encuentro?

📩 Escríbenos y únete como aliado estratégico:
administracion@revistaelmundocambio.com

LO QUE APRENDÍ DE CHERNOBYL:
EL SILENCIO COMO RIESGO ESTRATÉGICO EN LA GESTIÓN DE CRISIS

Ing. Erick Sarante,
Chief Security & Resilience Officer Grupo Seahawks.
República Dominicana

Imagen 1: El Escudo de la Verdad y el Sarcófago

Introducción: más que un accidente

El 26 de abril de 1986, el mundo no solo presenció un accidente nuclear en la Central Vladimir Ilich Lenin; asistió al colapso de un sistema sustentado en la opacidad. Cuatro décadas después, Chernobyl ha dejado de ser únicamente un evento de la ingeniería nuclear para consolidarse como un caso paradigmático de falla sistémica en la gestión de crisis.

Como plantea Svetlana Alexiévich (1997), el desastre no se limitó a la explosión del reactor: fue también una implosión moral y comunicacional. El problema no fue exclusivamente el diseño del reactor RBMK-1000, sino la incapacidad estructural de procesar y comunicar información crítica bajo presión.

El retraso de aproximadamente 36 horas en la evacuación de Prípiat, junto con la negativa inicial del Estado soviético a informar a la comunidad internacional, no solo incrementaron la exposición radiológica, sino que erosionaron la legitimidad institucional. Este patrón (que puede definirse como un déficit de señalización en entornos de alta incertidumbre) sigue siendo, en 2026, uno de los principales multiplicadores de riesgo en la seguridad global.

Chernobyl y la lógica del silencio: cuando la información falla

Chernobyl demuestra que, en una crisis, la información es un activo estratégico. La decisión de priorizar la gestión de percepciones sobre la contención del evento generó una asimetría informativa con efectos exponenciales.

Plokhy (2018) documenta cómo la respuesta tardía limitó tanto la mitigación local como la cooperación internacional en las primeras horas críticas. En términos operativos, esto implicó una ampliación del radio de impacto y una pérdida de control narrativo que agravó la crisis.

Es importante distinguir entre causas: el diseño del reactor contribuyó al accidente, pero fue la gestión deficiente de la información la que amplificó sus consecuencias humanas y geopolíticas. En este sentido, el silencio no actúa como mecanismo de contención, sino como acelerador del riesgo.
Esta lógica se traduce en un principio clave de resiliencia: los sistemas que ocultan sus vulnerabilidades no reducen su exposición, la redistribuyen de forma ineficiente y tardía.

De Chernobyl al presente: dos formas de opacidad

La relevancia contemporánea del caso radica en que el problema no ha desaparecido, sino que ha evolucionado. Hoy, la opacidad opera en dos dimensiones distintas pero estructuralmente conectadas.

Por un lado, la opacidad reactiva (como en Chernobyl) se manifiesta después de un evento crítico, cuando las instituciones intentan controlar la narrativa para preservar estabilidad política. Este enfoque incrementa el daño al retrasar decisiones clave.

Por otro, la opacidad preventiva caracteriza entornos donde la información se restringe antes de una crisis potencial, con el objetivo de mantener ventajas estratégicas. Este es el caso de programas nucleares con ambigüedad deliberada.

La diferencia es temporal, pero el riesgo es común: en ambos escenarios, la información incompleta distorsiona la toma de decisiones y aumenta la probabilidad de errores de cálculo. Como advierte Jervis (1976), la percepción errónea bajo incertidumbre es uno de los principales detonantes de escalada en política internacional.

Geopolítica nuclear y riesgos sistémicos

Estas dinámicas son visibles en múltiples escenarios actuales. En Europa del Este, instalaciones nucleares en zonas de conflicto han transformado infraestructuras críticas en activos estratégicos vulnerables. Informes recientes del Organismo Internacional de Energía Atómica (IAEA, 2023–2025) señalan que el riesgo ya no es únicamente técnico, sino operacional: incluye sabotaje, presión militar y manipulación informativa.

En Medio Oriente, la opacidad adquiere una lógica distinta. A diferencia de Chernobyl (donde el secreto fue reactivo), aquí predomina una opacidad preventiva orientada a la disuasión. Como explica Parsi (2017), la ambigüedad en torno a capacidades nucleares genera un equilibrio inestable basado en percepciones incompletas. El riesgo no es un accidente, sino un error de interpretación.

Ambos casos comparten un elemento estructural: la falta de verificabilidad. Sin mecanismos confiables de validación, el margen de incertidumbre se amplía y con él la posibilidad de escaladas no intencionadas.

A esto se suman escenarios de baja visibilidad, como el Sahel o Sudán, donde la ausencia de información confiable limita la respuesta internacional. El Global Risks Report (World Economic Forum, 2024) identifica esta dinámica como parte de un fenómeno más amplio: la acumulación de riesgos invisibles con efectos transnacionales, desde migración hasta crisis sanitarias.

Chernobyl demostró que los riesgos ignorados no desaparecen; se desplazan y amplifican.

Implicaciones operativas: gestionar información es gestionar riesgo
El principal aprendizaje de Chernobyl no es histórico, sino operativo. La gestión de crisis contemporánea requiere integrar la información como capacidad estratégica medible.
Tres variables resultan críticas:

- Tiempo de señalización: intervalo entre detección y comunicación efectiva
- Capacidad de verificación: calidad y credibilidad de los datos disponibles
- Arquitectura de decisión: reducción de cuellos de botella en la transmisión de información

Imagen 2: Resiliencia y Transparencia contra las Narrativas

P&P CONSULTING

P&P CONSULTING

LA CONFIABILIDAD EN MANOS DE EXPERTOS

- Consulta de talante judicial
- Visitas domicialiarias
- Referenciaciones académica y laboral
- Investicaciones administrativas
- Apoyo Judicial

Nuestra experiencia

Contamos con profesionales de más de **30 años** en el mercado.
Lideres en investigación empresariales.
Personal experto en inteligencia y contra inteligencia.

admipypconsulting@gmail.com
@pypconsulting_

Estas dimensiones permiten evaluar la resiliencia real de un sistema. En términos prácticos, reducir el tiempo de notificación y aumentar la transparencia verificable disminuye el costo total de contención y limita la propagación del impacto.
Hacia una nueva arquitectura de transparencia

A pesar del avance tecnológico, el comportamiento humano frente al error mantiene patrones constantes: negación, retraso y control de la narrativa.
Desde una perspectiva de seguridad y resiliencia, tres líneas de acción resultan críticas:

1. Protocolos de ayuda automática

Desvincular la asistencia en desastres de gran escala de decisiones políticas, mediante mecanismos de activación inmediata.

2. Soberanía compartida de datos críticos

Convertir la información sobre riesgos ambientales, sanitarios y nucleares en un bien público global, supervisado por organismos independientes con capacidad de verificación.

3. Contención del negacionismo estratégico

Establecer estándares internacionales que desincentiven la ocultación de información que afecte la seguridad humana.

Conclusión: de la narrativa al control

Chernobyl no fue únicamente una catástrofe tecnológica, sino una falla en la gobernanza de la información. La naturaleza del riesgo no cambió; lo que falló fue la capacidad de interpretarlo y comunicarlo a tiempo.
Como advierte Snyder (2017, cap. 10), la negación de la realidad debilita las instituciones. En el ámbito de la seguridad, esto se traduce en mayor tiempo de respuesta, mayor costo operativo y menor control estratégico.
La lección central es clara:
la ventaja en crisis no reside solo en capacidades materiales, sino en la capacidad de reducir la incertidumbre antes que el adversario o antes que el propio sistema colapse.
Chernobyl dejó una advertencia estructural: cuando la información falla, todo lo demás se vuelve secundario.

Imagen 3: El Valor de la Verdad y el Confinamiento de Chernobyl

Listos para tus eventos

Eleva tu próxima fiesta con comidas artesanales, servicio de buffet y catering sin estrés de expertos locales.

RESERVA AHORA

Contáctanos
+57 300 9772520

Sazón del Arriero

INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD FÍSICA AGROINDUSTRIAL: EL CAMBIO QUE LATINOAMÉRICA NO PUEDE IGNORAR

Juan Carlos Mejía Alarcón
Gerente General Silver-Group S.A.S. | **Ecuador**

El problema que nadie nombra correctamente

Cuando hablamos de inteligencia artificial en el sector agroindustrial latinoamericano, la conversación casi siempre gira en torno a producción: biomasa de camarón, rendimiento de cultivos, trazabilidad de cadena fría. Son conversaciones válidas. Pero hay una dimensión que permanece casi invisible en los foros especializados: la seguridad física patrimonial.

Ecuador es el segundo exportador mundial de camarón. Perú lidera la acuicultura de trucha en América del Sur. Colombia, Chile y Honduras sostienen cadenas agroindustriales que mueven miles de millones de dólares anuales. Sin embargo, la gran mayoría de estas operaciones — muchas ubicadas en zonas rurales, fluviales o de difícil acceso — siguen gestionando su seguridad con métodos que no han evolucionado en décadas: rondas manuales, registros en papel, comunicación por radio análoga y protocolos que nadie consulta durante una emergencia real.

El problema no es de recursos. Es de paradigma.

Lo que la IA ya puede hacer

La inteligencia artificial lleva años transformando la seguridad en banca, retail y transporte aéreo. En esos entornos los sistemas detectan anomalías en tiempo real, correlacionan incidentes y generan alertas antes de que el incidente ocurra. La pregunta que los profesionales de seguridad en agroindustria debemos hacernos no es si la IA puede hacer lo mismo en una camaronera — porque técnicamente ya puede. La pregunta es por qué todavía no lo estamos implementando.

Hoy es posible desplegar agentes de inteligencia artificial especializados en seguridad física que operan 24/7 sin fatiga, procesan protocolos embebidos, registran novedades en tiempo real y producen informes ejecutivos automáticos — todo desde cualquier dispositivo móvil. El costo de entrada es significativamente menor al de un supervisor adicional. La consistencia operacional, infinitamente mayor.

El triángulo del riesgo en entornos acuícolas y agroindustriales.

Las operaciones acuícolas y agroindustriales presentan tres vectores críticos que la seguridad convencional gestiona mal:

Dispersión territorial. Una operación de camaroneras puede cubrir cientos de hectáreas con múltiples piscinas, casetas, bodegas y puntos de acceso fluvial. La cobertura humana completa es económicamente inviable. Los puntos ciegos son estructurales, no accidentales.

Aislamiento operacional. Muchas instalaciones operan en zonas con conectividad limitada, lejos de respuesta policial inmediata. El tiempo de respuesta ante un incidente puede medirse en horas, no minutos, lo que exige que los equipos de seguridad internos tomen decisiones correctas sin dependencia de apoyo externo.

Amenaza interna subestimada. En operaciones rurales con alta rotación de personal y supervisión limitada, la ecuación del Triángulo del Fraude — motivación, oportunidad y justificación — se presenta con condiciones especialmente favorables para el incidente.

De la reacción a la anticipación

El modelo de seguridad tradicional en agroindustria es fundamentalmente reactivo. El guardia reporta el incidente después de que ocurrió. El supervisor lo documenta. El informe llega días después. Las medidas correctivas se discuten en una reunión que genera un acta que nadie vuelve a revisar. La IA permite invertir completamente esa lógica.

Un agente de inteligencia artificial entrenado con los protocolos específicos de la operación puede correlacionar datos de acceso, patrones de ronda y registros de novedades en tiempo real. Puede detectar que un vehículo no registrado ingresó por un punto secundario en el tercer turno consecutivo, o que un perímetro lleva 72 horas sin reporte de ronda. Nada de eso requiere infraestructura compleja. Requiere datos estructurados, protocolos bien definidos y un agente entrenado para procesarlos con criterio. El resultado no es reemplazar al equipo humano: **es multiplicar su efectividad.**

El profesional de seguridad en la era de la IA

La inteligencia artificial no amenaza al profesional de seguridad física bien posicionado. Lo potencia. Pero sí reemplaza al profesional que no evoluciona.

El Director de Seguridad del futuro no es el que gestiona más guardias. Es el que diseña sistemas más inteligentes, interpreta datos con criterio estratégico y comunica el riesgo en lenguaje de negocio a la alta dirección. Latinoamérica tiene el talento humano para hacer esa transición. Lo que necesita es decisión institucional, referentes aplicados y profesionales dispuestos a liderar el cambio desde adentro.

El sector agroindustrial y acuícola de nuestra región mueve economías enteras. Merece una gestión de seguridad a la altura de su relevancia estratégica. Y esa gestión, hoy, pasa necesariamente por la inteligencia artificial.

SECURITY SHOPS

Este mes de la *madre,* regale tranquilidad

Modernice la seguridad de su edificio con **Portería Automatizada**

3 MESES DE MONITOREO SIN COSTO

MÁS SEGURIDAD PARA QUIENES MÁS IMPORTAN

VIDEO PORTERO IP

Comunicación en tiempo real con reconocimiento facial.

CONTROL DESDE APP

Autorice o deniegue accesos desde su celular.

ACCESO VEHICULAR AUTOMATIZADO

Ingreso con tags o códigos únicos.

CCTV CON MONITOREO ACTIVO 24/7

Visualización en vivo y supervisión permanente.

CENTRAL DE MONITOREO 24/7

Integración con monitoreo profesional y reacción inmediata.

ESCRÍBANOS POR **WHATSAPP**

317 221 8128

DIAGNÓSTICO SIN COSTO »

Diseño de la Seguridad Perimetral en Instalaciones Modernas

Javier Nery Rojas B., MBA, CPP
Bogotá -Colombia

La seguridad física de una instalación no comienza dentro de los edificios; empieza en el perímetro. Un programa integral de seguridad perimetral debe considerar múltiples niveles de protección: desde la delimitación externa hasta la protección de espacios interiores y del contenido dentro de los edificios.

1. La Importancia de las Barreras Perimetrales

Las barreras son elementos esenciales para definir los límites de una instalación y controlar la penetración no autorizada. Estas pueden ser naturales, estructurales o artificiales. Sin embargo, ninguna barrera es completamente impenetrable: siempre requieren medidas complementarias de vigilancia, detección y patrullaje.

Barreras naturales como cuerpos de agua, desniveles o vegetación densa, si bien proporcionan un obstáculo inicial, deben ser reforzadas con barreras artificiales o cerramientos estructurales para ser realmente efectivas.

Barreras estructurales y artificiales incluyen cercas, muros y concertinas, diseñadas para resistir el escalamiento o la intrusión y, al mismo tiempo, servir como elemento disuasorio psicológico.

2. Tipos de Cerramientos

Cercas de Malla Eslabonada
La malla es el cerramiento más común en instalaciones modernas debido a su resistencia y facilidad de mantenimiento. Para ser efectiva:

- Debe emplearse alambre calibre 9 o superior, con alambre de púas en la parte superior.
- Su altura mínima es de 7 pies, comenzando a al menos 3 pulgadas del suelo.
- La base debe estar estabilizada contra levantamiento, mediante varillas metálicas o antepechos de concreto.
- La malla debe estirarse y fijarse a postes rígidos de metal, asegurando que las aperturas no superen las 2 pulgadas cuadradas.
- Una guarda de altura, con ángulo de 45° hacia afuera y 3 hilos de alambre de púas, debe elevar la altura total a 8 pies.
- Elementos cercanos como árboles o estructuras deben ser considerados y reforzados con medidas que impidan el escalamiento.

Cercas de Alambre de Púas

Se utilizan principalmente en instalaciones con requerimientos de alta seguridad temporal o rural:

- Alambre doble entorchado calibre 12, con puntas de cuatro puntas, separadas cada 4 pulgadas.
- Altura mínima de 7 pies y agregando guarda de altura similar a la malla eslabonada.

Postes metálicos espaciados cada 6 pies y hileras verticales no mayores a 6 pulgadas entre sí.

Concertinas

La concertina es un alambre de acero recortado en espiral, desarrollado originalmente por fuerzas militares, que forma barreras de hasta 50 pies de longitud y entre 16 a 60 pulgadas de altura por rollo. Es ideal para despliegue rápido y se usa generalmente en aplicaciones temporales o zonas críticas. Aunque extremadamente difícil de penetrar, requiere fijación segura al suelo y unión entre rollos.

Muros de Mampostería

Los muros de ladrillo, piedra o bloques ofrecen protección física y privacidad. Para mantener su efectividad:

- Deben alcanzar al menos 7 pies de altura, complementados con 3–4 hileras de alambre de púas.
- Su diseño interno debe permitir la vigilancia desde dentro, evitando puntos ciegos que puedan facilitar escalamiento.
- Deben cumplir con reglamentos locales que exigen transparencia mínima para cerramientos perimetrales.

3. Control de Accesos

Cada abertura en la barrera representa un punto vulnerable. Por ello, el número, tamaño y operación de portones debe limitarse estrictamente:

- Puertas peatonales: ancho de 4 a 6 pies para controlar la entrada y salida sin perder vigilancia.
- Portones vehiculares: adecuados al tipo de tráfico; pueden ser de hoja simple, doble, corrediza o elevable, manual o eléctricamente operados.
- Todas las puertas deben estar aseguradas cuando no están en operación y bajo supervisión de personal de seguridad.
- Talanqueras tipo paso a nivel permiten control del flujo vehicular y peatonal.

Otras aberturas como alcantarillas, drenajes, conductos y registros de servicios también requieren protección mediante rejillas, alambre de púas o cerramientos asegurados, especialmente si su área supera las 96 pulgadas cuadradas.

4. Protección y Vigilancia del Perímetro

Una barrera solo es efectiva si se combina con patrullaje, inspección y vigilancia constante. Las mejores prácticas incluyen:

- Mantener zonas despejadas a ambos lados de la barrera para maximizar visibilidad.
- Remover objetos que faciliten el escalamiento como postes, cuerdas o escombros.
- Podar vegetación, rellenar erosiones y reparar daños en mallas o muros.
- Instalar sistemas de detección electrónica en zonas donde no sea posible mantener áreas despejadas.

5. Seguridad Interna: Segunda Línea de Defensa

Los patios internos, espacios entre edificios y perímetro, son considerados una segunda línea de defensa:

- Mantener áreas ordenadas para facilitar la detección de irregularidades.
- Evitar almacenamiento desordenado que pueda ocultar actividad sospechosa.
- Parqueaderos dentro del perímetro deben estar restringidos, patrullados e iluminados.
- Vehículos de carga deben estacionarse dentro del perímetro, preferiblemente “cola con cola” y sellados, evitando apertura no supervisada.

Conclusión

El diseño de la seguridad perimetral combina barreras físicas, control de accesos y vigilancia constante. Una instalación bien protegida no solo disuade a intrusos indecisos, sino que también minimiza riesgos internos y externos. Las barreras modernas, combinadas con patrullaje, iluminación y tecnología de detección, forman un sistema integral capaz de proteger personas, activos y operaciones críticas.

PRO HUMANA SOLUCIONES

El riesgo no avisa.
Pero tú sí puedes anticiparte.

Carlos Andrés Valencia Hernández.

Paola Andrea Ramírez Ávila.

Cada día, miles de trabajadores enfrentan situaciones que no están en los protocolos tradicionales

AUTOCUIDADO INTEGRAL Y CONSCIENTE
7 pasos para prevenir el riesgo público

Muy pronto disponible en todas las plataformas.

TRUST BUT VERIFY

CUANDO SUENA EL PRIMER DISPARO, YA PERDISTE, **EL ERROR QUE NADIE QUIERE ADMITIR**.

Eduardo E. Hurtado – MBA, CPP
EEUU

La gran mayoría de los ciudadanos estadounidenses piensan que hay algo que no debería discutirse y el hecho de que cuando se trata de proteger al jefe de Estado de los EE. UU., No estamos hablando de “hacer un buen trabajo” ni de “hacerlo lo mejor que sea humanamente possible”; estamos hablando de no fallar y punto. El éxito no es reaccionar bien, ni evacuar rápido, ni controlar el impacto o daños... el éxito es que nunca haya existido una amenaza real dentro del perímetro. Cuando algo pasa, aunque no haya víctimas, el sistema ya falló, y aquí es donde la exigencia debe ser clara y sin concesiones, los estadounidenses estamos financiando con miles de millones de dólares a uno de los dispositivos de seguridad más avanzados del mundo, como lo es el Servicio Secreto, encargado de proteger el activo más importante del país, como ocurrió en su momento con el presidente Donald Trump, y eso no es un contrato para intentarlo eficientemente, es un compromiso para ejecutarlo de manera efectiva y perfecta, sin margen de error. No se trata de criticar por criticar, se trata de entender que en este nivel no hay espacio para el “casi”, ni para justificar fallas con esfuerzo o valentía. La ciudadanía no paga por la intención, paga por resultados. Y el único resultado aceptable es uno, “que el dignatario nunca esté en una posición donde su vida dependa de reaccionar a tiempo”. Si llegamos a ese punto, entonces algo "en algún lugar" no se hizo como se debía; y, dado que la responsabilidad no puede delegarse, alguien debe dar una explicación al respecto.

En el ámbito de la protección de dignatarios, existe una realidad operativa que, aunque incómoda, debe ser aceptada sin matices, cuando ocurre un ataque y se hace necesario reaccionar tácticamente, el sistema de seguridad ya ha fallado en su objetivo primario. Este principio cobra especial relevancia al analizar un incidente reciente vinculado a un evento donde participaba el presidente Donald Trump, en el cual un individuo armado, alojado en el mismo hotel donde se desarrollaba la actividad, logró vulnerar controles de acceso, posicionarse en una zona crítica y abrir fuego, impactando a un oficial de seguridad. Aunque la amenaza fue enfrentada y contenida, no fue neutralizada de inmediato, lo que expone una serie de fallas estructurales más allá de la respuesta táctica. Este tipo de eventos no debe analizarse desde la óptica superficial del heroísmo o la rapidez de reacción, sino desde una perspectiva estratégica que permita entender por qué el atacante tuvo la oportunidad de actuar.

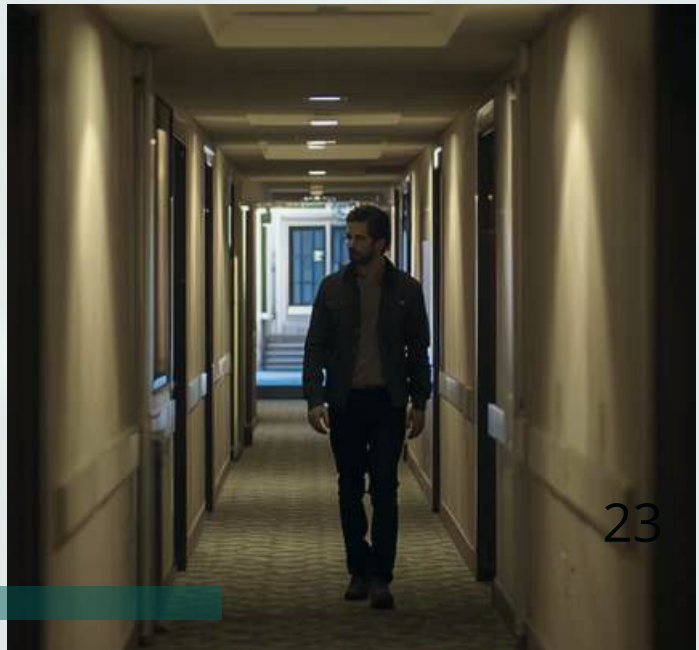
Durante años, la narrativa dominante dentro de la seguridad ejecutiva ha exaltado la preparación táctica como el eje central de la protección. Se entrena al personal en tiro bajo estrés, evacuación de emergencia, conducción evasiva y reacción ante amenazas activas, lo cual, sin duda, es necesario. Sin embargo, esta aproximación ha generado una distorsión peligrosa y es la creencia de que la capacidad de respuesta define la efectividad del sistema de seguridad. En realidad, la reacción es únicamente un mecanismo de contención del daño, no una demostración de éxito. Si un atacante logra ingresar al perímetro, superar controles y ejecutar una acción ofensiva, la cadena de seguridad ya ha presentado múltiples fallas acumulativas. La verdadera excelencia en protección de dignatarios no se mide por la calidad de la respuesta, sino por la capacidad de evitar que el incidente ocurra.

En este contexto, es imprescindible introducir un principio que debe ser considerado un estándar no negociable dentro de cualquier análisis de riesgos serio, asumir que un ataque es posible. Este concepto no es teórico ni opcional; es un "must" operativo dentro de metodologías como ESRM (Enterprise Security Risk Management) y HIRA (Hazard Identification and Risk Assessment). La **Seguridad Predictiva** se fundamenta precisamente en esta premisa, reconocer que el evento adverso puede materializarse y, en consecuencia, identificar señales tempranas, modelar escenarios y anticipar comportamientos. La seguridad preventiva, por su parte, toma esa información y la traduce en controles concretos diseñados para evitar que la amenaza se materialice. La integración de ambos enfoques no es un lujo, sino una necesidad estratégica, especialmente en entornos donde el impacto de un fallo puede ser catastrófico.

Un elemento crítico que debe incorporarse en esta ecuación es el principio de "**Trust but verify**" (Confía, pero verifica). Este concepto, ampliamente conocido pero frecuentemente mal aplicado, representa una disciplina operativa que obliga a validar constantemente la efectividad de los controles implementados. Confiar en que un sistema funciona sin someterlo a pruebas reales es una forma de complacencia. En el caso analizado, el atacante logró atravesar controles de acceso, lo que indica que existía una confianza en el sistema que no fue respaldada por una verificación rigurosa. En la práctica, este principio implica auditar continuamente los puntos de control, evaluar el desempeño del personal, realizar simulacros realistas y ejecutar ejercicios de red teaming para identificar vulnerabilidades antes de que sean explotadas. La confianza sin verificación no es profesionalismo; es exposición al riesgo.

La seguridad predictiva, correctamente aplicada, permite identificar patrones y señales que muchas veces pasan desapercibidas para equipos centrados exclusivamente en la reacción. En un entorno como un hotel que alberga un evento de alto perfil, cada individuo dentro del perímetro representa una variable de riesgo que debe ser evaluada. Esto incluye el análisis de reservas sospechosas, comportamientos atípicos, historial digital y posibles vínculos ideológicos o criminales. El uso combinado de inteligencia de fuentes abiertas (OSINT) y fuentes humanas (HUMINT) permite construir perfiles de riesgo que facilitan la detección temprana de amenazas. Además, el análisis de comportamiento en tiempo real puede revelar micro-indicadores como nerviosismo excesivo, movimientos erráticos o interés inusual en áreas restringidas. Estos elementos, aunque sutiles, pueden ser determinantes para prevenir un incidente.

Sin embargo, identificar el riesgo no es suficiente si no se traduce en medidas preventivas efectivas. La seguridad preventiva se materializa a través de controles diseñados para limitar la capacidad de acción de un potencial atacante. Esto incluye la segmentación de accesos, la creación de zonas buffer, la implementación de múltiples anillos de seguridad y la verificación cruzada de credenciales. En entornos de protección de dignatarios, no todos los individuos deben tener el mismo nivel de acceso ni la misma libertad de movimiento. La capacidad de restringir dinámicamente el acceso en función del comportamiento observado es una herramienta clave para mitigar riesgos. Asimismo, la intervención temprana mediante entrevistas, verificaciones adicionales o incluso la expulsión preventiva de un individuo sospechoso puede marcar la diferencia entre un evento controlado y una crisis de alto impacto.



PUBLICIDAD QUE TRASCIENDE FRONTERAS

Estrategia + Contenido = resultados reales.

Anunciar en la **Revista El Mundo Cambio!** Es una oportunidad unica **para destacar.**

Mas de **11 Millones de Visualizaciones** semanales llegando asi a 110 paises.

Mas de **400k de seguidores** en redes sociales

PAUTA CON REVISTA EL MUNDO CAMBIO / PAUTA CON REVISTA EL MUNDO CAMBIO

Contactanos hoy y potencia tu marca

300 7317523

EL MUNDO CAMBIÓ

Uno de los errores más frecuentes en la gestión de riesgos es la falta de comunicación efectiva de las amenazas identificadas y las medidas mitigantes. El análisis de riesgos no puede quedarse en un documento técnico que solo algunos entienden. Debe ser comunicado de manera clara, comprensible y operativa a todo el equipo involucrado. Un riesgo que no es entendido por el personal no puede ser gestionado adecuadamente. Las medidas mitigantes deben ser interiorizadas a través de entrenamiento constante, simulacros y ejercicios prácticos que permitan al equipo reaccionar de manera coordinada y efectiva. En situaciones críticas, el personal no actúa en función de lo que está escrito en un manual, sino de lo que ha practicado y comprendido profundamente.

El impacto del incidente analizado va mucho más allá del hecho de que no se hayan registrado fatalidades. Desde una perspectiva de gestión de riesgos, se trata de un evento de alto impacto con múltiples consecuencias operacionales, reputacionales y políticas. Un oficial resultó herido, se produjo una evacuación masiva, el evento fue suspendido, se activaron protocolos de crisis, el presidente y la primera dama fueron evacuados y la cobertura mediática generó un cuestionamiento directo a la efectividad del dispositivo de seguridad. Este tipo de impacto no puede ser minimizado. La pregunta que debe guiar el análisis no es qué tan bien se respondió, sino qué se pudo haber hecho para evitar que el incidente ocurriera.

El énfasis excesivo en la respuesta táctica también genera una dependencia peligrosa en el desempeño individual del operador. Se espera que el personal actúe con precisión y eficacia bajo condiciones de estrés extremo, lo cual, aunque deseable, no puede ser el único pilar del sistema de seguridad. Ningún operador es infalible, y la variabilidad humana bajo presión es un factor que debe ser considerado en el diseño del sistema. La seguridad moderna debe construirse sobre capas redundantes que reduzcan al mínimo la posibilidad de que un error individual escale a consecuencias críticas. Depender de un disparo certero como última línea de defensa no solo es una estrategia frágil, sino que está lejos de los estándares que exige la protección de dignatarios. Aquí es donde realmente cobra valor la seguridad predictiva. Un escenario en el que un oficial dispara cinco veces y falla todos los intentos no es aceptable desde ningún punto de vista operativo; además, cada disparo, por su naturaleza de alto riesgo, incrementa la probabilidad de daños colaterales. Lo que muchos aún no comprenden es que el mayor porcentaje del esfuerzo en la gestión de la protección debe concentrarse en evitar que el evento ocurra, no en tratar de manejar el factor sorpresa y confiar en que, bajo adrenalina y presión extrema, la respuesta será perfecta. En ese punto, las probabilidades de error son significativamente altas, y el sistema ya está operando en desventaja.

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE

30 Años
1996 - 2026

12° Congreso Mundial
Septiembre 1-2, 2026 | Miami

12° Congreso Mundial

Septiembre 1-2, 2026

Hyatt Regency Brickell
Miami, FL.

Prepárese para el evento más importante del año en comercio y seguridad, en Miami.

Costos por participación

Early Bird

Hasta junio 15 de 2026

Miembros BASC*: USD $580.00
Entrada General (No BASC): USD $580.00
Auditores Internacionales BASC: USD $650.00

Registro Regular

Desde junio 16 hasta agosto 31 de 2026

Miembros BASC*: USD $620.00
Auditores Internacionales BASC: USD $620.00
Entrada General (No BASC): USD $670.00
Tarifa especial para acompañantes:** USD $ 300.00

✓**Derecho a 1 almuerzo (1er o 2do día de la Conferencia).**
✓**1 entrada al Cóctel de Bienvenida.**

@CongresoMundialBASC_
@BASCGlobalConference

Contáctenos para inscripción:
Teléfono: +573102527801
E-mail: asistente.direccion@basc.org.co

*Miembros BASC: Empresas afiliadas y/o certificadas BASC, miembros de Juntas Directivas BASC, y colaboradores BASC.
**Aplica para conyuge e hijos.

El modelo operativo más efectivo es aquel que integra de manera jerárquica la seguridad predictiva, preventiva, la verificación constante y la capacidad de respuesta táctica. Primero, se debe aceptar que el ataque es posible y modelar los escenarios correspondientes. Luego, se deben diseñar e implementar controles preventivos que reduzcan la probabilidad de materialización del riesgo. A continuación, se debe verificar continuamente que estos controles funcionan como se espera, aplicando el principio de “Trust but verify”. Finalmente, se debe mantener una capacidad táctica robusta para responder en caso de que todas las capas previas fallen. Este enfoque no elimina el riesgo, pero lo gestiona de manera integral y sistemática.

La diferencia entre una seguridad funcional y una seguridad de élite radica en la capacidad de anticipación, la disciplina en la ejecución y la cultura organizacional orientada a la mejora continua. Los equipos de alto desempeño no se conforman con cumplir procedimientos; cuestionan constantemente sus propias suposiciones, buscan vulnerabilidades y se preparan para escenarios adversos incluso cuando la probabilidad es baja. La complacencia es, en última instancia, el mayor enemigo de la seguridad. Creer que un sistema es infalible es el primer paso hacia su fracaso.

El incidente analizado debe servir como un recordatorio contundente de que la seguridad de dignatarios no puede basarse únicamente en la capacidad de respuesta. La prevención, respaldada por una inteligencia sólida y una verificación constante, es el verdadero pilar de un sistema eficaz. La pregunta clave que todo equipo de seguridad debe hacerse no es cuán rápido puede reaccionar, sino por qué un atacante tendría la oportunidad de actuar. Responder esta pregunta con honestidad técnica, integrar las lecciones aprendidas en el análisis de riesgos y comunicar eficazmente las medidas mitigantes al equipo es lo que define la diferencia entre un sistema vulnerable y uno verdaderamente robusto.

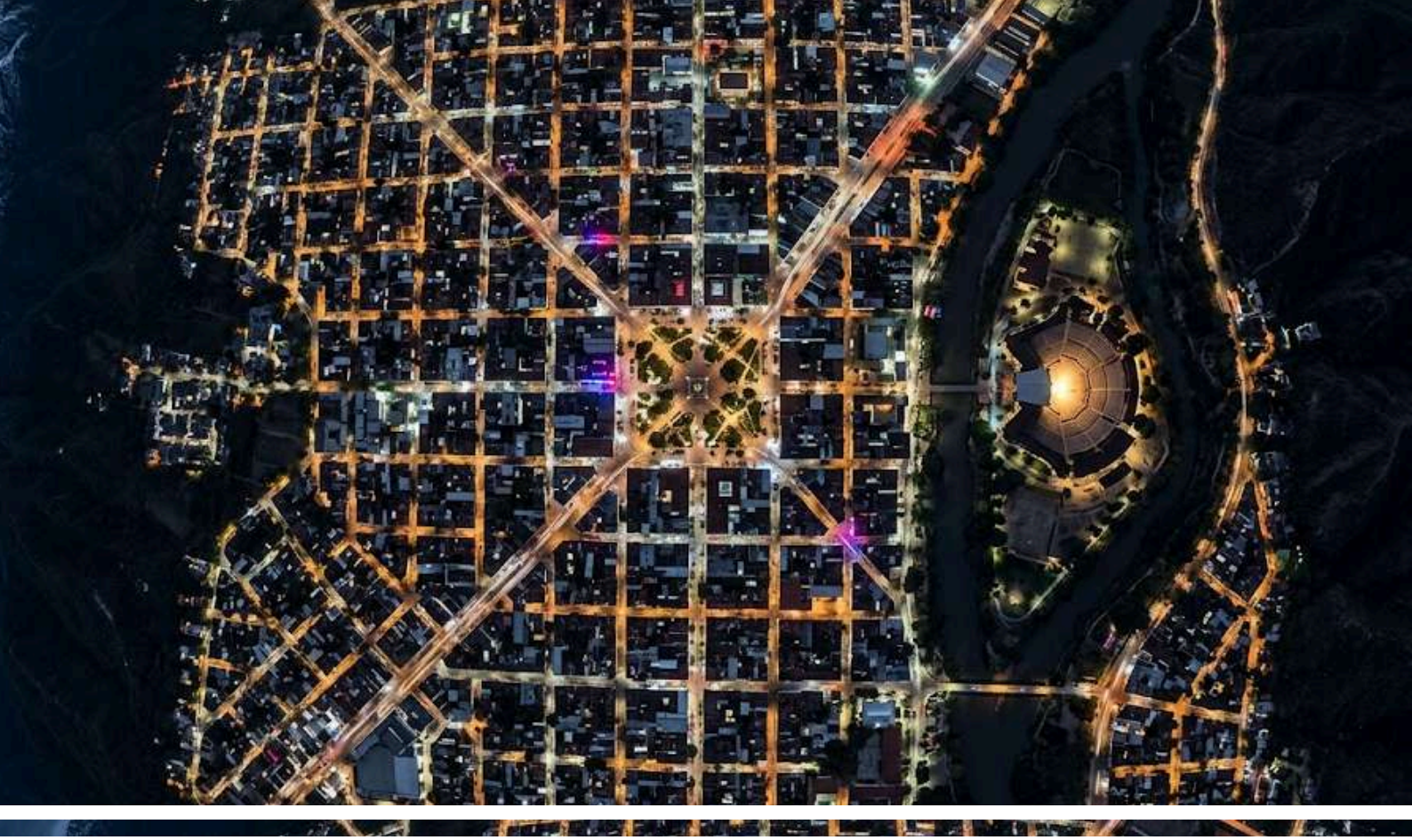
LA REXACA

DESPIERTA SIN GUAYABO

100% NATURAL

PRODUCTO A BASES DE AGUA , CIRUELA , ALCACHOFA, APIO, PEPINO Y PIÑA

@larexaca



DIMENSIÓN DE LA SEGURIDAD MULTIDIMENSIONAL Y SU INTERVENCIÓN EN EL DELITO COMPLEJO

Por Oleskyenio Flórez Rincón PhD
Colombia

Durante décadas, buena parte de la política criminal en América Latina ha cometido un error de origen: interpretar el delito como un fenómeno segmentado, aislado y lineal. Se persigue la extorsión como un problema autónomo, el microtráfico como una expresión barrial separada, el homicidio como una consecuencia individual, el narcotráfico como un asunto rural, la minería ilegal como una economía periférica y el contrabando como una simple infracción aduanera. Sin embargo, en la práctica, estos fenómenos no operan de forma independiente. Se conectan, se alimentan mutuamente y, en muchos casos, son ejecutados por las mismas estructuras criminales. El problema no es únicamente el delito: el problema es la lectura fragmentada que el Estado hace de él.

Ese es, precisamente, el punto de quiebre que obliga a repensar la seguridad desde una lógica multidimensional. No porque el concepto sea novedoso en lo doctrinal, sino porque resulta imprescindible en lo operativo. La criminalidad contemporánea ya no responde a esquemas rígidos ni a especializaciones estancas; muta, converge, se adapta y se expande. Su naturaleza ya no es lineal: es sistémica.

La criminalidad actual funciona como un ecosistema de rentas, violencias y capacidades ilegales. Una misma estructura puede controlar microtráfico en entornos urbanos, financiarse mediante extorsión, mover armas por corredores de contrabando, lavar capitales mediante economías legales, participar en minería ilegal y tercerizar homicidios para mantener control territorial. No se trata de delitos distintos ejecutados por actores distintos. Se trata, cada vez más, de una misma arquitectura criminal diversificando funciones, riesgos y mercados.

MAESTRÍA EN DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL

Más información: admisiones.madgsi@epfac.edu.co

INSCRIPCIONES ABIERTAS - 2026

DEL 23 DE FEBRERO AL 8 DE MAYO

MAESTRÍA EN
DIRECCIÓN Y GESTIÓN
DE LA SEGURIDAD INTEGRAL
ESCUELA DE POSTGRADOS DE LA FAC - EPFAC / SNIES 105260

INFÓRMATE AQUÍ

admisiones.madgsi@epfac.edu.co
(601) 3159816 Ext. 72557
Cel: 3218427993
www.epfac.edu.co

CON EL APOYO DE:

EL MUNDO CAMBIÓ

Mark Galeotti ha explicado que el crimen organizado contemporáneo dejó de comportarse como una jerarquía rígida para operar como una red flexible, oportunista y adaptativa. Ya no responde necesariamente a estructuras piramidales, sino a nodos funcionales que se conectan y desconectan según la oportunidad criminal. Esa flexibilidad es precisamente lo que les permite a las organizaciones criminales mutar de actividad sin perder capacidad operativa: hoy trafican cocaína, mañana controlan migración irregular, pasado mañana financian minería ilegal. No abandonan mercados: los acumulan.

Robert Muggah ha insistido en una idea similar: el crimen contemporáneo no se sostiene únicamente en la violencia visible, sino en infraestructuras criminales invisibles. Es decir, no basta con contar homicidios o capturar sicarios; hay que intervenir las finanzas, las redes logísticas, los mecanismos de corrupción, las economías ilícitas y la captura territorial que permiten que el crimen se reproduzca. El error del Estado ha sido seguir persiguiendo síntomas, mientras las estructuras conservan intacto el sistema que produce la violencia.

Este punto es fundamental: la criminalidad compleja no se define por la gravedad aislada del delito, sino por la interacción de múltiples delitos, actores, rentas y capacidades en una misma estructura funcional. La XXII Cumbre Judicial Iberoamericana fue clara al señalar que la criminalidad compleja no se limita al tipo penal, sino que se caracteriza por la convergencia de delitos conexos, pluralidad de actores, múltiples peritajes, cooperación internacional, afectación supraindividual y articulación con organizaciones criminales. Es decir: lo complejo no es solo el delito, sino el sistema que lo produce.

Esto obliga a una conclusión incómoda pero necesaria: buena parte de la arquitectura institucional del Estado sigue diseñada para perseguir delitos individuales, mientras el crimen ya opera como sistema integrado.

La fragmentación institucional ha producido una paradoja costosa: el Estado especializa cada vez más sus respuestas mientras el crimen integra cada vez más sus operaciones. El resultado es previsible: agencias separadas, información compartimentada, líneas investigativas desconectadas y estructuras criminales que se mueven más rápido que la burocracia que intenta perseguirlas.

Se investiga el homicidio sin conectar la renta que lo ordenó.
Se interviene el microtráfico sin seguir la estructura financiera que lo sostiene.
Se persigue la extorsión sin mapear la gobernanza criminal que la protege.
Se combate el narcotráfico sin comprender que sus rutas hoy son multimodales, híbridas y flexibles.
El crimen ya entendió algo que el Estado aún discute: la rentabilidad está en la convergencia.
Las rutas criminales ya no son lineales. Son multimodales. Un mismo corredor puede servir para mover droga, armas, oro ilegal, migrantes, divisas y mercancía de contrabando. La misma red logística cambia de producto sin cambiar de estructura. El mismo actor cambia de negocio sin cambiar de territorio. Por eso hoy resulta más preciso hablar de actores multicriminales: organizaciones polifuncionales con capacidad de mutar entre mercados ilícitos sin perder cohesión operativa.

David Kilcullen ayuda a entender esta lógica desde otra dimensión: los actores criminales contemporáneos ya no son simples delincuentes, sino estructuras híbridas que combinan funciones criminales, coercitivas, económicas y territoriales. No solo delinquen: regulan, disciplinan, financian, castigan y sustituyen funciones del Estado. Por eso su intervención no puede seguir pensándose únicamente como una reacción policial; exige una respuesta estratégica integral.

Aquí la seguridad multidimensional deja de ser un concepto doctrinal y se convierte en una necesidad operativa. Su valor no está en ampliar la lista de amenazas, sino en cambiar la lógica de intervención. La seguridad multidimensional obliga a entender que el delito no se enfrenta por segmentos, sino por sistemas; no por especialidades aisladas, sino por capacidades integradas; no por reacción, sino por articulación.

Eso exige revisar críticamente el modelo tradicional de especialización del servicio. No para eliminar capacidades técnicas, sino para superar su aislamiento funcional. La especialización sigue siendo necesaria; lo que resulta obsoleto es su fragmentación.

La pregunta ya no es si el Estado necesita unidades contra extorsión, narcotráfico, lavado o homicidio. La pregunta real es si esas capacidades seguirán operando como compartimentos cerrados o si, por fin, comenzarán a integrarse bajo una lógica de inteligencia convergente, análisis sistémico y operación coordinada.

La respuesta estratégica no pasa por crear más burocracia, sino por integrar mejor la existente. Esto supone, al menos, cinco cambios de fondo.

Primero, migrar de una lógica de delito aislado a una lógica de sistema criminal. El objeto de intervención ya no debe ser únicamente el hecho punible, sino la red que lo sostiene.

Segundo, pasar de estructuras de investigación por tipología penal a estructuras de análisis por convergencia criminal. No se trata solo de investigar qué delito ocurrió, sino qué sistema lo hizo posible.

Tercero, sustituir la fragmentación operativa por nodos de fusión interagencial, donde inteligencia, policía judicial, análisis financiero y control territorial operen sobre el mismo fenómeno.

Cuarto, reorganizar la lectura territorial del delito. El territorio no debe observarse como geografía administrativa, sino como plataforma funcional de economías criminales.

Quinto, intervenir la criminalidad con lógica de red: cortar nodos, interrumpir flujos, afectar rentas, desarticular enlaces y degradar la capacidad adaptativa del sistema criminal.

Eso implica un cambio de lenguaje, pero sobre todo un cambio de método.

Mientras el Estado siga hablando de delitos separados, seguirá llegando tarde.

Mientras siga investigando fenómenos aislados, seguirá golpeando periferias.

Mientras siga especializando sin integrar, seguirá persiguiendo fragmentos de un sistema que ya aprendió a operar como red.

La seguridad multidimensional no es una ampliación semántica de la seguridad. Es una corrección epistemológica y operativa. Obliga a entender que el crimen complejo no se combate por partes, porque no funciona por partes.

Y ese, quizás, sea el principal desafío estratégico de nuestra época: dejar de perseguir delitos y empezar, por fin, a desmantelar sistemas.

HUELLALogística

TU ALIADO ESTRATÉGICO EN SEGURIDAD DE LA INFORMACIÓN

IMPLEMENTA Y FORTALECE TU

SISTEMA DE GESTIÓN ISO 27001

PROTEGE TU INFORMACIÓN, FORTALECE TU EMPRESA

En Huella Logística te acompañamos en la implementación, mantenimiento y mejora continua de tu sistema de gestión de seguridad de la información, bajo el estándar ISO 27001.

BENEFICIOS PARA TU ORGANIZACIÓN

- PROTEGE TU INFORMACIÓN CRÍTICA
- CUMPLE CON ESTÁNDARES INTERNACIONALES
- MEJORA LA CONFIANZA Y COMPETITIVIDAD
- REDUCE RIESGOS Y PREVIENE INCIDENTES
- ACOMPAÑAMIENTO EXPERTO Y PERSONALIZADO

¡CONTÁCTANOS HOY!
Y LLEVA LA SEGURIDAD DE TU INFORMACIÓN AL SIGUIENTE NIVEL

+57 315-511-1916
servicioalcliente@huellalogistica.com
www.huellalogistica.com

COLBÙFALA
BUCARAMANGA

RESTAURANTE

EL SABOR AUTÉNTICO DEL BÚFALO

Ven y vive la experiencia
Colbúfala bga

TE ESPERAMOS

11:00AM-8:00PM

@COLBUFALABGA

CRA 30# 32-59
LA AURORA-BUCARAMANGA

EL NUEVO MAPA DEL CRIMEN:

Criminología corporativa y las amenazas invisibles del siglo XXI

Carlos Eduardo Valenzuela Oviedo
Asesor en Seguridad y Criminología Corporativa
Colombia

La corrupción no surge de repente: se construye lentamente, decisión tras decisión, racionalización tras racionalización.

Hubo un tiempo en que imaginar el crimen implicaba calles oscuras, persecuciones y delincuentes convencionales. Ese tiempo ha pasado. Hoy, las amenazas más devastadoras no provienen del exterior físico de las organizaciones, sino de sus propias entrañas: de las salas de juntas, los sistemas de información, los correos electrónicos y, en ocasiones, de los colaboradores que caminan por sus pasillos cada día.

La criminología corporativa —esa rama aplicada que analiza el comportamiento delictivo dentro del entorno empresarial— ha adquirido una urgencia sin precedentes. Las organizaciones manejan hoy más información que algunos gobiernos, operan en ecosistemas digitales altamente vulnerables y enfrentan amenazas que combinan sofisticación técnica con profunda astucia psicológica. Entender este paisaje ya no es una opción para los líderes de seguridad: **es una obligación estratégica.**

La psicología detrás del crimen corporativo

Uno de los aportes más duraderos de la criminología al mundo corporativo es el Triángulo del Fraude de Donald Cressey: tres fuerzas que, cuando convergen, transforman a un colaborador honesto en un actor de riesgo. La presión —financiera, laboral, familiar— actúa como el motor emocional. La oportunidad —controles débiles, procesos manuales, supervisión deficiente— abre la puerta. Y la racionalización —esa narrativa interna que el sujeto construye para justificar lo injustificable— le otorga el permiso moral para cruzar la línea.

Lo que hace particularmente complejo este fenómeno es que la gran mayoría de los actores no se perciben a sí mismos como delincuentes. Se convencen de que 'la empresa les debe', de que 'todos lo hacen', de que 'solo será esta vez'. Esta disonancia cognitiva no es una excusa: es una señal que las organizaciones deben aprender a leer antes de que el daño sea irreversible.

- La presión es el motor emocional del fraude: deudas, amenaza de despido, problemas familiares.
- La oportunidad es la puerta abierta: accesos mal gestionados, conciliaciones que nadie revisa.
- La racionalización es el permiso moral: 'No le hago daño a nadie', 'Solo por esta vez'.

El crimen que no se ve: corrupción y poder corpoartivo

La corrupción corporativa rara vez se presenta de forma evidente. Suele manifestarse en firmas aparentemente rutinarias, permisos que avanzan con inusual rapidez, contratos direccionados o procesos en los que siempre resultan favorecidos los mismos actores. Desde la perspectiva de la criminología corporativa, no debe entenderse como un hecho aislado, sino como un fenómeno sistémico: el resultado de culturas organizacionales que normalizan tolera o incluso incentivan prácticas ilícitas.

El perfil del corruptor corporativo resulta especialmente complejo. Con frecuencia se trata de personas con alto nivel educativo, posiciones de poder, conocimiento técnico y acceso a asesoría legal especializada. Sus conductas se sostienen mediante mecanismos psicológicos como la racionalización, el desplazamiento de la culpa, la deshumanización de la víctima y la sensación de impunidad.

Esta distancia entre la criminalidad corporativa y la delincuencia convencional hace que la corrupción empresarial sea, al mismo tiempo, una de las formas más dañinas y difíciles de detectar dentro de las organizaciones.

El ciber delito: cuando la pantalla se convierte en arma

El crimen digital ha reconfigurado el mapa de riesgos corporativos de manera irreversible. Hoy, un atacante no necesita presencia física para acceder a los activos más valiosos de una organización: bases de datos, estrategias comerciales, credenciales de acceso, información financiera. La anatomía de un ataque moderno sigue un patrón metódico: observación, infiltración gradual, movimiento lateral silencioso y, finalmente, ejecución cuando las defensas ya han sido mapeadas.

Pero la tecnología es solo la superficie. El verdadero campo de batalla es el factor humano, la ingeniería social —que explota confianza, autoridad y urgencia— convierte a colaboradores bien intencionados en vectores involuntarios del ataque, un correo que aparenta venir de un superior jerárquico, una solicitud urgente de transferencia, un enlace en un mensaje aparentemente legítimo: bastante para comprometer años de construcción institucional.

Tres estrategias definen al ciberdelincuente corporativo contemporáneo: la escalada gradual —que prueba límites silenciosamente antes del ataque principal—; la normalización del desvío —que convierte pequeñas infracciones toleradas en brechas estructurales—; y los ataques silenciosos —que operan dentro de los umbrales considerados 'normales' durante semanas o meses antes de revelarse.

RINO ESX

Producto 100% natural a base de chontaduro y borojó. NO tiene contraindicaciones ni efectos adversos.

Nos ayuda para el cansancio, nos aporta vitalidad y energía

PRINCIPIOS ACTIVOS:

- **CHONTADURO**
- **BOROJÓ**
- **VITAMINAS B1 B2 B3 B6 B12**

1 SOBRE
2
PASTILLAS

100% NATURAL

3219345161

@rinoesx

Una empresa madura no es la que evita todos los ataques, sino la que responde con rapidez, control y visión estratégica.

El insider threat: el enemigo en casa

De todas las amenazas que puede enfrentar una organización, pocas resultan tan complejas de gestionar como aquellas que se originan en su interior. El insider threat —riesgo generado por personas con acceso legítimo que actúan en contra de los intereses corporativos— combina el conocimiento profundo de los procesos, sistemas y vulnerabilidades internas con la capacidad de operar sin despertar sospechas inmediatas que puede tratarse de un empleado inconforme, un contratista con permisos excesivos o un colaborador manipulado por actores externos mediante técnicas de ingeniería social.

Lo que diferencia al insider threat de otras formas de criminalidad corporativa es su invisibilidad operativa, a diferencia del atacante externo, el actor interno ya ha superado las barreras de acceso y se mueve dentro de espacios, sistemas y rutinas previamente autorizadas. Sus conductas anómalas pueden confundirse con actividades laborales habituales, lo que dificulta su detección temprana.

Por esta razón, la respuesta organizacional no puede limitarse únicamente a controles tecnológicos, requiere un enfoque integral que combine analítica de comportamiento, segregación y rotación de funciones críticas, aplicación estricta del principio de mínimo privilegio, monitoreo proporcional de accesos sensibles y una cultura ética que promueva la denuncia responsable sin temor a represalias.

Matriz de amenazas corporativas y respuesta estratégica

Vector de riesgo	Mecanismo	Respuesta estratégica
Fraude interno	Presión + oportunidad + racionalización (Triada de Cressey)	Controles de acceso, segregación de funciones, línea ética
Corrupción corporativa	Normalización del abuso, impunidad percibida, cultura del resultado	Compliance real, debida diligencia a terceros, auditorías independientes
Ciberdelito	Ingeniería social, escalada gradual, ataques silenciosos	Cultura de seguridad, mínimo privilegio, gestión de incidentes
Insider threat	Acceso legítimo mal gestionado, colusión, exfiltración	Geofencing, rotación de roles, analítica de comportamiento

ZONALOGISTIK
LOGÍSTICA INDUSTRIAL A SU MEDIDA
Soluciones logísticas industriales
a la medida que operan 365 días
del año 24 horas del día.
Contáctanos: 321 427 2002

La prevención como ventaja competitiva

Durante décadas, la seguridad corporativa fue vista como un costo inevitable: una carga presupuestal que se justificaba en función de incidentes pasados. Ese paradigma ha caducado. Las organizaciones que han comprendido la criminología corporativa como disciplina estratégica entienden que la prevención es, en realidad, una ventaja competitiva.

Prevenir el crimen corporativo no se logra con cámaras, guardias o firewalls en solitario. Requiere la convergencia de tres pilares fundamentales. El primero es la educación y la conciencia: entrenar a empleados y directivos para identificar comportamientos de riesgo, reconocer señales de ingeniería social y denunciar sin temor a represalias. El segundo es la existencia de sistemas de control transparentes: auditorías éticas, evaluaciones de riesgo continuas, líneas de denuncia que funcionen de verdad. El tercero, y quizás el más poderoso, es el liderazgo ejemplar: cuando la alta dirección predica con el ejemplo, el mensaje se replica hacia todos los niveles de la organización.

La criminología corporativa también revela algo que la gestión de riesgos tradicional suele ignorar: los delitos no ocurren de manera espontánea. Se construyen lentamente, en la intersección entre presiones no atendidas, oportunidades no cerradas y culturas que toleran la ambigüedad ética. Una organización que entiende esto actúa preventivamente sobre esas tres variables antes de que el crimen tenga lugar.

Conclusión: seguridad como inteligencia organizacional

El siglo XXI ha convertido a las empresas en el nuevo laboratorio del crimen. Las amenazas son más sofisticadas, más silenciosas y devastadoras que nunca. Pero también hay más conocimiento disponible para enfrentarlas: la criminología corporativa, la analítica de comportamiento, la inteligencia de amenazas y los modelos de seguridad por capas ofrecen hoy herramientas sin precedentes para quien esté dispuesto a adoptarlas.

La clave está en dejar de entender el crimen corporativo como un riesgo financiero y comenzar a verlo como lo que realmente es: un riesgo humano. Los delitos no los cometen los sistemas; los cometen las personas, bajo determinadas condiciones, con determinadas motivaciones y en ausencia de guardianes efectivos.

Esa comprensión —profunda, interdisciplinaria, estratégica— es el verdadero punto de partida para construir organizaciones más seguras, más éticas y resilientes. En el nuevo mapa del crimen, la seguridad corporativa no es un departamento: es una mentalidad.

ESS+®
FERIA INTERNACIONAL DE SEGURIDAD

26 AL 28 AGOSTO 2026
›CORFERIAS‹

INTEGRACIÓN DE TECNOLOGÍAS GLOBALES

UN SOLO LUGAR PARA DECISIONES ESTRATÉGICAS EN SEGURIDAD

- Conocimiento experto
- Tecnología integrada
- Networking especializado

REGÍSTRESE AQUÍ

MÁS INFORMACIÓN EN SECURITYFAIRCOLOMBIA.COM

*Consulte T&C en securityfaircolombia.com

¿CORTINA DE HUMO?

General. (R) Juan Carlos Buitrago Arias

El comercio ilícito de tabaco no es una cortina de humo, es una peligrosa cadena criminal, sin fronteras ni barreras, con enorme poder resiliente y corruptor. Así se desprende del más reciente informe de KPMG, el cual indica que uno de cada tres cigarrillos consumidos en 11 países de América Latina y Canadá tienen origen ilegal, es decir 77.000 millones de unidades, equivalente al 31,9% del consumo total, representando además, 8.500 millones de dólares que se dejaron de recaudar en impuestos para alimentar a las estructuras criminales.

El reporte de KPMG (2026) es contundente: "el consumo ilegal de cigarrillos refleja estructuras regionales de abastecimiento, más que factores propios de cada país". Paraguay fue la principal fuente de cigarrillos ilegales en la región, responsable del 44% de todo el contrabando identificado en los once mercados estudiados. Aunque esa participación bajó frente al 57% registrado en 2024, el descenso no es una victoria, muestra que las redes se adaptan y diversifican constantemente.

Esta realidad se planteó también, la semana pasada, en Río de Janeiro, durante la III reunión sobre la Lucha contra el Comercio Ilegal de Directores de Aduanas de las Américas, convocada por la Alianza Transnacional para Combatir el Comercio Ilícito (TRACIT) y la Receita Federal de Brasil, que contó con delegados de 25 países y el sector privado. En este espacio, se presentó el documental “HUMO: el delito invisible", producido por la reconocida periodista argentina Lucía Salinas, el cual tuvo nuestra contribución, ayudando a develar el alcance de las mafias de cigarrillos en Sudamérica. Lamentablemente se ha vuelto usual, la recurrente ausencia de Colombia y México, en este y otros escenarios de discusión sobre las economías criminales.

Las autoridades realizan múltiples esfuerzos, pero la ilegalidad aumenta. El reporte de KPMG documenta algo revelador. Al tiempo que los flujos provenientes de Paraguay disminuyeron en 10.600 millones de cigarrillos en 2025, hubo un aumento de 5.800 millones de unidades de marcas sin etiquetado nacional identificable, es decir, cigarrillos producidos legalmente pero destinados desde el inicio al contrabando. La red no se desmanteló, mutó y sigue bajo el monopolio de la mafia de cigarrillos de ese país que tiene inundado a Latinoamérica.

Estas redes criminales tienen una enorme facilidad de adaptación frente a la presión, y la solución no está en más decomisos, se requiere anticipación a sus movimientos, mayores alertas efectivas y una adecuada inteligencia, análisis de datos, trazabilidad y oportuna cooperación para desarticularlas de raíz. También mayor conciencia del consumidor. La agenda de Río abordó precisamente esta brecha, "De los datos a las incautaciones: gestión de riesgos e inteligencia artificial" partiendo de una premisa clara, la gestión de riesgos es una herramienta clave para identificar envíos de alto riesgo y optimizar la asignación de recursos, incluyendo el uso de inteligencia artificial y analítica avanzada.

Y en esta tarea, la información del sector privado es crucial. Por ejemplo, los reportes sospechosos de transacciones financieras ayudan a identificar el flujo de dineros ilícitos. Así lo expuse la semana anterior en la Cumbre Antilavado - The Assembly by ACAMS (Association of Certified Anti-Money Laundering Specialists) celebrada en Hollywood, Florida, ante más de 1.500 asistentes. El mensaje fue directo, el comercio ilegal y el lavado de activos no son fenómenos separados. Estamos conviviendo con un serio problema, el tráfico de cigarrillos ilícitos como la moneda de cambio, para legalizar las utilidades del narcotráfico.

Otro frente donde el rezago institucional es más relevante, es el comercio digital, ante la proliferación inusitada de plataformas electrónicas destinadas al comercio ilegal. En TRACIT se analizaron los efectos no intencionados de estos regímenes, la subvaluación de mercancías y los desafíos de controlar flujos de mensajería de alto volumen sin bloquear el comercio legítimo. Las reglas fueron diseñadas para un mundo donde el comercio electrónico transfronterizo era marginal. Hoy es dominante, y sin trazabilidad los controles en frontera son insuficientes.

Los datos revelan geografías del fracaso que merecen atención política explícita. En 2025, Panamá que se destaca por sus resultados, registró una tasa de consumo ilegal de cigarrillos del 89% —casi nueve de cada diez eran ilegales—, seguida de Ecuador con 84% y Chile con 58% (KPMG). En Colombia casi 4 de cada 10 cigarrillos que se consumen son ilícitos. Y no obstante, los significativos avances de la Policía Fiscal y Aduanera, las cifras reflejan que estructuras poderosas del contrabando como la de Papá Pitufo, siguen operando con relativa facilidad.

El próximo mes en México, con el liderazgo de la ANDI, se llevará a cabo la XI reunión de la Alianza Latinoamericana contra el Contrabando ALAC que convoca múltiples autoridades y representantes de organizaciones multilaterales y del sector privado. De otro lado, en este mismo país, se activará en el segundo semestre del año, el capítulo norte de la Estrategia Triángulos coordinada por StrategosBIP, orientada a integrar esfuerzos accionables de actores públicos y privados para prevenir y combatir el comercio ilegal y el crimen organizado. Estos dos mecanismos, únicos en LATAM & Caribe, prometen dar pasos importantes, para afianzar la cooperación regional con enfoque práctico y acción efectiva contra estos fenómenos criminales.

@libroteoriaestado

YA DISPONIBLE

PROHIBIDO ELIMINAR FÍSICAMENTE AL OPONENTE

amazon kindle

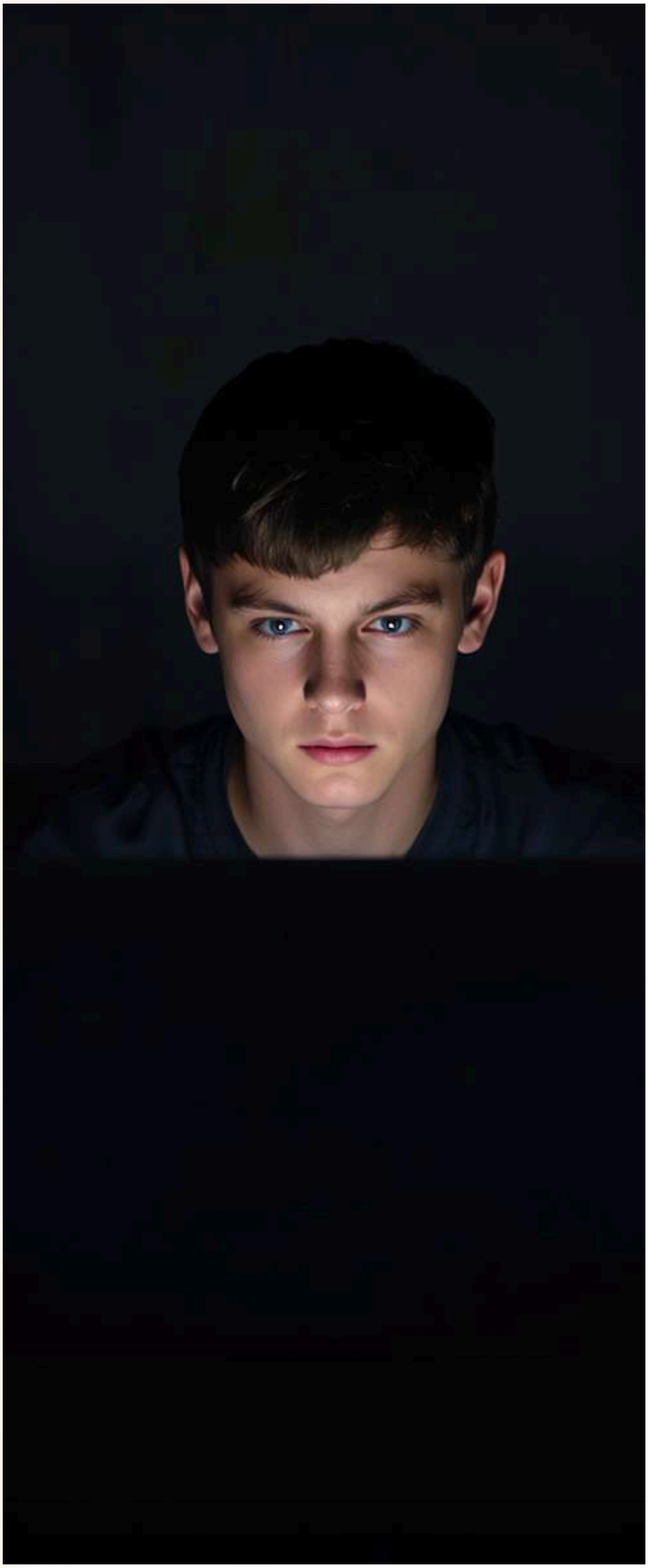
hotmart

Para más información
+57 300 7317523

Generación asistida:

El precio invisible de pensar menos en la era de más información

Mariana Tovar Mora



En un mundo interconectado, donde cada vez encontramos más información a disposición de nosotros por diferentes herramientas, es indispensable sentarse un momento, hacer una pausa y reflexionar sobre la información que estamos leyendo y encontrando en la web. Lo que antes tomaba horas de entendimiento o esfuerzo, ahora toma unos breves segundos y la pegunta clave no se centra en cuánto estamos avanzando, porque sin duda el mundo cambia en cada segundo, sino que estamos dejando de desarrollar en el camino.

Hoy hablaremos sobre la Inteligencia artificial y su rol en la educación. Sin duda la Inteligencia Artificial ha desarrollado un aspecto clave que es el aprendizaje personalizado, un estudiante ya no tiene que adaptarse al aprendizaje colectivo que se genera en un aula de clases, quedarse con dudas que van surgiendo en el transcurso del discurso del docente o ajustarse a los tiempos establecidos por las directivas, ahora puede aprender a su propio tiempo, desarrollando sus fortalezas y democratizando la educación. No obstante, este progreso trae consigo un riesgo silencioso: **la dependencia.**

Según el estudio “La inteligencia artificial en las tareas académicas: ¿Apoyo para el aprendizaje o dependencia tecnológica?” (2025), aproximadamente el **78% de los estudiantes utiliza la IA para estructurar sus respuestas y el 45% lo hace sin revisar críticamente el contenido**, lo que evidencia una tendencia hacia el uso pasivo de estas herramientas. Asimismo, investigaciones como “Consecuencias de la dependencia de la inteligencia artificial en habilidades críticas y aprendizaje autónomo” evidencian que existe una **relación significativa entre el uso excesivo de IA y la disminución de habilidades críticas, autonomía y capacidad de resolución de problemas**, afectando directamente el desarrollo cognitivo del estudiante.

Esto plantea una preocupación real, ya que cuando una herramienta responde por ti, piensa por ti y organiza por ti, surge una pregunta inevitable: ¿dónde queda el esfuerzo mental? ¿Dónde se fortalecen habilidades fundamentales como la memoria, la organización y la creatividad? En la práctica, este fenómeno ya se está evidenciando en contextos reales: docentes reportan que muchos estudiantes entregan trabajos correctos en forma, pero son incapaces de explicar su contenido, lo que refleja un aprendizaje superficial basado en resultados y no en procesos. Incluso estudios como el desarrollado por la Universidad del Rosario sobre el uso de inteligencia artificial generativa en jóvenes en Bogotá, muestran que estas herramientas pueden generar niveles de uso y atracción comparables a sistemas de recompensa, evidenciando un potencial de dependencia creciente en contextos educativos.

Este panorama no solo impacta la educación, sino también el futuro laboral, ya que las empresas buscan cada vez más habilidades como el pensamiento crítico, la creatividad y la capacidad de resolver problemas de manera autónoma; sin embargo, el uso excesivo de IA podría derivar en profesionales con menor tolerancia al error y mayor dependencia tecnológica para tareas básicas. Se configura así una paradoja: **la generación con mayor acceso a la información podría convertirse en una de las menos autónomas intelectualmente.**

A pesar de esto, la inteligencia artificial no debe entenderse como una amenaza, sino como una herramienta cuyo impacto depende del uso que se le dé, pudiendo ser un aliado para potenciar el aprendizaje o una “muleta cognitiva” que limite el pensamiento. En una era donde el conocimiento está al alcance de un clic, el verdadero desafío no es obtener respuestas, sino aprender a cuestionarlas, analizarlas y construir pensamiento propio. Frente a esto, surgen preguntas inevitables: ¿estamos aprendiendo realmente o solo obteniendo respuestas rápidas?, ¿qué pasaría si dejáramos de usar estas herramientas?, ¿podríamos sostener nuestro conocimiento sin apoyo tecnológico?, ¿estamos formando mentes críticas o simplemente usuarios eficientes?, y finalmente, ¿la inteligencia artificial está ampliando nuestras capacidades o comenzando a reemplazarlas?

Como estudiante, no se trata de rechazar la inteligencia artificial, sino de aprender a convivir con ella de forma consciente y estratégica. Por eso, es importante dejar algunas claves para su uso responsable: utilizarla como una guía y no como un sustituto del pensamiento propio, se puede buscar información, utilizarla como método de aprendizaje pero siempre es importante profundizar en las fuentes y contrastar con conocimientos previos al tema de estudio; cuestionar siempre las respuestas que ofrece en lugar de aceptarlas automáticamente, poner en paralelo las situaciones de la cotidianidad y encontrar el sentido de la información que se proporciona, buscar estudios relacionados a los temas y complementar la información con otras fuentes para evitar sesgos; intentar resolver primero los problemas por cuenta propia antes de acudir a la herramienta, y usarla como apoyo para profundizar el aprendizaje y no solo para cumplir tareas. La inteligencia artificial puede ser una aliada poderosa, pero el verdadero valor seguirá estando en la capacidad humana de pensar, analizar y crear, no hay nada más poderoso que la mente humana y su capacidad para generar conexiones y aprendizajes profundos, no podemos dejar perder esta capacidad que nos distingue de otras especies, debemos empezar a reflexionar y tomar acción en el desarrollo de ciertas habilidades nuevas en el aprendizaje que nos permitan usar la inteligencia artificial a nuestro favor para crecer más y no esperar a que nos reemplacen por la tecnología.

JEW

JEIDEN

ENGINEERS WEB

PROFESIONALES

WEB DEVELOPMENT

Diseñamos tu pagina Web

Web Design

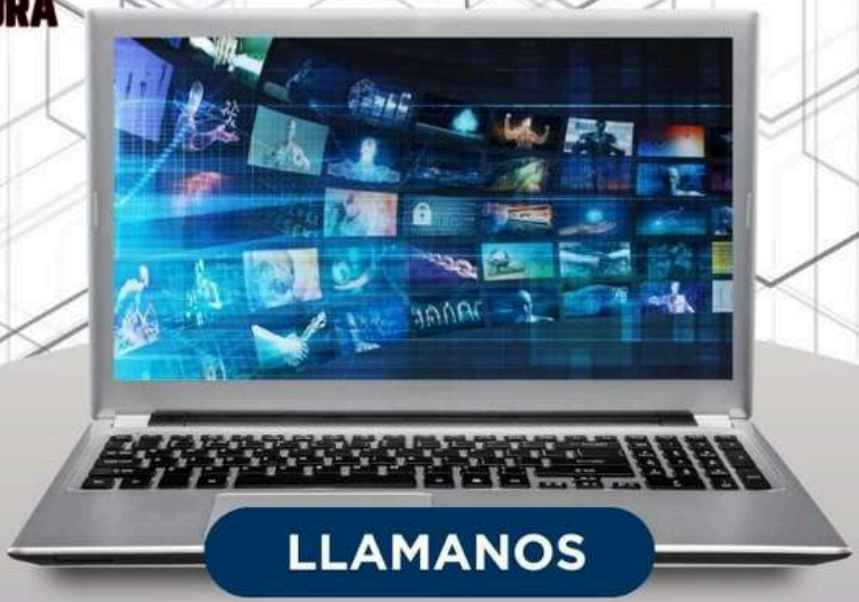
Front-end Development

Web Maintenance

"TRANSFORMA TU PRESENCIA DIGITAL CON EXPERTOS EN DESARROLLO WEB Y APLICACIONES MOVILES."

LICENCIAMIENTO
CORREO CORPORATIVO
DESARROLLO WEB A LA MEDIDA
ANTIVIRUS Y SEGURIDAD
INFRAESTRUCTURA

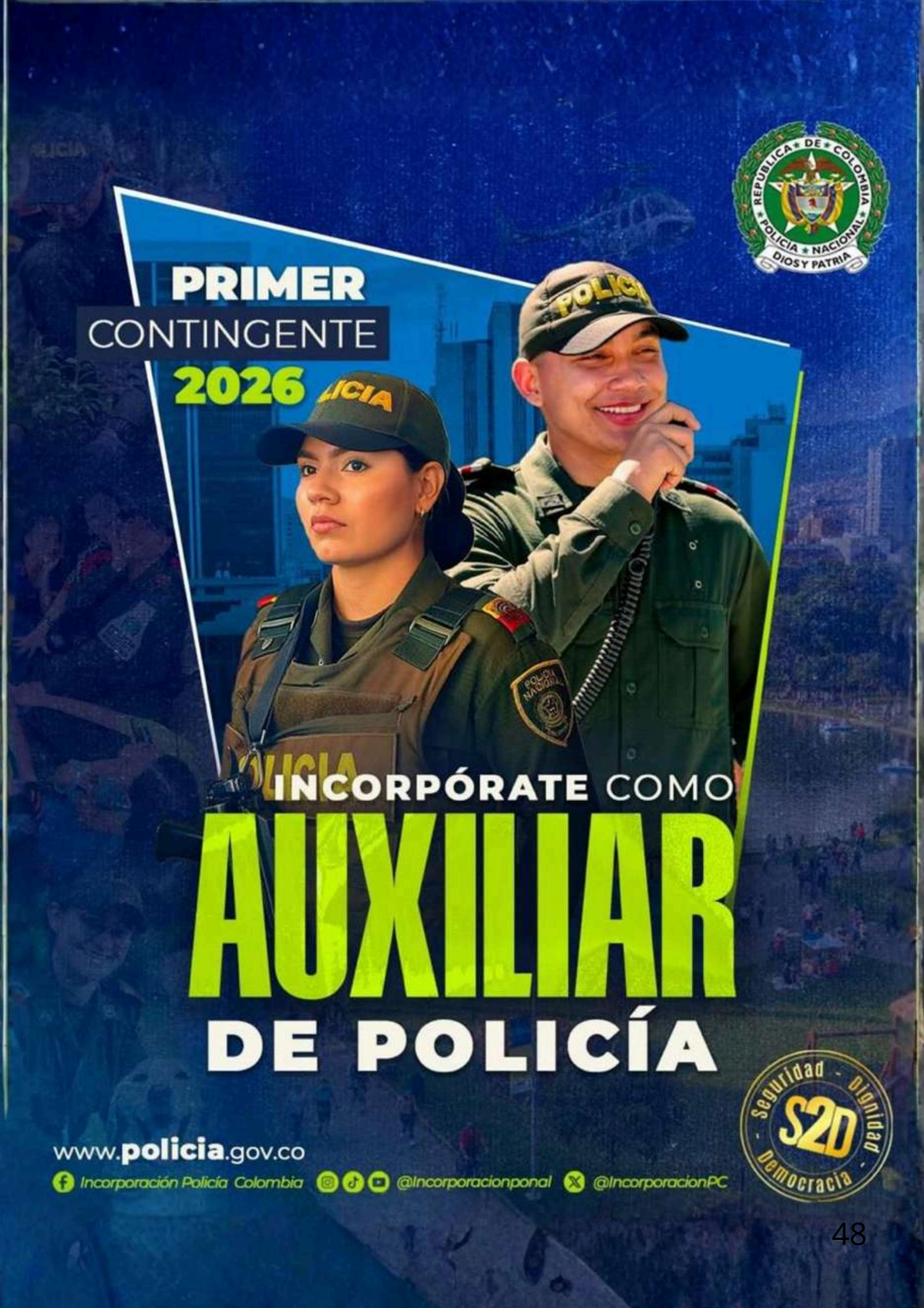
MANTENIMIENTO Y VENTA DE EQUIPOS
MARKETIN DIGITAL Y REDES SOCIALES
CREACION DE MARCA Y POSICIONAMIENTO



LLAMANOS

Mas Información
www.jeidenengineersweb.com

Contáctenos
+57 320 206 35 49


REPUBLICA DE COLOMBIA
POLICIA NACIONAL
DIOS Y PATRIA
PRIMER
CONTINGENTE
2026
INCORPÓRATE COMO
AUXILIAR
DE POLICÍA
Seguridad
Dignidad
S2D
Democracia
www.policia.gov.co
Incorporación Policía Colombia
@Incorporacionponal
@IncorporacionPC