

EDICIÓN 39
2026

Revista **EL MUNDO CAMBIÓ**

SEGURIDAD PRIVADA EN COLOMBIA: EL OCASO DEL MODELO BASADO SOLO EN EL VIGILANTE

Por: Ingeniero, Carlos Rojas



Por: Ingeniero, Carlos



26 de septiembre de 2026



1. SEGURIDAD PRIVADA EN COLOMBIA: EL OCASO DEL MODELO BASADO SOLO EN EL VIGILANTE

Autor: Ingeniero, Carlos Rojas.



11

2. LA PROTECCIÓN INTEGRAL DE NIÑOS, NIÑAS Y ADOLESCENTES FRENTE A TODA FORMA DE VIOLENCIA

Autora: Dra. Paula Fabiana Romano.



16

3. SEGURIDAD EMPRESARIAL: DE CENTRO DE COSTO A HABILITADOR ESTRATÉGICO

Autor: Oscar Mauricio Barreto Rodríguez.



19

4. LA PROFESIONALIZACIÓN POLICIAL: PUNTO ESTRATÉGICO EN LA GESTIÓN HUMANA Y LA CALIDAD DEL SERVICIO POLICIAL

Autor: Coronel Oleskyenio Flórez Rincón, PhD.



22

5. BIOMETRÍA Y PROTECCIÓN DE DATOS: UNA CONEXIÓN IMPRESCINDIBLE

Autor: Enrique Alonso Braña.



26

6. DE BISMARCK A LA INTELIGENCIA ARTIFICIAL: EVOLUCIÓN DE LA MEDICINA DEL TRABAJO EN ALEMANIA

Autor: Álvaro Castillo Strampfer.



31

7. GESTIÓN DE CRISIS Y REPUTACIÓN: CÓMO SOBREVIVE UNA EMPRESA AL ESCÁNDALO

Autor: Carlos Eduardo Valenzuela Oviedo – CPP.



34

8. TOXICOLOGÍA INDUSTRIAL Y GESTIÓN DEL RIESGO QUÍMICO: UN ENFOQUE INTEGRAL DESDE LA SEGURIDAD Y SALUD EN EL TRABAJO

Autor: Diego Alejandro Henao Ossa.



39

NUESTRO EQUIPO



administracion@revistaelmundocambio.com



+57 300 6412376



BSERVATORIO 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:



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.



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

Sumamos capacidades,
compartimos visión,
**construimos un país
más seguro y resiliente.**

ANUNCIAMOS **NUESTRA ALIANZA**



REVISTA ESPECIALIZADA EN
SEGURIDAD Y GESTIÓN DE RIESGOS



UNIVERSIDAD MILITAR
NUEVA GRANADA



Una alianza estratégica que nace del propósito común de promover la seguridad, el conocimiento y el desarrollo sostenible en las organizaciones.

TRABAJAREMOS JUNTOS EN:



Mesa Técnica de Seguridad

Espacio de análisis, diálogo y construcción de soluciones para los desafíos actuales en seguridad.



Eventos Académicos y de Seguridad Empresarial

Escenarios de formación, actualización y networking para profesionales y organizaciones comprometidas con la excelencia.



Unimos experiencia, conocimiento y redes para **generar impacto**.



Aportamos valor a la comunidad empresarial y académica.



Construimos juntos un entorno más seguro, competitivo y resiliente.

**JUNTOS, GENERAMOS CONFIANZA, COMPARTIMOS CONOCIMIENTO
Y CONSTRUIMOS FUTURO.**

Revista

EL MUNDO CAMBIÓ

Editorial:



Vivimos un momento en el que hablar de seguridad implica comprender que los riesgos están cambiando y que también deben transformarse las formas de prevenir, proteger y responder. La seguridad ya no depende únicamente de la presencia física o de la reacción frente al incidente. Hoy convergen tecnología, información, formación, gestión empresarial, protección de las personas y capacidad de anticipación. Esta edición propone precisamente esa mirada amplia: entender la seguridad como un sistema en el que diferentes capacidades deben conectarse para responder a los desafíos actuales.

Abrimos esta edición con “Seguridad privada en Colombia: el ocaso del modelo basado solo en el vigilante”, del **Ingeniero Carlos Rojas**. El autor analiza cómo los costos laborales, las exigencias regulatorias y el avance de la inteligencia artificial, la analítica de video, los sensores y los centros de monitoreo están transformando el sector. No se trata de la desaparición del vigilante, sino de su integración dentro de una arquitectura más amplia de protección, donde también importan la información, la tecnología y los resultados.

La protección de las personas ocupa un lugar fundamental en “La protección integral de niños, niñas y adolescentes frente a toda forma de violencia”, de la **Dra. Paula Fabiana Romano**. Desde una perspectiva de derechos humanos, la autora aborda las obligaciones de la familia, la sociedad y el Estado frente a la violencia contra la infancia. Su reflexión destaca la necesidad de fortalecer la protección sin desconocer la autonomía, dignidad y derecho a ser escuchados de niños, niñas y adolescentes.

La seguridad también adquiere un papel estratégico dentro de las organizaciones. En “Seguridad empresarial: de centro de costo a habilitador estratégico”, **Oscar Mauricio Barreto Rodríguez** plantea la necesidad de transformar la manera en que las empresas comprenden esta función. Los riesgos actuales pueden afectar simultáneamente a las personas, la operación, la reputación y los resultados financieros, por lo que resulta necesario integrar seguridad física, ciberseguridad, continuidad del negocio, inteligencia y gestión de crisis.

La profesionalización de quienes ejercen funciones de seguridad constituye otro desafío central. En “La profesionalización policial: punto estratégico en la gestión humana y la calidad del servicio policial”, el **coronel Oleskyenio Flórez Rincón, PhD**, plantea que la función policial requiere mucho más que entrenamiento operativo. El policía contemporáneo necesita conocimientos, ética, liderazgo, capacidad de discernimiento y aprendizaje permanente. Profesionalizar significa integrar entrenamiento, capacitación, educación y formación integral para fortalecer la calidad del servicio.

La tecnología también trae nuevos desafíos relacionados con la información personal. En “Biometría y protección de datos: una conexión imprescindible”, **Enrique Alonso Braña** analiza el uso de características físicas y conductuales para identificar y autenticar personas. Huellas, rostros y otros datos biométricos ofrecen posibilidades importantes para la seguridad, pero requieren un tratamiento responsable y acorde con las normas de protección de datos. La innovación debe avanzar acompañada de criterios de proporcionalidad, seguridad y privacidad.

La evolución de la protección laboral tiene raíces profundas. En “De Bismarck a la inteligencia artificial: evolución de la Medicina del Trabajo en Alemania”, **Álvaro Castillo Strampfer** recorre la transformación de la salud laboral desde las reformas impulsadas en la época de Bismarck hasta la consolidación de la colaboración entre médicos del trabajo e ingenieros de seguridad. El artículo permite comprender cómo la prevención ha evolucionado junto con los cambios sociales, industriales y tecnológicos, y plantea nuevos retos frente a la inteligencia artificial y las transformaciones del trabajo.

Pero la seguridad también se pone a prueba cuando una organización enfrenta una crisis. En “Gestión de Crisis y Reputación: cómo sobrevive una empresa al escándalo”, **Carlos Eduardo Valenzuela Oviedo – CPP** analiza cómo un incidente puede convertirse rápidamente en una amenaza para la confianza. El autor destaca la importancia de preparar protocolos, proteger a las personas, preservar evidencias, comunicar hechos confirmados y corregir aquello que permitió que la situación ocurriera. La reputación se reconstruye mediante decisiones y acciones coherentes.

Finalmente, “Toxicología Industrial y Gestión del Riesgo Químico: Un Enfoque Integral desde la Seguridad y Salud en el Trabajo”, de **Diego Alejandro Henao Ossa**, aborda uno de los campos más técnicos de la prevención. El autor analiza el peligro y el riesgo químico, los mecanismos de exposición y los efectos que determinadas sustancias pueden generar en el organismo. También destaca la importancia de identificar los peligros, comunicar adecuadamente la información y establecer barreras de control que permitan proteger la vida y la salud de los trabajadores.

Los ocho artículos de esta edición coinciden en una idea fundamental: la seguridad está dejando de ser una respuesta aislada para convertirse en una capacidad integral de anticipación, protección y transformación. Tecnología, formación, prevención, gestión empresarial, protección de derechos, salud laboral e inteligencia hacen parte de una misma conversación. Comprender estas conexiones permite acercarnos a una seguridad más profesional, integrada y preparada para una realidad en permanente cambio.

SAMSUNG

Galaxy S26 Series



Entrego
y estreno

Trade in, entrega tu celular
como parte de pago



Disfruta 0% de interés con
Davivienda y Bancolombia

Addi

Llévalo a
cuotas

**Llévate tu celular a
24 cuotas por un valor de \$211.662**

BARRANQUILLA

CC Buenavista 1
Piso 2 Local 219
CC Villa Country
Piso 111a zona Común
Pasillo Central
CC Portal del Prado
Isla Área común 16
Viva Centro Comercial
Isla 202
CC Parque Alegre
Piso 111a 1-18A
SOLEDAD
CC Plaza del Sol
Local 267 - 268

BOGOTÁ

CC Plaza de las Américas
Local 176
CC Gran Estación
Isla 1 - 123
CC Gran Estación
Isla diagonal a101

CALI

CC Llanogrande
Palmira, Valle
Burbuja 702 frente a
Rancho Viejo de Caldas
CC Unico 1
Burbuja 833

CARTAGENA

CC Mall Plaza el Castillo
Local 110 - 111 piso 1
CC Mall Plaza el Castillo
Isla
CC Plaza Bocagrande
Piso 111a 1-32
TURBACO
CC Plaza 90
Isla 10

SANTA MARTA

CC Ocean Mall
2º piso local E1 y E2
CC Buena Vista
Isla 137

VALLEDUPAR

CC Mayales Plaza
Local 256 e Isla #3
CC Guatapuri
1º piso al lado de la
plazuela de Juan Valdez

VISA

MasterCard

Redeal
Diners Club

Diners Club

Davivienda

PSD

AVAL

Colombia

Bancolombia

Banco de Bogotá

PROFESIONAL DE LA SEMANA

Fabio Leal
del Río



Fabio Leal del Río es un ingeniero con más de 20 años de trayectoria dedicada al fortalecimiento de procesos educativos dirigidos a población joven y adulta en Colombia. Actualmente se desempeña como director administrativo del Instituto Bolivariano en Soacha, del Centro de Estudios e Investigación Vida (CEVIDA) en Cali y del Colegio para Adultos San Nicolás en Facatativá. Además, es cofundador del Grupo Educativo Leal del Río, desde donde ha desarrollado iniciativas orientadas a ampliar las oportunidades de formación.

Su experiencia se ha enfocado especialmente en la atención de población vulnerable, liderando procesos educativos que actualmente benefician a más de 2.600 jóvenes y sus familias por semestre. A lo largo de su trayectoria, ha trabajado de manera articulada con la Policía Nacional, fortaleciendo proyectos educativos destinados a aportar a la construcción de proyectos de vida y a generar herramientas que permitan a los jóvenes afrontar de mejor manera los riesgos presentes en sus entornos.

El impacto de su labor se refleja en más de 30.000 jóvenes que han tenido acceso a procesos y herramientas educativas orientadas a fortalecer sus oportunidades y proyectar un futuro con mayores posibilidades de desarrollo. Su trayectoria se caracteriza por la articulación entre educación, prevención y trabajo social, con una apuesta permanente por contribuir a la transformación de contextos vulnerables a través de la formación.



La mayoría de las malas decisiones **se toman igual.**

No porque falte experiencia.

No porque falte inteligencia.

Sino porque se tomaron con **información incompleta.**

P&P
CONSULTING

**Es la solución a tus
problemas en la
toma de decisiones**



**Consulta de
talante judicial**



**Visitas
domiciliarias**



**Referenciaciones
académica y laboral**



**Investigaciones
administrativas**



Apoyo Judicial





Relaciones Internacionales,
Estrategia y Seguridad
Sede Bogotá

DIPLOMADO

Gerencia de la Seguridad

Inscripción: 01 al 21 de
agosto de 2026

Costo
inscripción: \$81.000

Matrícula: 22 al 28 de
agosto de 2026

Costo
diplomado: \$2.479.000

Intensidad
Académica: 120 horas

Modalidad: Remota
(mediada por tecnología)

Inicio probable de clases: 21 de septiembre de 2026

Se abre con un mínimo de 13 personas.

Horario: lunes a viernes de 6:00 a 10:00 p. m.

Contacto:

extensión.faries@unimilitar.edu.co – ruth.quitian@unimilitar.edu.co

WhatsApp: 3133775189

PBX: 650 00 00 ext. 1339

SEGURIDAD PRIVADA EN COLOMBIA:

EL OCASO DEL MODELO BASADO SOLO EN EL VIGILANTE

Costos, inteligencia artificial, tecnología y una nueva relación entre proveedores y consumidores

Por: Ingeniero, Carlos Rojas

Durante décadas, buena parte del mercado colombiano de seguridad privada se construyó alrededor de una ecuación sencilla: más puestos, más horas y más hombres equivalían a más protección. Esa fórmula todavía tiene sentido en determinados escenarios, pero está dejando de ser suficiente. La combinación de costos laborales, presión sobre las tarifas, nuevas exigencias regulatorias y el avance de la inteligencia artificial (IA), la analítica de video, los sensores y los centros de monitoreo está cambiando la naturaleza del servicio.

Hablar de “ocaso de la seguridad física” no significa anunciar la desaparición del vigilante. La evidencia disponible apunta a otra transformación: el ocaso del modelo que vende presencia humana como producto final y no como parte de una arquitectura integral de protección. La pregunta empresarial ya no debería ser cuántos hombres hay en un puesto, sino qué riesgo se cubre, con qué tecnología, con qué información, con qué capacidad de respuesta y con qué resultado medible.

El problema económico: cuando proteger cuesta cada vez más

La seguridad privada colombiana, tiene una particularidad: una parte importante de su estructura de costos está ligada al trabajo humano y a las obligaciones laborales. La Superintendencia de Vigilancia y Seguridad Privada explica que las tarifas mínimas deben permitir cubrir, entre otros componentes, salario, horas extras, recargos, prestaciones y costos operativos. Además, la regulación laboral ha reducido gradualmente la jornada máxima semanal de 48 a 42 horas, proceso que culminó el 15 de julio de 2026. Esto presiona la planeación de turnos y la necesidad de personal para mantener coberturas continuas.

El propio Gobierno reconoció en junio de 2026 la tensión entre costo y acceso: la Supervigilancia informó que estaba impulsando nuevas tarifas mínimas diferenciales para hogares, microempresas, establecimientos educativos y determinadas entidades públicas, señalando que el sector reúne aproximadamente 360.000 trabajadores. Es una cifra que muestra la dimensión económica y social de la industria, pero también la magnitud del desafío: cualquier incremento de costos tiene impacto en proveedores, clientes y empleo.

La presión no es solamente laboral. Una operación de vigilancia necesita supervisión, coordinación, dotación, comunicaciones, capacitación, gestión administrativa, reemplazos, control de calidad y cumplimiento normativo. Por eso, reducir una propuesta de seguridad al precio por puesto puede producir una paradoja: el comprador consigue una tarifa menor, pero termina comprando menos capacidad real de prevención.



La tecnología ya no es un accesorio: está cambiando el puesto de trabajo

Una cámara convencional registra. Una cámara con analítica puede interpretar eventos definidos: cruce de líneas, permanencia en áreas restringidas, objetos abandonados, conteo de personas, determinados patrones de movimiento o lectura de placas, según el sistema y el contexto. La diferencia es fundamental: el centro de control deja de intentar mirar todo y empieza a recibir eventos priorizados para verificación humana.

Este cambio ya está documentado en soluciones comerciales utilizadas en Colombia. Por ejemplo, se describe aplicaciones de IA para clasificación de objetos, detección de comportamientos anómalos y reconocimiento de matrículas; también se señala la integración de analítica predictiva, IA y comunicaciones en tiempo real en el nuevo perfil del personal de seguridad. Estas referencias empresariales demuestran que la tecnología no es una promesa abstracta, aunque sus resultados dependen del diseño, la calidad de los datos, la instalación, la supervisión humana y el cumplimiento de la normativa aplicable.

Hay además una señal institucional importante: la Supervigilancia publicó protocolos operativos específicos para los servicios de vigilancia electrónica. Esto confirma que el componente tecnológico forma parte de la evolución formal del sector y no simplemente de una tendencia de marketing.

Un ejemplo colombiano: menos observación pasiva, más información útil

La propia operación de la Red de Apoyo y Solidaridad Ciudadana muestra que el valor de la vigilancia privada no se limita a custodiar físicamente un inmueble. Con corte al 30 de septiembre de 2025, la Supervigilancia reportó 877 personas capturadas, 69 armas de fuego incautadas, 145 vehículos recuperados, 7.160 motivos de policía atendidos, mercancía recuperada por \$566 millones y más de 76.000 informaciones aportadas. Son resultados atribuidos a la información reportada por los servicios de vigilancia privada y procesada dentro de la red.

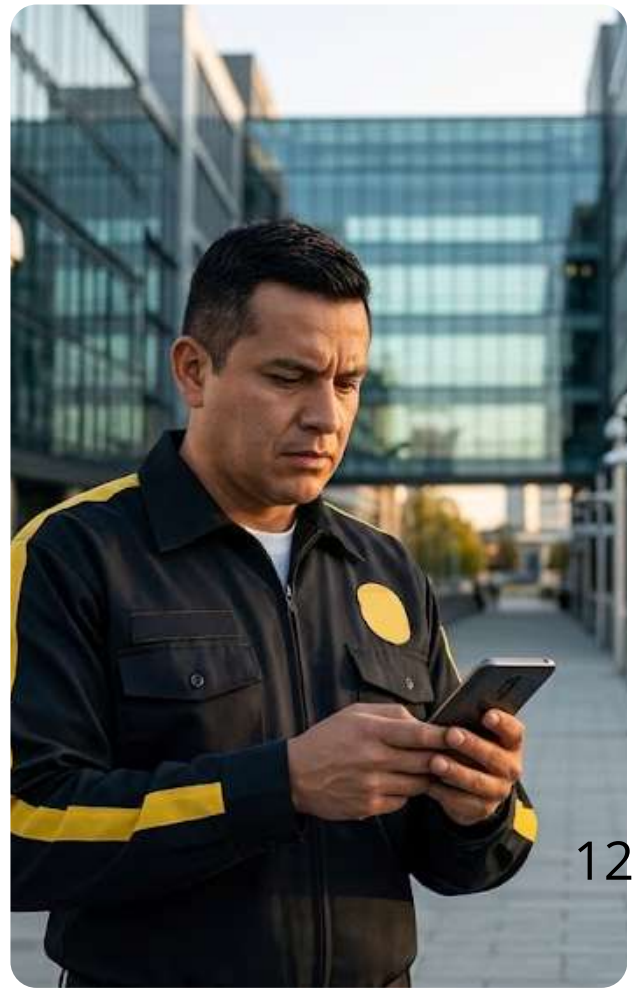
El ejemplo es revelador: el vigilante produce valor cuando observa, comunica, verifica y activa una respuesta. La tecnología puede ampliar esas capacidades. Un sistema de video analítico puede detectar un evento; un sensor puede generar una alerta; una plataforma puede georreferenciarla; un operador puede verificarla; y un equipo humano puede responder. En ese esquema, el vigilante no desaparece: cambia de función.

El verdadero riesgo para las empresas de seguridad

El mayor riesgo empresarial no es que una cámara reemplace a un vigilante mañana. El riesgo es que el cliente empiece a preguntarse por qué está pagando exclusivamente por presencia humana cuando existen alternativas para automatizar parte de la detección, documentar eventos, generar trazabilidad y medir desempeño.

Una empresa que continúe compitiendo únicamente con número de hombres, precio y uniformes queda expuesta a una guerra de tarifas. En cambio, una empresa que combine vigilancia física, monitoreo, analítica, gestión de riesgos, inteligencia de seguridad, automatización y datos puede vender una propuesta diferente: reducción de exposición al riesgo y capacidad de respuesta.

Esto obliga a cambiar incluso la conversación comercial. El marketing de una empresa de seguridad no debería limitarse a mostrar guardas, vehículos y centrales de monitoreo. Debe explicar problemas concretos: cuánto tarda en detectar un evento, cuántas falsas alarmas filtra, qué porcentaje de incidentes queda documentado, qué indicadores entrega al cliente, cómo integra tecnología y personas y qué ocurre cuando falla una capa de protección.



NUEVO CANAL

RECETAS DEL ARRIERO



Aquí encontrarás recetas explicadas paso a paso, con ingredientes sencillos y el auténtico sabor de la cocina casera.



SUBSCRIBE



ACTIVA LAS NOTIFICACIONES Y
NO TE PIERDAS NINGUNA RECETA.

*¡Cocinamos juntos,
sabores que te abrazan! ♥*

La reinversión debe dejar de ser una palabra y convertirse en evidencia

Durante años, muchos compradores han pedido al proveedor la llamada reinversión: capacitación, uniformes, equipos, tecnología o mejoras operativas. Esa exigencia sigue siendo válida, pero necesita evolucionar. El cliente debe preguntar: ¿qué parte de mi contrato se está convirtiendo en nueva capacidad de protección?

La reinversión moderna puede expresarse en analítica de video, sensores, control de acceso, botones de pánico, trazabilidad de rondas, aplicaciones para supervisores, integración de alarmas, inteligencia de datos, capacitación tecnológica, fortalecimiento del centro de operaciones e incluso dinero en efectivo. No se trata de instalar dispositivos por instalar. Cada inversión debe estar relacionada con un riesgo y producir un indicador.

Por ejemplo, un cliente puede exigir un tablero mensual con incidentes, falsas alarmas, tiempos de atención, disponibilidad de equipos, cumplimiento de rondas, eventos detectados automáticamente y acciones correctivas. Así, la conversación deja de ser “¿cuántos vigilantes me puso?” y pasa a ser “¿qué resultados de seguridad produjo el servicio?”.

Las alianzas serán decisivas

Ninguna empresa tiene que fabricar todo. El nuevo ecosistema requiere alianzas entre compañías de vigilancia, integradores tecnológicos, fabricantes de cámaras y sensores, desarrolladores de software, empresas de telecomunicaciones, analistas de inteligencia, universidades y especialistas en ciberseguridad. La seguridad del futuro será menos vertical y más colaborativa.

Para el proveedor, esto significa pasar de la lógica de “mi empresa debe resolverlo todo” a una arquitectura de socios confiables. Para el consumidor, significa evaluar si su proveedor tiene capacidad real para integrar tecnologías de terceros, proteger los datos, mantener la continuidad operativa y demostrar resultados.

También cambia el papel del marketing. Una alianza tecnológica que no se comunica, no se demuestra y no se convierte en una experiencia medible para el cliente difícilmente genera diferenciación. El marketing en seguridad debe dejar de ser solamente reputacional y convertirse en una herramienta para explicar capacidades, casos de uso, resultados y retorno de la inversión.

Supervigilancia. Resolución 20251000059517CS del 8 de agosto de 2025, actualización de tarifa mínima y fundamentos de costos laborales.
<https://supervigilancia.gov.co/documentos/7016/resolucion-n-20251000059517cs-de-08-08-2025-por-la-cual-se-actualiza-la-tarifa-minima-de-los-servicios-de-vigilancia-y-seguridad-privada/>

Supervigilancia. Preguntas frecuentes: tarifas mínimas de vigilancia y seguridad privada.
<https://supervigilancia.gov.co/publicaciones/6338/preguntas-frecuentes-supervigilancia/>

Supervigilancia. Boletín de prensa 11-2026, 18 de junio de 2026: proyecto de nuevas tarifas mínimas diferenciales y referencia a aproximadamente 360.000 trabajadores.
<https://www.supervigilancia.gov.co/web/content/18448?download=true>

Qué debería exigir hoy un comprador de seguridad

El comprador colombiano debería mirar al menos siete variables: 1) análisis real del riesgo; 2) calidad y estabilidad del personal; 3) tecnología integrada al servicio; 4) capacidad de monitoreo y respuesta; 5) indicadores y trazabilidad; 6) plan de continuidad ante fallas tecnológicas o humanas; y 7) capacidad de innovación y reinversión.

La tecnología tampoco debe convertirse en una excusa para contratar peor seguridad. Una cámara no reemplaza una decisión humana ante un incidente complejo; una alarma no interpreta por sí sola todo el contexto; y un algoritmo puede generar errores. La arquitectura adecuada es tecnológica y humana. La pregunta correcta no es “¿persona o IA?”, sino “¿qué debe hacer una persona, qué puede automatizarse y cómo se conectan ambas capacidades?”

No desaparece la seguridad física; desaparece una forma de venderla

Colombia no está ante el final de la seguridad privada, sino ante una transición profunda. Los costos obligan a optimizar; la tecnología permite detectar y documentar más; la regulación exige profesionalización; y los clientes comienzan a demandar resultados. El servicio basado únicamente en presencia física enfrenta una presión estructural que difícilmente desaparecerá.

La oportunidad está en convertir al vigilante en parte de un sistema inteligente de protección. El proveedor que entienda esta transición tendrá que invertir en tecnología, personas, datos, alianzas y marketing. El consumidor, por su parte, tendrá que dejar de evaluar únicamente cuánto paga por un puesto y empezar a evaluar cuánto riesgo realmente está cubriendo.

El futuro de la seguridad privada colombiana probablemente no será sin vigilantes. Será con menos dependencia de la vigilancia pasiva y con mayor integración entre personas, inteligencia artificial, sensores, analítica, comunicaciones y conocimiento del riesgo. En esa nueva ecuación, la empresa que no innove puede perder mercado; y el cliente que no exija innovación puede terminar pagando por una seguridad que pertenece al pasado.

Formación experiencial enfocado
en competencias
HUMANAS
Que transforman cultura.

Vivencias que conectan
con el **SER**, movilizan el
HACER y generan
resultados **reales y**
sostenibles.



LIDERAZGO



SEGURIDAD



RESULTADOS

En PODETEX
más que formar
transformamos.

www.Podetex.com



3176606549

3176606129

LA PROTECCIÓN INTEGRAL DE NIÑOS, NIÑAS Y ADOLESCENTES FRENTE A TODA FORMA DE VIOLENCIA

El deber reforzado de prevención, protección y garantía efectiva de derechos desde una perspectiva de derechos humanos

“Toda infancia merece un lugar seguro donde crecer, una voz que sea escuchada y alguien que permanezca a su lado cuando el mundo se vuelve oscuro.” (Romano Paula)

Por Dra. Paula Fabiana Romano

Resumen.

El presente trabajo aborda la protección jurídica de niños, niñas y adolescentes frente a toda forma de violencia desde el paradigma de la protección integral y el enfoque de derechos humanos. Se analiza especialmente el alcance del artículo 19 de la Convención sobre los Derechos del Niño. Se sostiene que la especial vulnerabilidad de la infancia no puede ser utilizada para disminuir su autonomía ni para justificar decisiones adulto-céntricas, sino que impone obligaciones reforzadas de protección a cargo de la familia, la sociedad y, fundamentalmente, del Estado. Se examinan el principio del interés superior, el derecho a ser oído, la obligación de prevención, la detección temprana de situaciones de riesgo, la violencia institucional y la responsabilidad derivada de las omisiones estatales. Finalmente, se propicia una concepción de la protección integral que coloque en el centro la dignidad, la integridad física y psíquica, el desarrollo y la participación efectiva de niños, niñas y adolescentes.

Palabras clave: niños, niñas y adolescentes — protección integral — violencia — vulnerabilidad — interés superior — derecho a ser oído — prevención — obligaciones estatales — derechos humanos.

Protección legal.

La ley tiene su alcance y debe proteger a mas vulnerable. La vida en la sociedad debe contener una norma donde la persona pueda desarrollarse con limites sin interrumpir ni alterar el derecho del otro.



Se consideran niños en la Convención de derechos del niño a aquella persona desde los cero años hasta los 18 años cumplidos. La misma protege para que puedan disfrutar libremente y ejercer sus derechos en forma plena, según los Tratados Internacionales de Derechos Humanos. Se hace hincapié a una vida protegida con el respeto a su intimidad, su salud. El derecho a disfrutar de un ambiente sano, no sufrir humillaciones ni abusos de Ningún tipo. El respeto a su honor, su imagen. A gozar de un nombre un documento, una nacionalidad. Se respeta su etnia, su idioma su origen. Conocer a sus padres biológicos, entablar vínculo con ellos, aunque estén separados o alguno se encuentre en prisión, salvo que ese vínculo pueda provocarle daño. A tener una familia alternativa o adoptiva que los críe cuando no puedan tener contacto directo con sus padres. A recibir educación pública y gratuita en todos los niveles, respetando su derecho a ingresar y permanecer en una escuela cerca del lugar donde viven. A gozar de los beneficios de la seguridad social. A expresar sus opiniones en la familia y que sean tenidas en cuenta tanto en la familia como en la escuela, considerando su grado de madurez. El niño debe ser escuchado, y ello no solo contempla su derecho innato, sino que en el artículo 12 de la Convención, claramente apunta a ese importante punto. A asociarse con fines culturales, deportivos o políticos siempre y cuando esas asociaciones o grupos estén sólo integradas por niños, niñas o adolescentes. Aquellos adolescentes a partir de 13 años, gozan de la libertad de poder trabajar en un ambiente libre de peligro. A los 16 años con autorización de sus representantes legales, pueden contraer nupcias. Entre esas edades pueden decidir sí mismo sobre la realización de cualquier tratamiento, siempre que no sea de tipo invasivo y no se ponga en riesgo su vida ni su integridad física. Si el tratamiento pone en riesgo su salud deben intervenir sus progenitores. Si es mayor de 16 años se lo considera como un adulto para todas las decisiones que se refieren al cuidado de su cuerpo. Si es mamá o papá a partir de los 13 años, puede decidir y realizar por sí mismo todas las tareas necesarias para el cuidado de sus propios hijos. Está prohibido que cualquier institución educativa, sea pública o privada, los sancione o discrimine por atravesar un embarazo o haber sido mamá o papá adolescente. Siempre y cuando aquellas tareas sean diligenciadas de manera eficaz y responsable, el niño atenderá a su prole autónomamente. **Cuentan con medidas de protección integral de los derechos de las niñas, niños y adolescentes., de manera integral.**



Protegerlos cuando sus derechos son amenazados o violados., en cualquier circunstancia, en caso que ello suceda el Estado intervendrá. Son las medidas de protección: Mantenerlos con su familia. Incluirlos en programas que busquen fortalecer y apoyar a las familias. Dándoles contención y protección. Si es necesario contar con una ayuda económica para que sus necesidades básicas sean satisfechas. Los programas de asistencia integral a la embarazada, donde podrá contar con los controles necesarios para un embarazo pleno y saludable.

Darles tratamientos médicos, psicológicos o psiquiátricos a cualquier menor que lo necesite o a sus padres.

Conclusiones.

Es deber del estado salvaguardar los derechos de niñas, niños y adolescentes, de manera integral y protectoria. No solo nuestra normativa cuenta con la ley de protección de la niñez, sino que claramente se encuentra, en toda la transversalidad de la convención. La protección integral de niño hasta su mayoría de edad, hace de una sociedad digna de salud mental y física para generaciones futuras y una sociedad más justa.

Referencias normativas y documentales
Convención sobre los Derechos del Niño, Naciones Unidas, especialmente arts. 3, 6, 12, 19 y concordantes. Ley 26.061, Ley de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes. **Constitución Nacional Argentina, art. 75 inc. 22.** Convención Americana sobre Derechos Humanos, especialmente arts. 5, 8, 19 y concordantes.



CONSULTORÍA EMPRESARIAL

ESTRATEGIAS QUE IMPULSAN,
RESULTADOS QUE TRANSFORMAN.

Brindamos soluciones a la medida para fortalecer la gestión, optimizar procesos y potenciar el crecimiento sostenible de tu organización.



BENEFICIOS PARA TU ORGANIZACIÓN



MEJORA DE
PROCESOS



MAYOR
PRODUCTIVIDAD



EFICIENCIA
OPERATIVA



TOMA DE DECISIONES
ESTRATÉGICAS



CRECIMIENTO
SOSTENIBLE



+57 315-511-1916



servicioalcliente@huellalogistica.com



www.huellalogistica.com.co

Seguridad empresarial: de centro de costo a habilitador estratégico

En América Latina y el Caribe, la seguridad dejó de ser una función de soporte, hoy puede convertirse en una ventaja competitiva.

Oscar Mauricio Barreto Rodríguez
Security Manager & Crisis Coordinator, North LATAM | Hitachi Energy
Bogotá, Colombia

Durante mucho tiempo, la seguridad empresarial fue vista principalmente como un mecanismo de control, dedicada a proteger instalaciones, administrar accesos y reaccionar cuando algo salía mal. Esa mirada aunque necesaria, ya resulta insuficiente. En el entorno actual, su verdadero valor está en **anticipar amenazas, reducir incertidumbre y ayudar a que el negocio tome mejores decisiones antes de que el riesgo se convierta en crisis.**

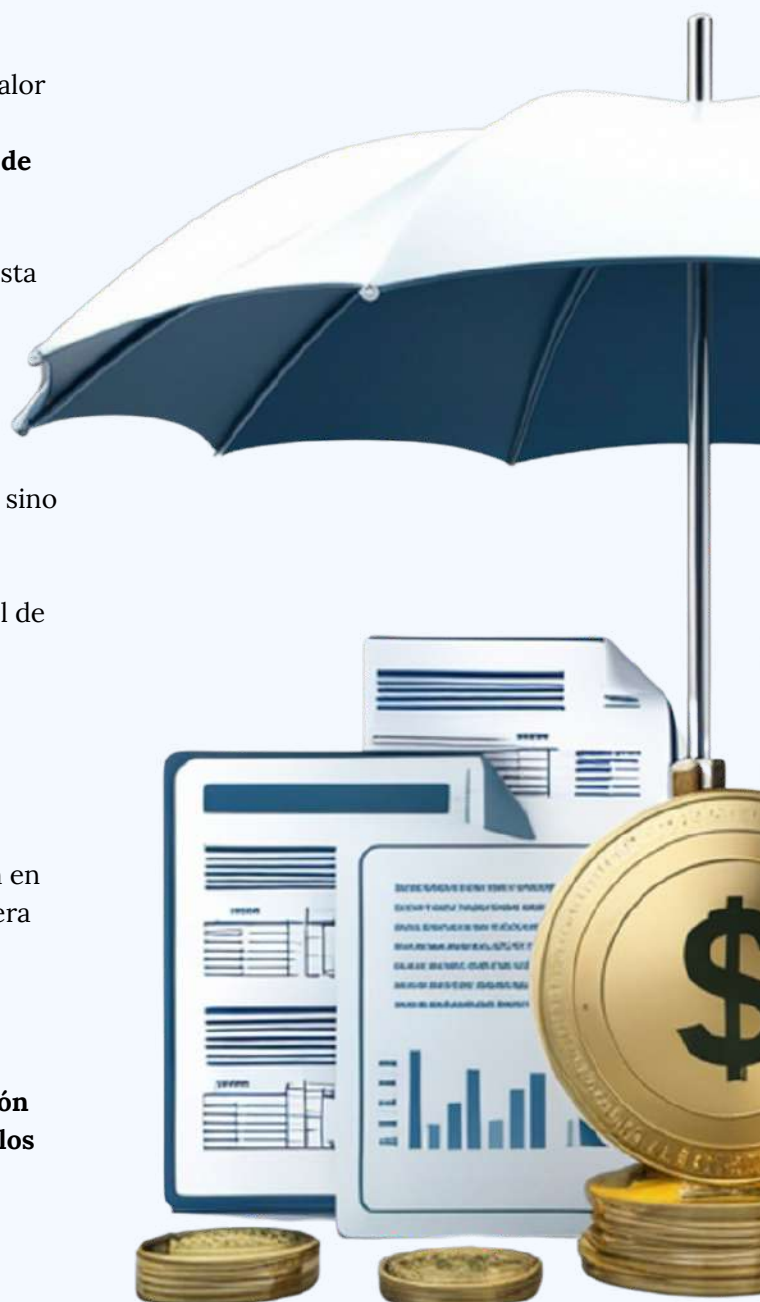
En nuestra región los ejemplos son cotidianos, una protesta que bloquea una ruta crítica, una amenaza contra un colaborador, la contaminación de una carga, un ataque cibernético que detiene sistemas esenciales o un evento natural que interrumpe comunicaciones y proveedores.

Lo importante no es que estos escenarios sean distintos, sino que todos pueden terminar afectando lo mismo, las personas, la operación, la reputación y los resultados financieros. Esa convergencia obliga a replantear el papel de la seguridad dentro de la organización.

Una región donde los riesgos convergen

América Latina y el Caribe operan sobre una realidad compleja comprendido en riesgos políticos, sociales, criminales, tecnológicos y naturales. Los cuales conviven en un mismo territorio y con frecuencia, se activan de manera simultánea.

Un análisis publicado en 2025 por el Programa de las Naciones Unidas para el Desarrollo señala que América Latina representa aproximadamente el **9 % de la población mundial, pero concentra cerca de una tercera parte de los homicidios globales.** Además, cerca del **40 % de estos homicidios** estaría relacionado con organizaciones criminales y pandillas.



umentó un **15 % el número de víctimas latinoamericanas identificadas en sitios de filtración relacionados con extorsión de datos y ransomware**. También se registró un incremento cercano al **38 % en los anuncios de intermediarios que comercializan accesos ilícitos a sistemas corporativos**.

Las cifras no deben leerse únicamente como estadísticas de seguridad pública. Para el sector empresarial, son una señal clara, el riesgo ya no se presenta en compartimentos separados. Una amenaza física puede tener un componente digital, un bloqueo social puede transformarse en una interrupción logística y una vulnerabilidad de un proveedor puede escalar hasta comprometer la continuidad del negocio.

El cambio que debe liderar la seguridad

Por eso, el reto de los gerentes y directores de seguridad no es simplemente identificar más amenazas. El verdadero desafío es lograr que la organización **entienda el riesgo, decida a tiempo y actúe de forma coordinada**. En la práctica, esto exige cambiar la conversación:

- Pasar de contar incidentes a explicar cómo impactan a las personas, los contratos, los ingresos y la continuidad del negocio.
- Pasar de reaccionar ante alertas a leer señales tempranas y anticipar escenarios.
- Pasar de proteger únicamente instalaciones a acompañar decisiones sobre proyectos, viajeros, cadenas de suministro y operaciones críticas.
- Pasar de administrar controles aislados a integrar seguridad física, ciberseguridad, continuidad del negocio, inteligencia y gestión de crisis.
- Pasar de solicitar recursos con base en la percepción de amenaza a demostrar reducción de exposición, continuidad operativa y valor tangible para el negocio.

Desde esta perspectiva, la seguridad moderna debe actuar como un puente entre la información del entorno y las decisiones de la alta dirección. Su aporte no está en decir únicamente qué no se puede hacer, sino en mostrar bajo qué condiciones el negocio puede avanzar con un nivel de exposición conocido, gestionado y aceptable.

Cinco capacidades que generan resiliencia

En mi opinión, las organizaciones que mejor enfrentan este entorno son las que fortalecen cinco capacidades básicas, pero decisivas:

1. **Inteligencia y alerta temprana:** transforman información política, criminal, social, climática y tecnológica en recomendaciones accionables.
2. **Protección integral de las personas:** incluyen colaboradores, contratistas, ejecutivos y viajeros, dentro y fuera de las instalaciones.
3. **Resiliencia de la cadena de suministro:** conocen sus rutas, proveedores críticos, puntos vulnerables y alternativas operativas.
4. **Coordinación multidisciplinaria:** conectan a Seguridad, Operaciones, Tecnología, Recursos Humanos, Comunicaciones, Legal y liderazgo empresarial.
5. **Preparación para crisis:** cuentan con criterios de activación, roles definidos, comunicaciones de emergencia, ejercicios y seguimiento de lecciones aprendidas.
- 6.

Pero estas capacidades no pueden quedarse en el discurso. Deben medirse con indicadores que conecten la gestión de seguridad con el negocio.

Del control a la confianza

La seguridad genera valor cuando permite que una organización entre a nuevos mercados, ejecute proyectos, movilice a su personal y mantenga operaciones críticas sin asumir riesgos invisibles o innecesarios.

Por eso, su éxito no debería medirse solo por la ausencia de incidentes, también debe evaluarse por su capacidad para proteger lo esencial, reducir sorpresas y darle confianza al negocio para seguir avanzando.

Una organización resiliente no es aquella que nunca enfrenta una crisis, es la que desarrolla la capacidad de leer señales tempranas, toma decisiones informadas, responde sin improvisación y recupera rápidamente su capacidad de generar valor.

Ese debería ser el nuevo propósito de la seguridad empresarial, dejar de ser vista como una barrera operativa y consolidarse como una función estratégica que ayuda a la organización a avanzar con mayor confianza, aun en contextos inciertos.



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

La profesionalización policial: punto estratégico en la gestión humana y la calidad del servicio policial

Por coronel Oleskyenio Flórez Rincón, PhD



En octubre, Costa Rica será sede de una nueva reunión de la Red de Internacionalización Educativa Policial (RINEP), espacio que congregará a directores y responsables de la educación policial de 38 instituciones de diferentes países, articuladas alrededor de aproximadamente 350 programas académicos. El encuentro constituye una oportunidad estratégica para discutir uno de los asuntos más determinantes para el futuro de los cuerpos policiales: la profesionalización de sus integrantes y su incidencia en la gestión humana, el desarrollo de la carrera y la calidad del servicio.

En varios países todavía persiste la tendencia a comprender la función policial como un empleo sustentado principalmente en el entrenamiento operativo y no como una profesión que demanda conocimiento especializado, capacidad de discernimiento, responsabilidad ética y aprendizaje permanente. Bajo esta visión limitada, la preparación del uniformado se concentra en el dominio de procedimientos, protocolos y respuestas operativas.

Estas competencias son indispensables, pero insuficientes frente a la complejidad del servicio. El policía contemporáneo debe interpretar contextos sociales, prevenir violencias, administrar conflictos, aplicar proporcionalmente la fuerza, proteger derechos, comprender nuevas formas de criminalidad, utilizar tecnologías y decidir en escenarios inciertos. No es solamente un ejecutor de instrucciones: es un profesional que ejerce autoridad pública y cuyas decisiones inciden en la libertad, la integridad, la convivencia y la confianza ciudadana.

Más allá del entrenamiento

La profesionalización no significa sustituir el entrenamiento, sino integrarlo dentro de una arquitectura educativa más amplia. Para ello debe fortalecerse el triángulo compuesto por entrenamiento, capacitación y educación, y formación integral.

El entrenamiento desarrolla destrezas para actuar con precisión, seguridad y oportunidad. La capacitación y la educación actualizan conocimientos, favorecen la especialización y permiten comprender las transformaciones de los fenómenos sociales y criminales. La formación integral construye identidad profesional, liderazgo, ética pública, disciplina y vocación de servicio.

Cuando alguno de estos componentes se impone sobre los demás, el modelo pierde equilibrio. El entrenamiento sin educación puede producir respuestas mecánicas; la educación sin entrenamiento puede generar conocimientos difíciles de aplicar; y ambos, sin formación ética, pueden convertirse en capacidades desprovistas de sentido público.

Profesionalizar implica que el uniformado no solo sepa ejecutar un procedimiento, sino que comprenda por qué debe realizarlo, cuáles son sus límites, qué consecuencias puede producir y cómo contribuye a resolver el problema que motivó la intervención.

De escuelas a universidades policiales

Uno de los principales retos de la RINEP consiste en determinar cómo adecuar las normas, los planes de estudio y las estructuras institucionales para que las escuelas de formación evolucionen hacia verdaderas instituciones de educación superior policial.

Este cambio no puede limitarse a sustituir la palabra *escuela* por *universidad*. Una universidad policial exige rigor académico, profesores cualificados, investigación, producción de conocimiento, innovación curricular, internacionalización y sistemas verificables de aseguramiento de la calidad.

Aunque respondan a necesidades particulares de los cuerpos de policía, estas instituciones no pueden permanecer aisladas de la regulación, inspección y vigilancia de los ministerios de Educación o de las autoridades académicas competentes. Este control garantiza la calidad de los programas, la idoneidad de los docentes, la transparencia de los procesos, la validez de los títulos y el reconocimiento de sus egresados dentro y fuera de la institución policial.

La especificidad del servicio no debe convertirse en una excepción frente a los estándares académicos nacionales. El desafío consiste en construir un modelo equilibrado: con identidad policial en sus contenidos y propósitos, pero sometido al mismo rigor exigido a las demás instituciones de educación superior.

Educación y calidad del servicio

La principal justificación de la educación superior policial se encuentra en la calidad del servicio que recibe la ciudadanía. No se trata únicamente de aumentar el número de programas o uniformados titulados, sino de formar policías capaces de comprender mejor los problemas, tomar decisiones más acertadas y actuar con mayor legitimidad.

La calidad del servicio se manifiesta en actuaciones legales, oportunas, efectivas, proporcionales y respetuosas. También se expresa en la capacidad para escuchar al ciudadano, explicar las decisiones, resolver conflictos, anticipar riesgos y aprender de los errores. Estas competencias no se adquieren exclusivamente mediante la repetición de procedimientos; requieren educación, reflexión e investigación.

La educación superior fortalece la capacidad para analizar información, argumentar decisiones, evaluar intervenciones y producir conocimiento. Permite comprender que cumplir un procedimiento no siempre equivale a solucionar el problema que lo originó y que la eficacia policial debe acompañarse de legitimidad, justicia procedimental y respeto por los derechos.

Un título académico no garantiza automáticamente un servicio de calidad. La educación debe articularse con liderazgo, supervisión, bienestar, recursos, evaluación y cultura institucional. Sin embargo, una policía que no desarrolla pensamiento crítico ni conocimiento especializado tendrá mayores dificultades para responder a la complejidad social y criminal.

Por ello, la calidad educativa también debe medirse por sus efectos sobre el servicio: reducción de errores, mejor toma de decisiones, disminución de conductas indebidas, innovación operativa, uso adecuado de la fuerza, solución de problemas y fortalecimiento de la confianza ciudadana.



Profesionalización y gestión humana

La educación policial alcanza su verdadero valor cuando se integra con una política moderna de gestión humana. No basta con educar al funcionario; es necesario proyectar cómo ese conocimiento acompañará su ingreso, desempeño, movilidad, especialización, ascenso, liderazgo y preparación para el retiro.

Los cuerpos policiales necesitan planes de carrera claros, conocidos y previsibles. Cada integrante debe comprender cuáles son las rutas de desarrollo disponibles, qué competencias requiere cada nivel de responsabilidad, cómo puede acceder a funciones especializadas y cuáles son los criterios para la movilidad y el ascenso.

Para conseguirlo se requieren mapas de competencias, perfiles de cargo, catálogos de especialidades, sistemas de información sobre formación y experiencia, evaluaciones del desempeño, planes de sucesión, bancos de talentos y rutas educativas relacionadas con los distintos momentos de la carrera.

La educación superior puede organizarse mediante ciclos progresivos: técnico profesional, tecnológico, universitario y de posgrado, de acuerdo con la regulación de cada país. La experiencia acumulada en el servicio también debe ser evaluada y reconocida, evitando que conocimientos construidos durante años permanezcan invisibles para el sistema educativo.

Esta articulación no significa que un policía especializado deba permanecer indefinidamente en un mismo cargo o territorio. La movilidad y la atención de las necesidades del servicio forman parte de la naturaleza de las organizaciones policiales. Las instituciones deben conservar la capacidad de trasladar y reubicar a sus integrantes según sus prioridades operativas.

No obstante, esas decisiones deben apoyarse en información suficiente. Siempre que sea posible, la movilidad debe conciliar las necesidades institucionales con las competencias, la experiencia y el potencial de las personas. El propósito no es inmovilizar el talento humano, sino emplearlo estratégicamente. Incluso la rotación puede enriquecer el perfil profesional cuando responde a una trayectoria deliberada y no a movimientos desconectados del plan de carrera.

Educar para toda la vida

La gestión humana también debe preparar al uniformado para su vida en la reserva. Después de décadas de servicio, el policía no puede retirarse con una enorme experiencia, pero sin herramientas para proyectarse hacia la docencia, la investigación, la consultoría, la administración pública, la seguridad privada o el liderazgo social.

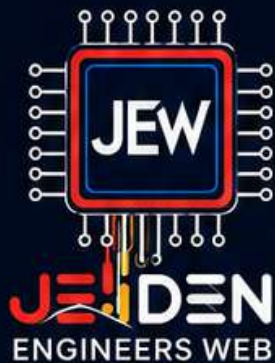
La RINEP puede desempeñar un papel decisivo mediante estándares compartidos, reconocimiento académico, movilidad de docentes y estudiantes, investigaciones comparadas y programas conjuntos. Su dimensión permite pensar en una auténtica comunidad internacional de conocimiento policial.

El debate de fondo consiste en decidir si los cuerpos policiales continuarán preparando personas para ocupar empleos o si formarán profesionales capaces de construir una carrera, producir conocimiento y prestar un servicio de alta calidad.

Una organización que solamente entrena responde a los problemas conocidos. Una organización que educa, investiga y gestiona estratégicamente su talento humano está en mejores condiciones de comprender los cambios, anticipar los riesgos y transformar su servicio.

Profesionalizar al policía es reconocer que detrás del uniforme existe un servidor público que piensa, decide, aprende y evoluciona. La calidad del servicio comienza mucho antes de la actuación en la calle: empieza en la forma como cada institución selecciona, forma, educa, emplea, moviliza y proyecta a su talento humano.





SOLUCIONES DIGITALES

CREAMOS EXPERIENCIAS QUE HACEN CRECER

Diseñamos páginas web modernas, rápidas y funcionales que impulsan tu negocio.



NUESTROS SERVICIOS



DISEÑO WEB

Sitios web atractivos, modernos y adaptados a tu marca.



DESARROLLO FRONT-END

Interfaces rápidas, intuitivas y optimizadas para todos los dispositivos.



MANTENIMIENTO WEB

Actualizaciones, mejoras y soporte técnico para que tu web siempre funcione.



SOLUCIONES DIGITALES

Integramos herramientas digitales que optimizan y automatizan tu negocio.

¿POR QUÉ ELEGIRNOS?

- Diseños 100% personalizados**
Creamos sitios únicos que reflejan la identidad de tu marca.
- Tecnología de vanguardia**
Usamos las mejores herramientas para garantizar rendimiento y seguridad.
- Enfoque en resultados**
Desarrollamos soluciones que generan impacto y te ayudan a crecer.
- Acompañamiento continuo**
Estamos contigo en cada etapa, antes, durante y después del proyecto.



BENEFICIOS PARA TU NEGOCIO

- Mayor presencia digital**
Conecta con más clientes y haz crecer tu marca.
- Más clientes potenciales**
Sitios web diseñados para convertir visitas en oportunidades.
- Rendimiento y velocidad**
Webs optimizadas para cargar rápido y ofrecer la mejor experiencia.
- Seguridad garantizada**
Protegemos tu sitio y la información de tus usuarios.



LLEVEMOS TU NEGOCIO
AL SIGUIENTE NIVEL

Transforma tu presencia digital con expertos en **desarrollo web** y **aplicaciones móviles**.



MÁS INFORMACIÓN

www.jeidenengineersweb.com



CONTÁCTENOS

+57 320 206 35 49



CORREO CORPORATIVO

jeidenengineersweb@gmail.com

Biometría y protección de datos: una conexión imprescindible

Enrique Alonso Braña.

Director y Jefe de seguridad. Detective privado.
España

¿Están la biometría y la protección de datos unidos realmente por una conexión imprescindible?

¿Qué significa el término biometría?

La palabra biometría viene del griego “bios” – vida y “metron” – medida, y puede definirse como el estudio para el reconocimiento inequívoco de personas, basado en uno o más rasgos físicos o conductuales propios de uno mismo.

Con el paso del tiempo se ha establecido como el medio más adecuado para identificar y autenticar personas de forma rápida, pero sobre todo con mucha confiabilidad, a través del uso de características biológicas únicas del sujeto.

Existen las características de conducta, entre las que encontramos por ejemplo la forma de andar o la firma. Sin embargo, dentro de las características físicas están la huella dactilar o nuestro rostro.

En un mundo tan tecnológico, cada vez está más extendido el tratamiento de datos biométricos en ámbitos muy diversos y con numerosas finalidades.

En el sector de la seguridad su utilización cada vez es mayor en sistemas de control de acceso a recintos. También en el control de acceso a aplicaciones y también se ha adaptado como herramienta “onboarding” de muy alta fiabilidad para otras tecnologías.

No obstante, debemos pararnos a analizar si aquello que estamos instalando como una ingeniería especializada es adecuado para el objetivo que se persigue. También sobre todo si cumple con las normativas vigentes en materia de protección de datos:

-Reglamento General de Protección de Datos (RGPD): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (DOUE núm. 119, de 4 de mayo de 2016, páginas 1 a 88)

-la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD): Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE núm. 294, de 06/12/2018).



¿Cómo recoge el RGPD la biometría?

A este respecto, teniendo en cuenta que los datos biométricos vienen definidos en el RGPD como datos personales, el tratamiento que se haga de los mismos debe cumplir con la normativa de protección de datos y es por ello que hemos de ser especialmente cuidadosos en la interpretación de los artículos 4.14 y 9.1 del RGPD.

El artículo 4.14 del RGPD define como dato biométrico a los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o huellas dactilares.

Por otro lado, el artículo 9.1 del RGPD incluye entre los muchos datos de categoría especial los datos biométricos que están dirigidos a identificar de manera unívoca a una persona física. Entonces, llevando a cabo una interpretación conjunta de ambos artículos, se entiende que:

Los datos biométricos solo constituirían una “categoría especial” de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a “identificar de manera unívoca” a una persona física.

Es por ello que la regulación e interpretación jurídica de los sistemas biométricos debe estar ligada a dos puntos:

- Las características técnicas: qué datos se van a tomar en nuestros sistemas.
- Objetivo final y condiciones de funcionamiento: para qué se van a tomar esos datos.

¿Y cuándo podemos utilizar datos de carácter personal?

Los datos de carácter personal solo pueden utilizarse si son adecuados, convenientes y no excesivos. Ello implica que se debe analizar en cada caso la necesidad y proporcionalidad de los datos tratados. Si la finalidad perseguida podría alcanzarse de una forma menos agresiva o invasiva.

Para analizar la proporcionalidad de un sistema biométrico, este debe superar tres juicios:

- Idoneidad: valorar si el sistema es eficaz para el objetivo perseguido.
- Necesidad: analizar si el sistema biométrico es necesario para dar respuesta a la necesidad detectada, y no únicamente es el sistema más adecuado o rentable.
- Proporcionalidad en sentido estricto: valorar si la pérdida de intimidad del individuo es proporcional a los beneficios que se esperan obtener.

El uso de un sistema de identificación biométrica debe estar “justificado” y debe contar con todas las medidas de seguridad necesarias para garantizar la confidencialidad de los datos biométricos usados por el sistema de manera que dichos datos no se usen con otros fines diferentes a los aceptados por los interesados y de los que han sido informados.

Resumiendo, sobre lo anterior, hay que analizar cómo se llevará el tratamiento de datos biométricos desde el punto de vista de protección de datos, siempre centrados en la relación directa con los sistemas de control de acceso y sus implicaciones en el marco del RGPD.

Verificación o identificación

Y llegamos a un punto importante sobre la forma de realizar un reconocimiento biométrico. Debemos escoger si trabajar con verificación/autenticación o identificación.

Es importante diferenciar qué tipo de consulta se lleva a cabo con los datos biométricos. Aparecen entonces en escena dos términos que pueden parecer similares pero son muy distintos: verificación (1:1) e identificación biométrica (1:N).

Hablamos de verificación/autenticación cuando el proceso busca una correspondencia “uno a uno”.

Antes de nada, el usuario se identifica con un dato que puede ser un nombre o un DNI por ejemplo, y después el sistema recoge la característica biométrica y se compara con la muestra almacenada (adquirida antes con la verificación).

Es un proceso sencillo pues está comparando solo dos muestras con un resultado de OK o KO.

En cambio, si nos referimos a identificación entonces estamos comprobando si una persona es uno de los miembros de un grupo determinado (compara con todos a la vez).

Consiste en la comparación de la muestra recogida del usuario, obtenida en el momento de la identificación, frente a una base de datos de plantillas de usuarios ya registradas con anterioridad. Este método, conocido como “uno a muchos”, necesita comparar la muestra con cada una de las que ya estaban almacenadas para buscar un “matching”.

Hasta hoy en día esta cuestión referida a Verificación/Autenticación e Identificación siempre se trató desde el punto de vista técnico, pero ahora ya tiene implicaciones con la protección de datos que han tomado máxima relevancia.

LÍDERES QUE TRANSFORMAN DECISIONES EN RESULTADOS

Desarrolla una visión estratégica multidimensional para liderar con impacto en un mundo complejo y cambiante.



Enfoque multidimensional
Integra perspectivas militares, policiales y corporativas.



Metodología experiencial
Conferencias, ejercicios prácticos, casos reales y estancias nacionales e internacionales.



Red de alto nivel
Conecta con líderes y expertos a nivel nacional e internacional.



Mentoring personalizado
Acompañamiento continuo para potenciar tu liderazgo y toma de decisiones.

+57 316 5236604

palem@unimilitar.edu.co
martha.tovar@unimilitar.edu.co

Escuela de Altos Estudios
Estratégicos Nueva Granada



Inscripciones
abiertas
Del 31 de julio al
12 de diciembre
de 2026



Valor total
\$64.950.000
Descuentos
institucionales



Campus
Nueva Granada
Cajicá - Colombia

EL PALEM fortalece tus competencias en:



Liderazgo y
toma de decisiones



Desarrollo
productivo



Gobernanza y
Asuntos Globales



Estrategia,
geopolítica
y perspectiva



Innovación
tecnológica

Anteriormente mencionamos los artículos 4.14 y el artículo 9.1 del RGPD que definen lo que se considera dato biométrico de carácter especial, haciendo hincapié sobre el tratamiento técnico específico para identificar sin equivocación a una persona concreta.

Además, vemos que el Considerando 51 del RGPD dice lo siguiente: “El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física”.

Una vez analizados estos artículos del RGPD se puede interpretar que todo tratamiento de datos biométricos no debe ser considerado como tratamiento de datos de categorías especial.

Si adicionalmente nos fijamos en las diferencias entre identificación biométrica (1:N) y verificación/autenticación biométrica (1:1), aunque el artículo 4 del RGPD podría hacer pensar que el concepto de dato biométrico incluye a los dos, hemos visto que los datos biométricos únicamente tendrán la consideración de “datos de categoría especial” en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (1:N) y no cuando se corresponda con verificación biométrica (1:1).

La importancia del cumplimiento legal

Hemos estado viendo RGPD, datos de categoría especial, juicios de idoneidad, necesidad y proporcionalidad, confidencialidad, diferenciación entre verificación e identificación..., pero aún hay más asuntos que se deben tener en cuenta. Hay un factor de cumplimiento legal muy importante que requiere que todos estos aspectos mencionados sean analizados. Antes de nada, mediante la realización de una evaluación de impacto de protección de datos que determine si se cumplen los juicios antes expuestos. Si se está aplicando correctamente el reconocimiento biométrico.

Una Evaluación de Impacto de Protección de Datos es una evaluación relacionada con la privacidad cuyo objetivo es identificar y analizar cómo la privacidad de los datos puede verse afectada por determinadas acciones que se apliquen incorrectamente. Siempre se exigirá una Evaluación de Impacto de Protección de Datos cuando el tratamiento de los datos pueda suponer un alto riesgo para los derechos y libertades de las personas o para su privacidad y siempre previamente a cualquier trabajo sobre el tratamiento de los datos.

Hay que analizar cómo va a ser el tratamiento en sí. Evaluar los riesgos que el mismo supone y aplicar las medidas correctoras oportunas para poder llevarlo a cabo. Es posible que se concluya que el tratamiento de datos no se puede llevar a cabo. Otra opción es que se debe cambiar el sistema de tratamiento por otro diferente, menos invasivo.

En conclusión

Existe mucha reglamentación que no todas las empresas tienen en cuenta a la hora de diseñar una solución de seguridad que implique un tratamiento de datos biométricos.

No solo hay que escoger un sistema de reconocimiento biométrico porque un cliente lo solicite. Tampoco porque esté de moda o porque pensemos que puede ser el más idóneo. Se debe analizar cuál va a ser el impacto sobre la privacidad de nuestra información biométrica.

Hay que estudiar de forma exhaustiva si es válido para el objetivo. También valorar si es realmente necesario si la pérdida de privacidad es proporcional al beneficio que se va a entregar.



@bascbogotá-colombia



SEGURIDAD COMO VENTAJA COMPETITIVA

LA DIFERENCIA ESTÁ EN
CÓMO GESTIONAS EL RIESGO

BASC Bogotá - Colombia

Seguridad que protege

Confianza que genera **oportunidades**



De Bismarck a la inteligencia artificial: evolución de la Medicina del Trabajo en Alemania

Álvaro Castillo Strampfer
Especialista en Medicina del Trabajo

La Medicina del Trabajo probablemente sea la rama de esta profesión que, con mayor sensibilidad, refleja aspectos socioeconómicos, culturales y hasta políticos de una sociedad. Entrar en el plano comparativo por países sería tanto un error, como también innecesario y carente de sentido. Conocer sus distintas facetas debe ayudarnos a comprender mejor y enriquecer nuestra perspectiva humanista.

Si bien la base médico-científica es casi siempre bastante similar, fue la normativa técnico-jurídica la que debió adaptarse al entorno en cada país para concretar esos fundamentos científicos en la práctica.

Son pocos los casos en los que la seguridad y la salud en el trabajo van más allá del conjunto de estándares o normas y forman parte integral de la propia evolución histórica. Alemania es uno de ellos.

Para comprender plenamente la esencia de la Medicina del Trabajo alemana es necesario retroceder más de 150 años, hasta la época de la Revolución Industrial. Este proceso llegó al país varias décadas después que en Inglaterra y llegó a consolidarse con la creación del Imperio alemán en 1871.

La figura de Otto von Bismarck, primer canciller del Imperio alemán, desempeñó un papel decisivo. Con una visión muy avanzada para su tiempo, impulsó políticas sociales innovadoras que sentaron las bases de lo que más tarde se convertiría en el actual sistema alemán de seguridad social y, posteriormente, en las normas que regulan la protección laboral y la Medicina del Trabajo.

El desarrollo industrial en las décadas posteriores a la fundación del Imperio, caracterizado por el auge de las industrias química y electrotécnica, provocó un crecimiento urbano acelerado debido a la migración masiva de población procedente del medio rural en busca de empleo. Este fenómeno, unido a las deficiencias sanitarias de la época, favoreció la aparición de epidemias y elevó la mortalidad, además de las enfermedades y accidentes que diariamente se producían en las fábricas. Esta situación impulsó a Bismarck a adoptar medidas destinadas a modernizar el Estado, garantizar la productividad y mejorar las condiciones de vida de la población.



En la década de 1880 se crearon el Seguro de Enfermedad, el seguro obligatorio de accidentes de trabajo y el Seguro de Invalidez y Vejez.

Casualmente, en aquella época, científicos como Robert Koch, Paul Ehrlich y Emil von Behring, en el célebre Charité de Berlín, contribuían decisivamente al desarrollo de la microbiología y de la inmunología modernas, cuyos avances siguen teniendo una enorme relevancia en el ámbito de la prevención laboral.

La industrialización trajo consigo también importantes avances sociales; Robert Bosch, el célebre industrial suabo, implantó en sus fábricas, a principios del siglo XX, la jornada laboral de ocho horas, así como comedores, viviendas y diversos beneficios sociales para sus trabajadores, estableciendo un precedente que aún hoy se recuerda.

Con la fundación de la República Federal de Alemania en 1949 después de la guerra, la nueva Constitución estableció un sólido marco basado en un profundo respeto a la dignidad humana, la vida, la integridad física, la libertad y la igualdad de derechos.

Ello tuvo, inevitablemente, importantes repercusiones en las prestaciones sociales y laborales, muchas veces difíciles de comprender desde otros contextos culturales, donde con frecuencia son interpretadas como excesivamente permisivas o generosas.

La segunda mitad del siglo XX marcó una etapa decisiva en la protección de la seguridad y la salud en el trabajo. La aprobación de la Ley de Seguridad en el Trabajo en 1973 y de la Ley de Protección Laboral en 1996 consolidó el modelo de colaboración entre el médico del trabajo y el ingeniero de seguridad, estableciendo funciones claramente definidas y la presencia regular de ambos profesionales en empresas de todos los tamaños y rubros. Entre las funciones del médico del trabajo destacan principalmente los reconocimientos médico-ocupacionales.

Los primeros años del siglo XXI trajeron consigo importantes innovaciones normativas y organizativas. Entre ellas destaca la Segunda Norma de la Mutua Alemana de Accidentes en el Trabajo, que determina de manera precisa el tiempo que tanto el médico del trabajo como el ingeniero de seguridad deben dedicar a cada empresa en función del nivel de riesgo y del número de trabajadores.

El año 2013 constituye asimismo un hito de especial relevancia. En esa fecha se reformó en profundidad la ordenanza reguladora de los reconocimientos médico-ocupacionales, aclarando de forma muy pragmática el tradicional dilema entre la vigilancia preventiva y la evaluación de la aptitud laboral. Esta reforma supuso una transformación sustancial en la práctica de la Medicina del Trabajo, del propio concepto de prevención y de las relaciones entre empleadores y trabajadores.

Desde mi experiencia profesional y tras haber vivido de primera mano las transformaciones de las dos últimas décadas, considero que Alemania dispone actualmente de un sistema sólido y preparado para afrontar los desafíos del siglo XXI. Cuenta con una base apta para responder a los grandes retos que se vislumbran: el cambio climático, el envejecimiento demográfico, la inteligencia artificial y una creciente interconexión global.

Si Bismarck entendió que la salud del trabajador era un tema de Estado, hoy la inteligencia artificial nos obliga a preguntarnos qué significa proteger la dignidad del trabajo en un entorno completamente nuevo.





EL SABOR AUTÉNTICO DEL BÚFALO

Ven y vive la experiencia
Colbúfala bga

RESTAURANTE

TE ESPERAMOS



11:00AM-8:00PM



@COLBUFALABGA



CRA 30# 32-59

LA AURORA-BUCARAMANGA

GESTIÓN DE CRISIS Y REPUTACIÓN

Cómo sobrevive una empresa al escándalo

Casos reales y estrategias para responder ante un delito corporativo o una filtración mediática

“Una crisis reputacional no se resuelve solo comunicando; se resuelve controlando el hecho, asumiendo responsabilidades y demostrando cambios verificables.”

Carlos Eduardo Valenzuela Oviedo – CPP
Asesor de Seguridad y Criminología Corporativa

Cuando el incidente deja de ser operativo

Una organización puede tardar décadas en construir confianza y apenas unas horas en ponerla en riesgo. Una investigación judicial, una conducta irregular de sus empleados, una filtración de información, un fraude interno, un ataque informático o la difusión de un video en redes sociales pueden transformar rápidamente un problema operativo en una crisis capaz de afectar clientes, trabajadores, inversionistas, autoridades y opinión pública. En ese momento ya no está en juego solamente lo que ocurrió: también importa la forma en que la empresa responde.

La primera reacción suele ser tratar la crisis reputacional como un problema de comunicaciones: preparar un comunicado, designar un vocero y reducir la exposición mediática. Esa visión es insuficiente. Una crisis seria compromete al mismo tiempo la seguridad, la operación, el cumplimiento normativo, el área jurídica, el liderazgo y la reputación. Por eso, gestionar una crisis exige capacidad para tomar decisiones bajo presión, proteger a los afectados, preservar evidencia, coordinar a los responsables y comunicar únicamente aquello que pueda sostenerse con hechos.

No todos los incidentes se convierten en crisis reputacionales. El salto ocurre cuando el evento empieza a cuestionar algo más profundo: la confianza en la organización. Si un funcionario manipula contratos para favorecer a un proveedor, el asunto puede comenzar como una investigación interna. Pero si posteriormente aparecen documentos que demuestran que otros directivos conocían la situación y no actuaron, la discusión deja de centrarse en un individuo y pasa a cuestionar la cultura de la empresa, sus controles y la conducta de sus líderes.

La primera regla: no defender la reputación antes de entender los hechos

La presión pública puede impulsar a una organización a negar de inmediato las acusaciones, minimizar su gravedad o señalar rápidamente a un responsable. El riesgo es evidente: cada declaración queda registrada. Si después aparecen correos, grabaciones, informes o testimonios que contradicen la primera versión, la empresa enfrenta dos problemas simultáneos: la crisis original y una nueva crisis provocada por su propia respuesta. Rapidez, por tanto, no significa improvisación. Es preferible reconocer que hay hechos en verificación, explicar las medidas de contención y comprometer nuevas actualizaciones que ofrecer certezas falsas para tranquilizar momentáneamente al mercado o a la opinión pública.



Volkswagen: cuando el problema es la integridad

El caso conocido como Dieselgate ilustra cómo una falla técnica puede convertirse en una crisis de integridad. En 2015 se reveló que Volkswagen había instalado software en determinados vehículos diésel para detectar cuándo estaban siendo sometidos a pruebas de emisiones y modificar su comportamiento. La gravedad reputacional no provenía solamente de que los automóviles emitieran más contaminantes de lo permitido, sino del carácter deliberado del mecanismo. La pregunta pública cambió de “¿qué falló?” a “¿quién lo sabía y por qué se permitió?”.

Wells Fargo: cuando los indicadores terminan gobernando la conducta

Un segundo caso permite observar una dimensión distinta. En 2016 se conoció que empleados de Wells Fargo habían abierto cuentas y solicitado productos financieros sin autorización de los clientes para cumplir metas comerciales. La investigación mostró que los sistemas de incentivos y la presión por resultados favorecían este tipo de prácticas. El caso demuestra que una empresa puede tener códigos de ética, políticas de cumplimiento y canales de denuncia bien redactados y, al mismo tiempo, generar condiciones que empujan a las personas en sentido contrario.

Desde una mirada de criminología corporativa, el análisis no puede detenerse en el trabajador que ejecutó la conducta irregular. También debe preguntarse qué mecanismos organizacionales la hicieron posible: ¿había metas desproporcionadas?, ¿se ignoraban señales de alerta?, ¿los supervisores conocían la práctica?, ¿existían castigos por no alcanzar objetivos?, ¿las denuncias internas eran escuchadas? Despedir responsables puede ser necesario, pero rara vez es suficiente si el sistema que produjo el comportamiento permanece intacto.

Equifax: una filtración tecnológica puede convertirse en una crisis de confianza

La brecha de seguridad sufrida por Equifax en 2017 comprometió información personal de aproximadamente 147 millones de personas. El incidente mostró que la ciberseguridad dejó de ser un asunto exclusivo de los equipos de tecnología. Cuando una empresa almacena información sensible, proteger esos datos forma parte de la promesa que mantiene con clientes y ciudadanos. Una falla en esa protección puede afectar simultáneamente la continuidad operacional, la responsabilidad jurídica, la confianza del público y la relación con autoridades regulatorias.

Frente a una filtración de este tipo, la comunicación cumple una función práctica y no solamente reputacional. Las personas necesitan saber qué ocurrió, qué información puede estar comprometida, qué riesgos existen y qué deben hacer para protegerse. Retrasar estos mensajes para evitar impacto mediático puede aumentar el daño. En una crisis tecnológica, la protección del afectado debe estar por encima del impulso de controlar la narrativa.

Controlar antes que maquillar

Los tres casos anteriores muestran una diferencia esencial entre gestionar una crisis y gestionar su apariencia. Ante una situación grave, la organización necesita activar un equipo con capacidad real de decisión. Dependiendo del evento, este puede integrar alta dirección, seguridad corporativa, área jurídica, cumplimiento, comunicaciones, tecnología, recursos humanos y operación. Lo importante es que exista una sola imagen de situación, una cadena clara de decisiones y un mecanismo permanente de actualización.

Las primeras preguntas deberían ser concretas: ¿qué sabemos?, ¿qué todavía no sabemos?, ¿quién puede resultar afectado?, ¿el evento continúa?, ¿qué debemos detener de inmediato?, ¿qué evidencia debe preservarse?, ¿qué autoridades deben ser informadas?, ¿qué obligaciones contractuales o regulatorias se activan?, ¿quién está autorizado para hablar? Estas preguntas reducen el riesgo de que cada área actúe por separado y termine transmitiendo mensajes contradictorios.

Solo después debe definirse la comunicación pública. La primera declaración no necesita resolver toda la crisis. Puede informar que existe una situación bajo investigación, describir las medidas inmediatas adoptadas y anunciar cuándo habrá una nueva actualización. Lo fundamental es evitar afirmaciones que la organización no pueda demostrar. En contextos de alta exposición, reconocer lo que aún no se sabe suele ser más responsable que aparentar una certeza que puede desmoronarse horas después.





CUMBRE GLOBAL DE SEGURIDAD

Más unidos por la sostenibilidad

CONSTRUYENDO SEGURIDAD, DESDE LAS REGIONES

TE INVITAMOS A LA 3^{RA} CUMBRE GLOBAL DE SEGURIDAD 2026



**Gobierno y Sectores
público/privado:**

Un encuentro que nos une con seguridad.



JUEVES
29 DE OCTUBRE
2026



07:00 AM



HOTEL MARRIOTT
Ciudad salitre
Calle 25 B #69 B - 53



VALOR INSCRIPCIÓN
\$ 900.000

TEMAS:



**RETOS REGULATORIOS
DE LA VIGILANCIA Y LA
SEGURIDAD PRIVADA**



**INTELIGENCIA
ARTIFICIAL EN LA
GESTIÓN DEL RIESGO**



**RESILIENCIA
Y RECUPERACIÓN**



**VOCES DE
AUTORIDADES,
GREMIOS, EMPRESARIOS
Y EXPERTOS.**



INSCRÍBETE AQUÍ
ATRAVÉS DEL FORMULARIO

ORGANIZA:



PATROCINADOR OFICIAL:



APOYA:



Lo que realmente protege la reputación

La reputación comienza a reconstruirse cuando las decisiones respaldan el discurso: detener la conducta dañina, cooperar con las autoridades, apoyar a los afectados, revisar controles y rendir cuentas. La transparencia no exige divulgar información reservada; exige distinguir entre hechos confirmados e hipótesis, evitar la manipulación y mantener coherencia entre lo que la empresa comunica hacia afuera y lo que realmente está haciendo por dentro.

Línea de tiempo: fases de respuesta corporativa ante una crisis reputacional

De la reacción al aprendizaje

La secuencia no es una fórmula rígida, pero ayuda a ordenar prioridades. En la precrisis se construyen protocolos, comités, voceros y sistemas de alerta. En las primeras horas se contiene el evento, se protege a las personas y se preserva evidencia. Después se comunica lo confirmado, se investiga con mayor profundidad, se estabiliza la operación y se corrigen versiones. La fase de corrección exige reparar daños, establecer responsabilidades y ajustar controles; finalmente, la postcrisis convierte la experiencia en aprendizaje organizacional.

Sobrevivir al escándalo

Una crisis no necesariamente destruye una empresa. Lo que puede hacerlo es la incapacidad para comprender su gravedad, asumir responsabilidades y corregir aquello que permitió que ocurriera. Volkswagen muestra cómo una conducta deliberada puede cuestionar la integridad corporativa; Wells Fargo evidencia el impacto de una cultura de incentivos mal diseñada; y Equifax confirma que una vulnerabilidad tecnológica puede transformarse en una crisis masiva de confianza. Los orígenes son distintos, pero el reto es el mismo: responder de forma coherente, verificable y responsable. En definitiva, la reputación no depende solo de encontrar las palabras correctas, sino de hacer lo correcto cuando todos están mirando.

La gestión eficaz combina preparación, contención, comunicación, investigación, corrección y aprendizaje.

Línea de tiempo: fases de respuesta corporativa ante crisis reputacional

De la preparación al aprendizaje, una respuesta más sólida para un futuro con mayor confianza.



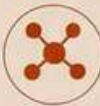


NUEVO LANZAMIENTO
PRÓXIMAMENTE

LA REVOLUCIÓN
DE LA BELLEZA
Sin Cirugía

CIENCIA
QUE TRANSFORMA.
RESULTADOS
QUE SE VEN.

UNA NUEVA ERA. UN NUEVO TÚ.
PRÓXIMAMENTE, CONOCE MÁS.



PÉPTIDOS
DE ÚLTIMA
GENERACIÓN



EXTRACTOS
NATURALES
PREMIUM



APOYA TU
METABOLISMO
Y DEFINICIÓN



BIENESTAR
Y PROTECCIÓN
INTEGRAL

MÁS QUE UN PÉPTIDO,
ES TU PRÓXIMA EVOLUCIÓN.

@lipoflackcolombia

@lipoflack

3219345161

Toxicología Industrial y Gestión del Riesgo Químico: Un Enfoque Integral desde la Seguridad y Salud en el Trabajo

Por: Diego Alejandro Henao Ossa.
Ingeniero industrial, químico industrial, especialista en SST

Resumen

El presente artículo analiza en profundidad la gestión de los peligros químicos en el entorno industrial, evaluando la relación intrínseca entre las propiedades fisicoquímicas de los componentes activos y sus efectos fisiopatológicos en el cuerpo humano. A través de un enfoque técnico-científico, se examinan los mecanismos de toxicocinética y toxicodinamia que desencadenan patologías de origen ocupacional. Finalmente, se delimitan las responsabilidades legales y los compromisos estratégicos del área de Seguridad y Salud en el Trabajo (SST) para la implementación de barreras de control efectivas basadas en la jerarquía del riesgo, asegurando la sostenibilidad operativa y la protección de la vida humana, desde la gestión real y mi experiencia en prevención, seguridad química, conversaciones con higiene industrial, procesos, formación y hechos reales que me llevan a dejar este mensaje a muchos lectores para generar cambio consciente en como estamos asumiendo este peligro en las organizaciones.

1. Introducción y Delimitación del Peligro Químico

El desarrollo industrial contemporáneo está intrínsecamente ligado al uso de una vasta diversidad de compuestos sintéticos y naturales. Sin embargo, la manipulación de estas sustancias introduce en el ambiente laboral el denominado peligro químico, definido como la capacidad inherente de una sustancia (o mezcla de ellas) para generar efectos adversos, daños materiales o alteraciones ambientales debido a sus propiedades intrínsecas.

Para comprender el peligro químico desde una perspectiva técnica, es imperativo diferenciar entre la peligrosidad de la sustancia y el riesgo asociado. La peligrosidad es una propiedad estática e inalterable del componente activo, determinada por su estructura molecular, su reactividad, su volatilidad y su capacidad de interactuar con matrices biológicas. En contraste, el riesgo es una variable dinámica que resulta de la probabilidad de que ocurra la exposición y de la severidad del daño consecuente.

La clasificación internacional de estos peligros se rige actualmente por el Sistema Globalmente Armonizado (SGA), el cual categoriza las sustancias en peligros físicos (como la inflamabilidad, piroforicidad, inestabilidad explosiva o capacidad comburente), peligros para la salud (toxicidad aguda, carcinogenicidad, mutagenicidad, teratogenicidad y corrosión cutánea) y peligros para el medio ambiente. El análisis predictivo de estos peligros dentro de una organización constituye la piedra angular de cualquier sistema de gestión de la seguridad industrial.

2. Análisis Dinámico de los Riesgos Asociados

La presencia de una sustancia peligrosa en el nodo productivo desencadena una matriz de riesgos multifactoriales que pueden clasificarse en tres grandes vertientes operacionales: riesgos higiénicos, riesgos de seguridad (accidentabilidad) y riesgos reactivos.

Los riesgos higiénicos están vinculados a la exposición crónica o aguda a concentraciones ambientales de contaminantes químicos. Estos riesgos dependen directamente de variables ambientales como la tasa de ventilación, la temperatura del proceso —que puede incrementar la presión de vapor y, por ende, la tasa de evaporación— y la sinergia entre diferentes compuestos presentes en el mismo ecosistema laboral. La cuantificación de estos riesgos requiere de metodologías de muestreo higiénico validadas por organismos de referencia como NIOSH u OSHA, contrastando los resultados con los Valores Límite Permisibles o Threshold Limit Values (TLV).

Por otra parte, los riesgos de seguridad química involucran eventos disruptivos súbitos. Las atmósferas explosivas (ATEX), originadas por la acumulación de gases, vapores o polvos combustibles en concentraciones comprendidas entre sus límites inferior y superior de inflamabilidad (LII/LSI), representan uno de los mayores desafíos en la ingeniería de procesos. Asimismo, el riesgo de reacciones exotérmicas descontroladas por incompatibilidad química durante el almacenamiento o el transporte puede derivar en incendios a gran escala, liberaciones masivas de nubes tóxicas o fallas estructurales por sobrepresión en reactores y contenedores.

3. Interacción del Componente Activo con el Cuerpo Humano y la Salud

Para determinar el impacto real de las sustancias químicas en la salud ocupacional, es fundamental estudiar la relación entre el componente activo (la entidad química responsable de la acción biológica) y los sistemas fisiológicos del trabajador. Este fenómeno se desglosa en dos fases críticas: la toxicocinética y la toxicodinamia.

3.1 Vías de Ingreso y Toxicocinética

La toxicocinética describe el tránsito de la sustancia a través del organismo mediante el modelo ADME: Absorción, Distribución, Metabolismo y Excreción. Las principales vías de ingreso ocupacional son:

Vía Inhalatoria: Es la ruta de mayor relevancia epidemiológica en la industria. Los gases, vapores y el material particulado (fracciones respirable, torácica e inhalable) acceden directamente al árbol traqueobronquial y a los alvéolos. La permeabilidad de la membrana alvéolo-capilar permite que los componentes activos hidrosolubles o liposolubles ingresen al torrente sanguíneo de forma casi instantánea, evitando el efecto de primer paso hepático.

Vía Dérmica: Sustancias con un alto coeficiente de partición octanol-agua (Log Kow) poseen la capacidad de disolverse en los lípidos del estrato córneo de la piel, penetrando hacia la dermis y los capilares subyacentes. Compuestos como los solventes aromáticos y los pesticidas organofosforados aprovechan esta vía, causando a menudo toxicidad sistémica sin necesariamente generar una lesión visible en la piel.

Vía Digestiva y Parenteral: Generalmente accidentales u originadas por malas prácticas de higiene celular (comer o fumar con las manos contaminadas). Aunque menos comunes en procesos estables, representan un riesgo crítico en laboratorios y actividades de mantenimiento.

Una vez absorbido, el componente activo se distribuye a través del plasma hacia los órganos diana. El hígado, mediante el sistema enzimático del Citocromo P450, intenta bio-transformar la sustancia para facilitar su excreción (principalmente renal o biliar). No obstante, en ocasiones este proceso metabólico genera "activación metabólica", transformando un xenobiótico relativamente inocuo en un metabolito altamente reactivo y electrofílico.

3.2 Toxicodinamia y Efectos Fisiopatológicos

La toxicodinamia estudia el mecanismo de acción molecular del componente activo en el receptor biológico. Los efectos sobre la salud se manifiestan en diferentes niveles de organización biológica:

Al nivel de la **toxicidad celular y molecular**, los componentes activos interactúan con macromoléculas celulares. Por ejemplo, los metales pesados como el plomo (saturnismo) o el cadmio se unen a los grupos sulfhidrilo de enzimas esenciales, inhibiendo la síntesis del grupo hemo o alterando la homeostasis mitocondrial, lo que induce estrés oxidativo severo y apoptosis celular. Por su parte, los solventes halogenados alteran la fluidez de las membranas celulares en el sistema nervioso central, comportándose como depresores anestésicos.



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

En lo que respecta a la **toxicidad sistémica y de órganos diana**, se observan efectos específicos como la hepatotoxicidad, donde la exposición a compuestos como el tetracloruro de carbono produce esteatosis hepática y necrosis centrolobulillar debido a la formación de radicales libres de cloro. La nefrotoxicidad se manifiesta cuando los riñones, al concentrar las toxinas en los túbulos renales para su excreción, sufren necrosis tubular aguda (común en la exposición a glicoles y metales).

Finalmente, la **neumoconiosis y patologías respiratorias** son causadas por la acumulación de polvos inorgánicos como la sílice cristalina o el asbesto en el parénquima pulmonar. Esto desencadena una respuesta macrófaga persistente que culmina en fibrosis pulmonar progresiva e irreversible, disminuyendo drásticamente la capacidad de difusión de oxígeno.

A largo plazo, los efectos más devastadores corresponden a la **carcinogénesis, mutagénesis y toxicidad reproductiva**. Sustancias calificadas como cancerígenas del Grupo 1 por la IARC (como el benceno o el cromo hexavalente) actúan como agentes alquilantes del ADN. Estos compuestos inducen mutaciones puntuales o aberraciones cromosómicas que desregulan los protooncogenes y los genes supresores de tumores, dando origen a leucemias linfoides o carcinomas bronco génicos tras períodos de latencia que pueden oscilar entre los 10 y los 30 años.

4. Responsabilidades Legales y Compromisos desde la Seguridad y Salud en el Trabajo (SST)

La gestión del riesgo químico no puede limitarse a una respuesta reactiva ante la enfermedad o el accidente; exige una estructura de gobernanza corporativa y el estricto cumplimiento de marcos normativos locales e internacionales. Las responsabilidades y compromisos del área de SST se articulan en tres dimensiones fundamentales.

4.1 Caracterización y Evaluación Rigurosa del Riesgo

El primer compromiso ineludible del profesional en SST es mantener un inventario de sustancias químicas actualizado al 100%, indexado con sus respectivas Fichas de Datos de Seguridad (FDS) conformes al SGA de 16 secciones. Queda estrictamente prohibido el uso de sustancias sin trazabilidad de origen.

La evaluación del riesgo debe ser cuantitativa en aquellos puestos donde la modelación matemática o el histórico sospechen una cercanía al 50% del TLV (Nivel de Acción). Esto implica diseñar campañas de monitoreo higiénico personal que capturen la variabilidad de la jornada laboral, considerando factores de corrección por jornadas extendidas (modelos de Brief y Scala).

4.2 Aplicación de la Jerarquía de Controles de Ingeniería y Procesos

El diseño ambiental y operacional bajo la estricta observancia de la jerarquía de controles representa la mayor responsabilidad técnica del gestor de SST:

[Eliminación] ---> Suprimir el uso de la sustancia peligrosa del proceso.

|

[Sustitución] ---> Cambiar por un componente activo de menor toxicidad o volatilidad.

|

[C. Ingeniería] --> Implementar sistemas de ventilación por extracción localizada (VEL),
| aislamiento de procesos o automatización robótica.

|

[C. Administrativos] Reducir tiempos de exposición, rotación de personal, señalización
| y programas continuos de capacitación especializada.

|

[EPP Específico] -> Filtros de carbón activado, trajes de Tychem, protección ocular
estanca frente a salpicaduras y guantes con barrera de permeación ensayada.

Es un error conceptual y una falta a la ética profesional priorizar el Uso de Equipos de Protección Personal (EPP) como primera línea de defensa. El EPP es la barrera más vulnerable y depende enteramente del factor humano; por ende, los controles colectivos e ingenieriles en la fuente y en el medio deben anteponerse sistemáticamente.

4.3 Vigilancia Epidemiológica y Control Médico Laboral

El área de SST debe consolidar un programa de Vigilancia Epidemiológica Específico para Riesgo Químico. Esto incluye la realización de exámenes médicos ocupacionales orientados al órgano diana de la sustancia manipulada (por ejemplo, espirometrías seriadas para trabajadores expuestos a alérgenos respiratorios, o perfiles hepáticos y renales para operadores de plantas de beneficio con solventes).



ESTATAL
DE SEGURIDAD

¿TODAVÍA NO TIENE **VERDADERA PROTECCION?**

Profesionales competentes + Tecnología + Datos
para operar al ritmo de tu negocio.

TECNOLOGÍA

Cámaras con analítica • Controles de
acceso • Alarmas e intrusión

CONSULTORÍA EN SEGURIDAD

Consultoría en riesgos corporativos •
Pruebas de confiabilidad • Poligrafía

VIGILANCIA HUMANA

Vigilantes • Escoltas • Caninos

Conoce nuestro portafolio completo en
www.estataldeseguridad.com para que puedas tener una
VERDADERA PROTECCIÓN.

Asimismo, se deben implementar Indicadores de Exposición Biológica (BEI) como control de tercera línea. La medición de metabolitos en matrices biológicas (ácido mucónico en orina para benceno, plomo en sangre total, o actividad de la colinesterasa eritrocitaria para organofosforados) permite detectar la absorción interna de la sustancia antes de que se manifieste una alteración fisiológica clínica, sirviendo como el predictor más temprano de la eficacia de los controles ambientales implantados.

5. Conclusiones

La gestión del peligro químico en la industria moderna no permite empirismos. La comprensión profunda de la naturaleza íntima del componente activo y sus rutas metabólicas dentro del cuerpo humano es la única herramienta válida que posee el profesional de Seguridad y Salud en el Trabajo para diseñar entornos de trabajo verdaderamente resilientes y seguros.

Las responsabilidades en SST trascienden el mero cumplimiento documental; se insertan en la bioética industrial y en la optimización de los procesos de manufactura. Solo mediante la inversión en controles de ingeniería de alta eficiencia, un monitoreo higiénico con rigor estadístico y un programa de vigilancia médica proactivo, se podrá garantizar que el progreso tecnológico y económico de las organizaciones no se traduzca en el detrimento de la salud y la integridad de la fuerza laboral.

Profundización Normativa y Responsabilidades desde la SST

La gestión técnica del TDI debe estar rígidamente alineada con la legislación nacional e internacional vigentes. El incumplimiento de estos parámetros expone a las organizaciones a severas sanciones administrativas, demandas civiles por culpa patronal y, fundamentalmente, al deterioro de la salud de su capital humano.

4.1 Estándares Internacionales de Referencia (OSHA / ACGIH)

A nivel internacional, la Administración de Seguridad y Salud Ocupacional de EE. UU. (OSHA) establece un Límite de Exposición Permisible (PEL) que históricamente se ha considerado alto frente a los criterios científicos modernos. Por ello, la Conferencia Americana de Higienistas Industriales Gubernamentales (ACGIH) actualiza periódicamente los Valores Límite Permisibles (TLV), los cuales sirven de base técnica global:

- TLV-TWA (Media ponderada en el tiempo para 8 horas): $\backslash(0.001\text{ ppm})\backslash \backslash(0.007\text{ mg/m}^3\backslash)$ en su fracción inhalable y vapor.
- TLV-STEL (Límite de exposición a corto plazo para 15 minutos): $\backslash(0.005\text{ ppm})\backslash \backslash(0.035\text{ mg/m}^3\backslash)$.
- Anotaciones: Clasificado como SEN (Sensibilizante respiratorio y cutáneo) y Skin (indica peligro de absorción significativa a través de la piel).

4.2 Marco Normativo en Colombia e Implementación Industrial

Colombia posee una de las legislaciones más robustas de la región en materia de riesgo químico, la cual obliga a las empresas del sector plásticos a cumplir con las siguientes disposiciones en relación con el TDI:

A. Adopción de Límites Permisibles (Resolución 2400 de 1979)

El Estatuto de Seguridad Industrial en su Artículo 154 determina que, en ausencia de límites fijados explícitamente por el Ministerio del Trabajo, se adoptarán de forma obligatoria los **TLVs de la ACGIH vigentes**. Por lo tanto, cualquier empresa en Colombia que manipule TDI debe diseñar sus sistemas de ventilación para asegurar que ningún trabajador esté expuesto a más de $\backslash(0.001\text{ ppm})\backslash$ en su jornada diaria.

B. Sistema Globalmente Armonizado (Decreto 1496 de 2018)

Este decreto reglamenta la obligatoriedad de implementar el SGA en el territorio nacional para la clasificación y etiquetado de productos químicos puros y mezclas. El departamento de SST tiene la responsabilidad legal de:

- Garantizar que todas las estaciones de inyección de poliuretano tengan las Etiquetas SGA legibles con los pictogramas de "Toxicidad Aguda" (Calavera) y "Peligro para la Salud" (Silueta humana con estrella).
- Garantizar el acceso inmediato a las Fichas de Datos de Seguridad (FDS) en idioma castellano y estructuradas según las 16 secciones del SGA.

C. Sistema de Gestión de SST (Decreto 1072 de 2015 y Resolución 0312 de 2019)

Bajo los Estándares Mínimos de la Resolución 0312 y los requisitos del Capítulo 6 del Decreto 1072, la empresa debe evidenciar la ejecución de un Programa de Vigilancia Epidemiológica Ocupacional (PVEO) específico para riesgo químico. Los componentes críticos auditables son:

EL NUEVO ROSTRO DE LA DELINCUENCIA.

¿Tu empresa está preparada para
las **amenazas de hoy?**

Hoy una amenaza puede comenzar
con un correo fraudulento, una llamada
falsa o una filtración de información.
Anticiparse ya no es una opción:
es una necesidad.

LAS AMENAZAS EVOLUCIONAN.
LA PREVENCIÓN
TAMBIÉN.



DESDE 1971
SIEMPRE PRESENTES

PROTEGEMOS LO QUE IMPULSA **TU EMPRESA**

Diseñamos ecosistemas de seguridad que integran
talento humano, tecnología e inteligencia para proteger
la continuidad de tu operación.



VIGILANCIA
FÍSICA



MONITOREO
INTELIGENTE
24/7



SEGURIDAD
ELECTRÓNICA



GESTIÓN INTEGRAL
DEL RIESGO



Agenda un diagnóstico de
seguridad para tu empresa.

☑ 310 257 0799

☑ gerenciacomercial@seguridaddecolombia.com

☑ www.seguridaddecolombia.com

1. Evaluación de la Exposición: Realización anual (o semestral si se supera el nivel de acción de 0.0005 ppm) de mediciones higiénicas por personal con Licencia vigente en SST.

2. Controles de Ingeniería Obligatorios: El área de mezcla y curado de poliuretano debe disponer de un sistema de Ventilación por Extracción Localizada (VEL) diseñado según los manuales de la ACGIH (Industrial Ventilation Manual), capturando los vapores de TDI en la fuente antes de que ingresen a la zona respiratoria del trabajador. El aire extraído debe pasar por torres de lavado químico o lechos de carbón activado específicos para isocianatos antes de ser emitido a la atmósfera exterior.

3. Vigilancia Médica Específica: Los exámenes médicos de ingreso y periódicos deben incluir de forma mandatoria:

- Cuestionarios específicos de síntomas respiratorios (ej. Escala del Medical Research Council).
- Espirometría simple con prueba de broncodilatación (para descartar hiperreactividad bronquial preexistente). Está legalmente contraindicado ubicar a un trabajador con antecedentes asmáticos o atópicos severos en puestos con manipulación de TDI.

4. Monitoreo Biológico (BEI): Se adopta el control biológico mediante la cuantificación de la Toluendiamina (TDA) en orina, recolectada estrictamente al final del turno de trabajo. El límite biológico de exposición establecido por la ACGIH es de $5 \mu\text{g/g}$ de creatinina. Un resultado por encima de este valor es un indicador legal de falla en los controles ingenieriles o en el uso del EPP, obligando al retiro temporal del trabajador del área.

5. Conclusiones

La gestión del peligro químico en la industria moderna no permite empirismos. La comprensión profunda de la naturaleza íntima del componente activo y sus rutas metabólicas dentro del cuerpo humano es la única herramienta válida que posee el profesional de Seguridad y Salud en el Trabajo para diseñar entornos de trabajo verdaderamente resilientes y seguros.

Las responsabilidades en SST trascienden el mero cumplimiento documental; se insertan en la bioética industrial y en la optimización de los procesos de manufactura. Solo mediante la inversión en controles de ingeniería de alta eficiencia, un monitoreo higiénico con rigor estadístico y un programa de vigilancia médica proactivo, se podrá garantizar que el progreso tecnológico y económico de las organizaciones no se traduzca en el detrimento de la salud y la integridad de la fuerza laboral.





¡CUIDADO!

¿Sabe cómo **prevenir** ser víctima del *paseo millonario*?

1

Preferiblemente, solicite su servicio de transporte a través de aplicaciones reguladas por las autoridades.



2

Tome fotografías del vehículo en las que se observe la placa, comparta su ubicación en tiempo real e informe a alguien de confianza sobre su destino y la ruta que tomará.



3

Observe su entorno y el camino que toma el vehículo. Si nota que se desvía de la ruta habitual, pídale al conductor que lo deje en un lugar público y busque ayuda.



4

Evite establecer conversaciones sobre triunfos financieros frente a personas desconocidas.



5

Controle el consumo de bebidas alcohólicas y evite dormir durante el recorrido.



Su seguridad es lo primero. No se convierta en víctima del paseo millonario

YO NO PAGO DENUNCIO
GAULA POLICÍA NACIONAL



Unidos contra la
Extorsión
y el secuestro





Dios y Patria



ESMERALDA

Estrategia integral contra el narcotráfico

Dirección de Antinarcótics



Todos unidos

contra el sistema de drogas ilícitas





ESMERALDA

Estrategia integral contra el narcotráfico

Dirección de Antinarcóticos

Denunciar el narcotráfico paga. Línea nacional Antidrogas



**Absoluta
Reserva**

**Línea Whatsapp
312 5300000**

