

Revista **EL MUNDO CAMBIÓ**

EDICIÓN 31
2026



BOGOTÁ SE CONVIERTE EN EL EPICENTRO
latinoamericano de la innovación en seguridad
con la Feria Internacional ESS+ 2026
Feria Internacional de Seguridad



31 julio de 2026



Revista El Mundo Cambio

BOGOTÁ SE CONVIERTE EN EL EPICENTRO LATINOAMERICANO DE LA INNOVACIÓN EN SEGURIDAD CON LA FERIA INTERNACIONAL ESS+ 2026

Feria Internacional de Seguridad



10

LA SEGURIDAD INTEGRAL Y LAS REDES SOCIALES EN COLOMBIA: CUANDO EL PROFESIONAL SE VUELVE VIRAL POR SUS PROPIOS ERRORES.

Dixon Ruiz



15

CUANDO YA NO HAY UN CENTRO QUE ATACAR LO QUE LAS REDES EN MALLA PUEDEN ENSEÑARLE A LA SEGURIDAD DE UNA EMPRESA

Carlos Eduardo Valenzuela Oviedo



22

21 KILÓMETROS CUANDO CORRER TAMBIÉN ES APRENDER A GESTIONAR EL RIESGO

Yinna Marcela Gutiérrez Orjuela



27

INCENDIOS DE AUTOS ELÉCTRICOS: EL RIESGO INVISIBLE ESTÁ EN EL HUMO

Hernán Javier Domínguez



32

INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y GEOPOLÍTICA: UNA CONVERGENCIA ESTRATÉGICA INEVITABLE

Ing. Erick Sarante



38

LA SEGURIDAD CORPORATIVA COMIENZA ANTES DE LA CRISIS - LO QUE TODA EMPRESA DEBE TENER BAJO CONTROL.

Eduardo E. Hurtado - MBA, CPP.



41

SIN RECURSOS PARA FORTALECER LAS FF AA.

Hugo Acero Velásquez



46

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

Ofertas de hasta 48% Dto. en Tablets



Tab A11 | A11+



Tab S10 Lite



BARRANQUILLA

CC Buenavista 1
Piso 2 Local 219
CC Villa Country
Piso 11a, zona Común
Pasillo Central
CC Portal del Prado
1a Área común 16
Viva Centro Comercial
1a 202
CC Parque Alegre
Piso 11a 1-118A
SOLEDAD
CC Plaza del Sol
Local 267 - 268

BOGOTÁ

CC Plaza de las Américas
Local 176
CC Gran Estación
1a 1-103
CC Gran Estación
1a diagonal a101

CALI

CC Llanogrande
Palmira, Valle
Burbuja 702 frente a
San Viejo de Caldas
CC Unico 1
Burbuja 835

CARTAGENA

CC Mall Plaza el Castillo
Local 103 - 101 piso 1
CC Mall Plaza el Castillo
1a
CC Plaza Bocagrande
Piso 1a 1-52
TURBACO
CC Plaza 90
1a 10

SANTA MARTA

CC Ocean Mall
2º piso local 51 y 52
CC Buena Vista
1a 137

VALLEDUPAR

CC Mayales Plaza
Local 256 e 1a 16
CC Guatapuri
1º piso al lado de la
plazoleta de Juan Valdez



Revista

EL MUNDO CAMBIÓ

Editorial:



Vivimos un momento en el que la seguridad atraviesa una transformación sin precedentes. Las amenazas ya no responden únicamente a modelos tradicionales: hoy convergen el crimen organizado, la inteligencia artificial, la ciberseguridad, la protección de infraestructuras críticas, la desinformación, los riesgos tecnológicos y los desafíos asociados al liderazgo y la resiliencia organizacional. En este contexto, proteger personas, organizaciones y Estados exige una visión más amplia, donde la innovación, el análisis estratégico y la capacidad de anticipación se convierten en factores determinantes.

Abrimos esta edición con "**Bogotá se convierte en el epicentro latinoamericano de la innovación en seguridad con la Feria Internacional ESS+ 2026**", un recorrido por el evento que reunirá en la capital colombiana a líderes, autoridades, empresas y expertos internacionales para analizar las tecnologías, tendencias y estrategias que están redefiniendo la seguridad en América Latina. La ESS+ consolida un espacio donde convergen la inteligencia artificial, la protección de infraestructuras críticas, las ciudades inteligentes y la cooperación público-privada como pilares del futuro de la seguridad.

Continuamos con "La seguridad integral y las redes sociales en Colombia: cuando el profesional se vuelve viral por sus propios errores", de **Dixon Ruiz**, quien reflexiona sobre el impacto que las redes sociales tienen hoy en la reputación y la credibilidad de los profesionales de la seguridad. El autor analiza cómo una publicación imprudente puede comprometer operaciones, afectar organizaciones y convertir la exposición digital en un riesgo estratégico que exige ética, criterio y responsabilidad.

Desde una perspectiva innovadora, **Carlos Eduardo Valenzuela Oviedo** presenta "Cuando ya no hay un centro que atacar: lo que las redes en malla pueden enseñarle a la seguridad de una empresa", una propuesta que replantea los modelos tradicionales de protección organizacional. A partir del concepto de redes distribuidas, el autor demuestra cómo la resiliencia, la descentralización del conocimiento y la circulación oportuna de la información fortalecen la capacidad de las empresas para enfrentar amenazas cada vez más complejas.

La gestión del riesgo adquiere una dimensión profundamente humana en "21 kilómetros: cuando correr también es aprender a gestionar el riesgo", de **Yinna Marcela Gutiérrez Orjuela**, quien establece un interesante paralelismo entre la preparación para una media maratón y la planificación de la seguridad física. Su experiencia demuestra que la anticipación, la disciplina, la resiliencia y la toma de decisiones oportunas son principios comunes tanto en el deporte como en la gestión profesional del riesgo.

La innovación tecnológica también plantea nuevos desafíos para la respuesta a emergencias. En "Incendios de autos eléctricos: el riesgo invisible está en el humo", **Hernán Javier Domínguez** analiza la evidencia científica sobre los riesgos asociados a la fuga térmica en vehículos eléctricos, resaltando la importancia de comprender los peligros que representan los gases tóxicos para brigadas, bomberos y primeros respondientes, así como la necesidad de actualizar protocolos y planes de emergencia.

La dimensión estratégica del nuevo entorno internacional es abordada por el **Ing. Erick Sarante**, quien en "Inteligencia artificial, ciberseguridad y geopolítica: una convergencia estratégica inevitable" explica cómo estas tres disciplinas han dejado de actuar por separado para convertirse en factores determinantes del poder de los Estados. Su análisis invita a reflexionar sobre la soberanía digital, la resiliencia tecnológica y el papel de la innovación en la seguridad nacional y corporativa.

En "La seguridad corporativa comienza antes de la crisis: lo que toda empresa debe tener bajo control", **Eduardo E. Hurtado – MBA, CPP** expone cómo la seguridad moderna debe integrarse a la estrategia empresarial mediante procesos de gobernanza, gestión del riesgo, cumplimiento, continuidad del negocio y liderazgo preventivo. El autor plantea que una organización verdaderamente resiliente se construye mucho antes de enfrentar una contingencia.

Finalmente, cerramos esta edición con "Sin recursos para fortalecer las FF. AA.", de **Hugo Acero Velásquez**, quien analiza los desafíos presupuestales que enfrenta Colombia para modernizar su Fuerza Pública frente a las nuevas dinámicas del crimen organizado. Su reflexión pone sobre la mesa la necesidad de orientar estratégicamente las inversiones en capacidades tecnológicas, inteligencia, drones y sistemas de defensa acordes con las amenazas del presente.

PROFESIONAL DE LA SEMANA

Oscar Mauricio Barreto Rodríguez es un profesional con una amplia trayectoria en seguridad corporativa, gestión del riesgo e investigación criminal, respaldada por una sólida formación académica como Administrador de Empresas, Administrador Policial y especialista en Derecho Informático y en Gestión de la Seguridad y Salud en el Trabajo (HSE). Su perfil se fortalece con certificaciones nacionales e internacionales en consultoría de seguridad, BASC, OEA, SARLAFT, continuidad del negocio y sistemas de gestión, consolidándolo como un referente en la protección integral de organizaciones y activos estratégicos.

Actualmente se desempeña como Gerente de Seguridad para los Países Andinos, Centroamérica y el Caribe en Hitachi Energy, donde lidera estrategias regionales orientadas a la gestión de riesgos, continuidad del negocio, protección de ejecutivos, seguridad física, manejo de crisis e investigaciones corporativas. Su experiencia también incluye una destacada carrera en la Policía Nacional de Colombia, desempeñando funciones de liderazgo en investigación criminal, inteligencia y lucha contra el crimen organizado, aportando una visión integral que combina la experiencia operativa con la estrategia empresarial.

A lo largo de su carrera ha impulsado modelos de seguridad basados en la prevención, la innovación y el cumplimiento de estándares internacionales, promoviendo una cultura organizacional enfocada en la resiliencia, la protección de las personas y la continuidad de las operaciones. Su capacidad para integrar tecnología, inteligencia y liderazgo lo convierte en un profesional altamente reconocido en el ámbito de la seguridad corporativa y la gestión estratégica del riesgo.



Oscar Mauricio
Barreto
Rodríguez





PREMIOS A LA EXCELENCIA

NO TODOS RECIBEN UN RECONOCIMIENTO.
LOS QUE TRASCIENDEN, SÍ.

Conoce las categorías y participa en el reconocimiento que **destaca a los líderes, empresas y profesionales** que están transformando la seguridad y la gestión de riesgos.

28
AGOSTO

BOGOTÁ
¡Postúlate y lleva tu
trayectoria al siguiente nivel!

administracion@revistaelmundocambio.com



+57 3007317523

Organiza:



UNIVERSIDAD MILITAR
NUEVA GRANADA



Bogotá
Chapter



Un espacio donde
la experiencia se convierte en

conocimiento



La Revista **El Mundo Cambió**, junto con aliados estratégicos, reúne a líderes del sector público, privado y académico para impulsar la innovación, **fortalecer la cooperación y construir el futuro de la seguridad.**

INSCRÍBETE

En el marco de la Feria
Internacional de Seguridad ESS+



27, 28 de Agosto | Bogotá

Aula máxima - Universidad
Militar Nueva Granada -
sede calle 100



Patrocinadores



REAL TIME SECURITY



Bogotá se convierte en el epicentro latinoamericano

de la innovación en seguridad con la Feria Internacional ESS+ 2026

La alianza entre el sector público y privado impulsará una agenda sin precedentes sobre inteligencia artificial, ciudades seguras, infraestructura crítica y las tecnologías que están transformando la seguridad en América Latina.

Bogotá, Colombia. Del 26 al 28 de agosto de 2026, Corferias será el escenario de la Feria Internacional de Seguridad ESS+, el encuentro especializado más importante de América Latina para la industria de la seguridad integral, que reunirá a autoridades gubernamentales, organismos internacionales, fuerzas de seguridad, empresas líderes, expertos y tomadores de decisión de toda la región para analizar los desafíos y las soluciones que definirán el futuro de la seguridad.

En su edición 2026, ESS+ consolida una alianza estratégica entre el sector público y el sector privado, con la participación de la Secretaría Distrital de Seguridad, Convivencia y Justicia de Bogotá y la Policía Nacional de Colombia, quienes presentarán los avances más relevantes en materia de seguridad ciudadana, inteligencia artificial, analítica de datos, videovigilancia inteligente, centros de comando y control, interoperabilidad tecnológica y modelos de prevención orientados a construir ciudades más seguras, eficientes y resilientes.

Bogotá: un laboratorio de innovación para las ciudades del futuro

La capital colombiana será presentada como un caso de estudio para América Latina, mostrando cómo una ciudad en permanente crecimiento afronta los retos de la seguridad mientras desarrolla algunos de los proyectos de infraestructura urbana más importantes de su historia, entre ellos la construcción de la Primera Línea del Metro de Bogotá.

Los asistentes conocerán las estrategias implementadas para proteger obras de infraestructura crítica, fortalecer la vigilancia ciudadana mediante tecnologías inteligentes, integrar plataformas de monitoreo y optimizar la capacidad de respuesta de las autoridades a través de herramientas basadas en inteligencia artificial.

La experiencia de Bogotá permitirá compartir aprendizajes sobre la manera en que la innovación tecnológica puede acompañar el desarrollo urbano, proteger a los ciudadanos y fortalecer la convivencia.



Foro Internacional de Infraestructuras Críticas

Uno de los espacios académicos de mayor relevancia será el Foro Internacional de Infraestructuras Críticas, donde expertos nacionales e internacionales analizarán la protección de activos estratégicos indispensables para la estabilidad económica y social.

El foro tendrá un énfasis especial en la seguridad de:

- Puertos marítimos y fluviales.
- Terminales logísticas.
- Infraestructura de transporte.
- Corredores estratégicos.
- Sistemas urbanos de movilidad.
- Servicios esenciales para las ciudades.

La agenda abordará los nuevos riesgos derivados del crimen organizado, el terrorismo, las amenazas híbridas, los ataques cibernéticos y la necesidad de integrar tecnologías inteligentes para garantizar la continuidad operativa de estas infraestructuras fundamentales para el desarrollo de la región.

Ciudades Seguras: innovación para proteger a los ciudadanos

La ESS+ desarrollará un gran Foro Internacional de Ciudades Seguras, donde gobiernos, empresas tecnológicas, operadores urbanos y organismos especializados compartirán experiencias sobre:

- Inteligencia Artificial aplicada a la seguridad ciudadana.
- Analítica predictiva para la prevención del delito.
- Videovigilancia inteligente.
- Plataformas unificadas de comando y control.
- Automatización de procesos de seguridad.
- Gestión de emergencias.
- Integración de datos para la toma de decisiones.
- Protección de espacios públicos mediante tecnologías inteligentes.

Este espacio permitirá conocer casos reales de transformación digital implementados en diferentes ciudades de América Latina y promoverá el intercambio de buenas prácticas entre autoridades y empresas especializadas.



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

ALAS reconocerá la innovación latinoamericana

Como parte de la programación internacional, la Asociación Latinoamericana de Seguridad (ALAS) realizará la entrega de los Premios ALAS, reconocimiento que destaca los proyectos más innovadores de América Latina en implementación tecnológica para la seguridad.

Los premios exaltan iniciativas que han logrado generar impactos medibles en protección de infraestructura, seguridad ciudadana, transformación digital, automatización, monitoreo inteligente y desarrollo de soluciones innovadoras que fortalecen la protección de personas, organizaciones y territorios.

Tecnología en operación: la innovación funcionando en tiempo real

Más de 300 empresas nacionales e internacionales presentarán durante los tres días del evento las tecnologías que hoy están transformando la industria de la seguridad en América Latina.

Los visitantes podrán conocer soluciones operando en tiempo real en áreas como:

- Inteligencia Artificial.
- Analítica avanzada de video.
- Videovigilancia inteligente.
- Ciberseguridad.
- Control de accesos.
- Automatización.
- Drones y sistemas autónomos.
- Seguridad electrónica.
- Protección contra incendios.
- Seguridad industrial.
- Gestión de riesgos.
- Integración de plataformas.
- Monitoreo remoto.
- Seguridad para ciudades inteligentes.

La feria ofrecerá demostraciones en vivo, lanzamientos tecnológicos, casos de éxito y espacios de relacionamiento comercial que permitirán conocer de primera mano las innovaciones que marcarán la evolución del sector en los próximos años.

América Latina se reúne en Bogotá

La ESS+ recibirá delegaciones oficiales, empresarios, distribuidores, integradores, organismos públicos y compradores provenientes de Centroamérica, Suramérica y el Caribe, consolidándose como la principal plataforma regional para el intercambio de conocimiento, el desarrollo de negocios y la cooperación internacional.

La presencia de representantes de múltiples países fortalecerá el diálogo regional sobre los desafíos comunes en materia de seguridad, protección de infraestructuras críticas, transformación digital y construcción de ciudades más inteligentes, resilientes y sostenibles.

Un escenario para construir el futuro de la seguridad. 300 expositores, 27 países representados, 17.000 visitantes profesionales, 15.000 m² de exhibición y La Feria Internacional de Seguridad ESS+ 2026 reafirma su liderazgo como el principal punto de encuentro para quienes diseñan, implementan y lideran las estrategias de seguridad en América Latina.

Durante tres días, gobiernos, fuerzas de seguridad, empresas tecnológicas, operadores de infraestructura crítica, industria, academia y organizaciones internacionales compartirán una visión común: impulsar la innovación, fortalecer la cooperación público-privada y acelerar la adopción de tecnologías que permitan anticipar riesgos, proteger los activos estratégicos y construir ciudades más seguras para los ciudadanos.

La ESS+ será el espacio donde la tecnología deja de ser una promesa para convertirse en soluciones reales





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



LA SEGURIDAD INTEGRAL Y LAS REDES SOCIALES EN COLOMBIA:

CUANDO EL PROFESIONAL SE VUELVE VIRAL POR SUS PROPIOS ERRORES.

Dicxon Ruiz

"Un uniforme de Seguridad no es un disfraz para ganar aplausos en las pantallas, ni la calle un escenario para egos digitales; el respeto se gana con disciplina y doctrina, no con quince segundos de fama que terminan enterrando la dignidad de toda una profesión."

El tribunal invisible de la opinión pública en la seguridad integral

Cuando no existe un liderazgo firme que forme, guíe y marque la pauta pedagógica dentro de las instituciones y empresas, el profesional de la seguridad queda a la deriva. Sin una orientación clara fundamentada en el honor, la disciplina y la responsabilidad inherentes a su rol, el personal termina actuando a ciegas o buscando validación en plataformas digitales, publicando contenidos que destruyen la credibilidad de todo el gremio. En este artículo analizaremos las causas y consecuencias de la ausencia de liderazgo en las organizaciones de seguridad integral; un problema que abarca a gran parte de nuestro continente, pero en el cual nos centraremos en el hermano país, Colombia, por ser uno de los escenarios donde con mayor claridad se refleja esta problemática a través de las redes sociales.

Antes, los errores operativos, las faltas de criterio o las desavenencias de un miembro de la fuerza pública o de un operador de seguridad privada se quedaban en el parte diario de novedades, en el informe de turno o en la discreción de la unidad. Hoy, las reglas del juego cambiaron drásticamente: la sociedad entera está hiperconectada, provista de cámaras en alta definición listas para registrar cualquier tropiezo. Lo más grave de este fenómeno no es el acecho externo, sino que los propios profesionales, por falta de orientación de sus superiores, se han convertido en sus peores verdugos al exponerse en redes sociales y minar la credibilidad institucional ante los ojos del mundo. Comprender esta realidad es el primer paso para solucionarla: se vuelve urgente que los líderes de las instituciones y empresas asuman la responsabilidad de capacitar, formar, orientar y guiar a su personal, enseñándoles el impacto global de sus actos y el comportamiento ético que deben mantener, tanto en las calles como en el entorno digital.

El autogol de la imprudencia y los casos reales que dañan la reputación de nuestra imagen

Para cualquier líder de la seguridad con visión internacional, resulta profundamente indignante y doloroso ser testigo de la pérdida de mística, disciplina y respeto por el servicio. Al realizar un recorrido por las redes sociales enfocándonos en Colombia, queda al descubierto cómo personal de seguridad ejecuta actos que atentan directamente contra el decoro y la dignidad que exige el porte del uniforme. He visto personalmente a guardias de seguridad, tanto femeninos como masculinos, bailando y cantando de forma absurda mientras prestan servicio o dentro de sus garitas de control; exhibiendo armas de fuego letales como simples objetos de entretenimiento para captar atención en internet. Esta realidad demuestra cómo la sociedad actual cae en lo efímero. Tales conductas no solo exponen una grave falta de criterio individual, sino que evidencian la ausencia de supervisión y liderazgo en las organizaciones, distorsionando por completo la percepción pública. Cabe preguntarse: ¿Qué puede pensar el cliente de una empresa de seguridad que paga por un servicio profesional y termina observando a ese mismo personal ridiculizado en redes sociales? Por ello, a continuación, compartiremos varios casos reales que suelo citar en nuestras capacitaciones sobre “Liderazgo Ético y Valores en los Profesionales de la Seguridad” dictadas por medio de INSEAL LATAM, con el firme propósito de generar conciencia y prevenir estas situaciones a futuro.

Caso real 1: El vigilante "monta piedras"

Un caso sintomático y ampliamente debatido en mis clases es el de un oficial de seguridad privada en Colombia, vinculado a una cooperativa del sector, que recurrió a la plataforma TikTok para denunciar públicamente presunto acoso laboral y anomalías internas como corrupción. Más allá de la validez o veracidad de sus reclamos, ver a un profesional uniformado expuesto en redes sociales para ventilar los conflictos de su organización expone una falla estructural profunda: la existencia de gerencias y mandos medios desconectados, incapaces de mantener canales de comunicación efectivos, así como un vacío absoluto en la gestión y resolución de conflictos internos. Cuando los problemas laborales se exponen en un video viral y no en un comité de convivencia o en el despacho de un líder, la institución sufre un doble impacto: por un lado, se evidencia la desorientación del subordinado; por el otro, se desenmascara la incapacidad del mando para escuchar, orientar y resolver. Al final, cuando la disciplina y el diálogo se rompen, toda la organización queda expuesta al escarnio y al deterioro de su credibilidad.

Caso real 2: Pelea pública entre un Policía Nacional y un guardia de Seguridad Privada

Otro caso que circula en plataformas digitales expone de forma cruda la precariedad formativa en ambos lados del servicio: un miembro de la Policía Nacional de Colombia y un oficial de seguridad privada enfrentados entre gritos, empujones y descalificaciones en plena vía pública. Por una parte, se observa al vigilante pretendiendo arrogarse una autoridad legal que las normas no le otorgan, extralimitándose en sus funciones por pura soberbia; por la otra, a un agente de la ley incapaz de ejercer su investidura con firmeza, equilibrio emocional y solvencia doctrinal. Este lamentable espectáculo no solo genera indignación en la sociedad, sino que demuestra una falla estructural en ambas trincheras: la carencia absoluta de herramientas en resolución de conflictos, la nula capacidad de gestión de crisis y un desconocimiento alarmante de los marcos legales, límites y roles que a cada uno le corresponden dentro del Estado.



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

Caso real 3: Policías Nacionales y militares femeninas, “perreando” uniformadas

Un claro reflejo de esta pérdida de brújula ética se visualizó en el sonado caso de funcionarias de la Policía Nacional y del Ejército de Colombia, captadas bailando de forma explícita con prácticas conocidas dentro de la cultura urbana actual como “perreo” y “sandungueo”, con los uniformes puestos durante un acto decembrino, nada menos que frente a la mirada atónita o alcahueta de sus superiores, compañeros y familiares. Definidos por movimientos pélvicos de alta connotación erótica y festiva, estos ritmos, aunque populares en el entretenimiento de la juventud, van totalmente en contra de la moral pública, el decoro y la compostura cuando se ejecutan bajo la investidura institucional. Que este contenido salte a la luz pública y se viralice a nivel internacional no constituye una simple anécdota simpática; es la radiografía exacta de una ausencia total de mando, de una crisis de autoridad y de una ignorancia alarmante sobre lo que significa custodiar la sobriedad, el honor y la dignidad de las instituciones. Este fenómeno retrata con precisión lo que expongo en mi libro *HABLÓ EL SARGENTO MAYOR*: Ante los antivalores de la humanidad, en el capítulo titulado “La paradoja humana: ¿Entendemos el problema?”: la triste tendencia de la sociedad contemporánea a sumergirse en comportamientos efímeros y vacíos que sacrifican el respeto, los valores fundamentales y la mística profesional a cambio de unos minutos de espectáculo en las redes sociales. Si bien, luego del espectáculo se observó al jefe de la Policía Nacional de Colombia dando declaraciones públicas al respecto, no todo pasa por retractarse y mostrar inconformidad, sino por tomar acciones para orientar y capacitar a todo su personal subordinado, evitando que cometan estos errores que rebajan la reputación de las instituciones que representan.

Caso real 4: La guerra tóxica, la indisciplina y el acoso expuesto en pantallas

Este caso expone uno de los quiebres más destructivos en la cadena de mando: la instrumentalización de las redes sociales para exponer a un subordinado, lo que destruye el principio de la disciplina interna y la dignidad del liderazgo. Un episodio lamentable que transita por las redes sociales involucra a una funcionaria de la Policía Nacional y a su superior directo. En el material, la uniformada, en medio de un evidente trasfondo de tensión y presunto acoso laboral, es grabada por su propio oficial en el preciso instante en que desobedece una orden, video que posteriormente fue difundido en internet. Esta maniobra desnuda algo mucho más grave que una falta de indisciplina individual: revela una intencionalidad destructiva por parte del superior y expone una nula formación en liderazgo, la ruptura del reconocimiento jerárquico sano y la pérdida absoluta del respeto mutuo. La verdadera disciplina no se construye sometiendo o ridiculizando al subalterno ante la opinión pública; se cultiva desde la inteligencia emocional, el ejemplo, la justicia en el mando y la protección de la dignidad institucional en cada escalón de la cadena de mando



Caso real 5: La otra cara de la moneda - Lo positivo a rescatar

A pesar de este panorama sombrío, es fundamental señalar que no todo es oscuridad en el vasto ecosistema digital. Afortunadamente, las redes sociales también nos muestran la senda de la excelencia profesional a través del trabajo tesonero de hombres y mujeres de la seguridad pública y privada que han comprendido el poder transformador de estas plataformas. Ejemplo de ello es el caso de un guardia de seguridad privada venezolano en Colombia, quien, portando su uniforme de forma pulcra e impecable, aprovecha de manera ejemplar el espacio digital para orientar, educar e instruir a la ciudadanía en materia de seguridad preventiva. Asimismo, presenciamos a profesionales íntegros que destinan sus canales a la divulgación de contenido puramente pedagógico: analistas que explican cómo prevenir el delito, expertos en autoprotección y uniformados que acercan la institución a la comunidad bajo principios de respeto y doctrina sólida. Este fenómeno nos deja una lección contundente: crear contenido de servicio no está mal, siempre y cuando se fomente la cultura del equilibrio. Esto implica utilizar los momentos de descanso o pausas autorizadas para educar, sin descuidar jamás la vigilancia activa ni las funciones operativas por las cuales se percibe un salario. El uso de las redes sociales no debe prohibirse bajo una censura anacrónica; por el contrario, debe ser guiado por directrices claras emanadas desde las gerencias y mandos institucionales. Cuando el canal digital se enfoca en enseñar y aportar valor a la sociedad sin comprometer el deber, la tecnología se convierte en la más poderosa aliada de la profesionalización.

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! ♥*

El impacto reputacional: La quiebra de la confianza pública y el valor de los profesionales honestos

¿Qué nivel de confianza puede albergar el ciudadano o un cliente corporativo cuando observa a quien debe proteger su vida y su patrimonio protagonizando conductas ridículas, controversias callejeras o ventilando el caos interno en plataformas digitales? Las redes sociales operan hoy como un tribunal implacable donde el desatino de un solo individuo es capaz de manchar el sacrificio de miles de hombres y mujeres honrados que, bajo el sol y la lluvia, entregan su vida con verdadera vocación de servicio. Cuando estos videos se viralizan, la sociedad generaliza de forma inmediata: la percepción de la seguridad integral se desploma y el profesional de la prevención pasa a ser visto como un actor improvisado sin criterio operativo. Esta realidad genera un estado de profunda indefensión social y destruye el valor de la profesión. Es urgente detener esta espiral reputacional: los mandos deben reaccionar con liderazgo, doctrina y acompañamiento ético, recordando que la autoridad no se impone en una pantalla, se construye con disciplina, respeto y servicio en la calle.

Conclusiones: Hacia una cultura de profesionalización, liderazgo ético y mejora continua

El diagnóstico presentado a lo largo de este análisis no debe ser interpretado como un simple reproche destructivo, sino como un llamado urgente y reflexivo a la acción correctiva. La seguridad integral, tanto en el ámbito público como en el sector privado, atraviesa un punto de inflexión decisivo en la era de la hiperconectividad. Los errores, la falta de mística y la pérdida de compostura observados en plataformas digitales no son fallas aisladas del operador o del funcionario; son la manifestación visible de un vacío doctrinario y de un déficit de liderazgo en las estructuras de mando.

Para revertir esta espiral reputacional en Colombia y consolidar un modelo de excelencia operacional a nivel internacional, es imperativo implementar un plan de acción sustentado en cuatro pilares fundamentales:

1. Reestructuración de la formación en Liderazgo

Ético: Las instituciones y empresas de seguridad privada deben trascender la capacitación puramente táctica o normativa. Se requiere priorizar programas de formación continua centrados en valores, mística profesional, inteligencia emocional y resolución pacífica de conflictos internos y comunitarios.

2. Institucionalización de canales de comunicación y resolución de crisis: La exposición de conflictos laborales o de acoso en redes sociales evidencia la quiebra de los conductos regulares. Es indispensable habilitar y fortalecer comités de convivencia, protocolos de mediación y despachos de mando de puertas abiertas, garantizando que la disciplina se ejerza con justicia y que el descontento se tramite de forma legal y profesional.

3. Regulaciones claras sobre el uso del uniforme y el entorno digital: Prohibir la tecnología es un enfoque anacrónico e ineficaz. Las directrices corporativas e institucionales deben establecer códigos de conducta explícitos sobre la huella digital. Se debe promover una "cultura del equilibrio" donde la creación de contenido de valor pedagógico o preventivo se realice fuera de las horas de servicio o en pausas autorizadas, protegiendo siempre la imagen institucional y el cumplimiento del deber.

4. Dignificación de la función de seguridad: La sociedad y las gerencias deben comprender que el profesional de la seguridad no es un activo prescindible ni un actor improvisado. La dignidad de la profesión se rescata capacitando al personal, respetando sus derechos laborales y exigiendo, a cambio, el más alto nivel de pulcritud, criterio operativo y respeto por el uniforme.

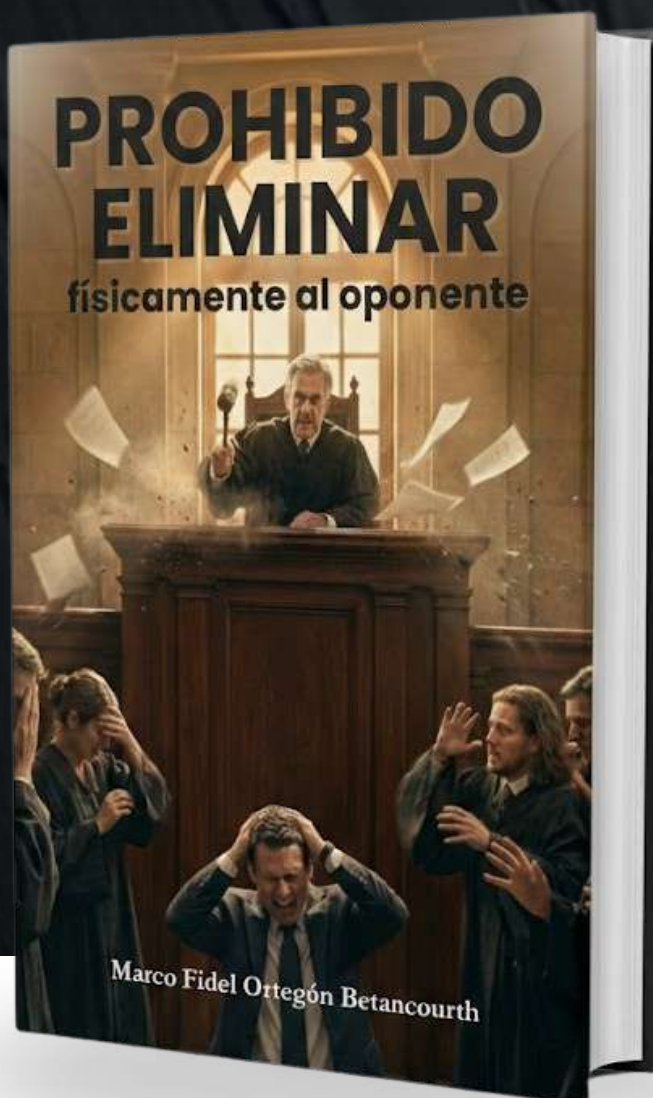
Dignificar la imagen de nuestras instituciones no se logra ocultando los problemas ni emitiendo comunicados de inconformidad tras un escándalo viral. Se construye en la garita, en la patrulla, en el puesto de control y en las aulas de clase, mediante una supervisión consciente y una pedagogía constante. Solo cuando los líderes asuman la responsabilidad integral de guiarlos, el uniforme volverá a ser símbolo indiscutible de honor, protección y orgullo ante la sociedad. En INSEAL LATAM, estamos dispuestos a contribuir capacitando de manera virtual o presencial al personal de seguridad integral y así erradicar el problema de raíz. Pueden visitar nuestro portal web: www.inseal.us para que nos contacten y conozcan nuestros programas de capacitación y mejora continua.



@libroteoriaestado

YA DISPONIBLE

PROHIBIDO ELIMINAR FÍSICAMENTE AL Oponente



amazon
kindle



hotmart

Para más información
+57 300 7317523



CUANDO YA NO HAY UN CENTRO QUE ATACAR LO QUE LAS REDES EN MALLA PUEDEN ENSEÑARLE A LA SEGURIDAD DE UNA EMPRESA

Por Carlos Eduardo Valenzuela Oviedo

Imagine una carretera con un solo puente. Si ese puente se cae, todo el tráfico se detiene. Ahora imagine una ciudad con cientos de calles conectadas entre sí: si una calle se bloquea, los carros toman otra y la vida sigue. Esa segunda imagen es lo que en tecnología se llama una «red en malla». No tiene un centro que la controle. Cada punto se conecta con varios otros. La información —igual que los carros o el agua— siempre encuentra un camino. Esta idea, que hoy hace funcionar internet y las aplicaciones de mensajería, tiene mucho que enseñarle a quienes trabajamos cuidando a las empresas.

Cuando las empresas se pensaban como castillos

Durante muchos años, la seguridad de una empresa se pensó como si fuera un castillo. Había un centro fuerte —una oficina, un jefe, un cuarto de control— y una muralla alrededor para protegerlo. Este modelo servía porque los peligros también eran claros: un ladrón, un grupo criminal con un líder visible, un enemigo con nombre y dirección.

Pero ese mundo ya no existe. Hoy las amenazas vienen de muchos lados a la vez. Un ataque por internet puede llegar desde cientos de computadores al mismo tiempo. La corrupción se cuela por varios puntos de una cadena de proveedores. La extorsión no depende de un solo jefe. Las mentiras se multiplican solas en redes sociales. Frente a peligros que no tienen un centro, defender un centro se ha vuelto un error muy caro.

«Cuando los peligros vienen de muchos lados a la vez, defender un solo lugar deja de servir.»

Tres virtudes que vale la pena copiar

Una red en malla tiene tres virtudes que a cualquier empresa le convienen. La primera: si un punto falla, la información toma otro camino. La segunda: nadie puede paralizar todo el sistema atacando un solo lugar, porque no existe un solo lugar clave. La tercera: nadie puede silenciar un mensaje importante, porque siempre hay rutas alternas para que llegue.



Traído al mundo de una empresa, esto dibuja un modelo de seguridad muy distinto al de antes. Uno donde el saber sobre los riesgos no está guardado en una sola oficina, sino repartido entre muchas personas: los operarios, los técnicos, los conductores, los contratistas. Un modelo donde responder a un peligro no depende de que un jefe autorice cada paso. Un modelo donde la información importante viaja por varios caminos y no se atasca en un solo cuello de botella.

Tres cambios difíciles pero necesarios

Para que una empresa funcione como una red en malla se necesitan tres cambios que suenan sencillos pero cuestan mucho en la práctica.

El primero: aceptar que quienes más saben sobre los riesgos no siempre son los que tienen los cargos más altos. El operario que nota algo raro en una válvula, el conductor que ve un carro sospechoso siguiéndolo, o el contratista que siente una presión indebida en una licitación, saben cosas que la gerencia no ve. Todos ellos son fuentes valiosas de información, aunque no aparezcan en el organigrama con nombres importantes.

El segundo: dejar de depender de una sola línea vertical para pasar las alertas hacia arriba. Cuando toda la información tiene que pasar por una sola persona antes de llegar a quienes deciden, esa persona se convierte —sin quererlo— en el punto más débil. Si se equivoca, se ausenta o alguien la presiona, toda la empresa queda ciega.

El tercero, y quizá el más difícil: entender que dejar circular la información incómoda es una forma de cuidar la empresa. Cuando dentro de una organización se castiga al que trae malas noticias o se penaliza al que señala un problema, la empresa se queda sin ojos para ver lo que le está pasando por dentro.

«Silenciar una mala noticia dentro de una empresa suele costar más caro que enfrentarla.»

Cuando la empresa ya es, físicamente, una red

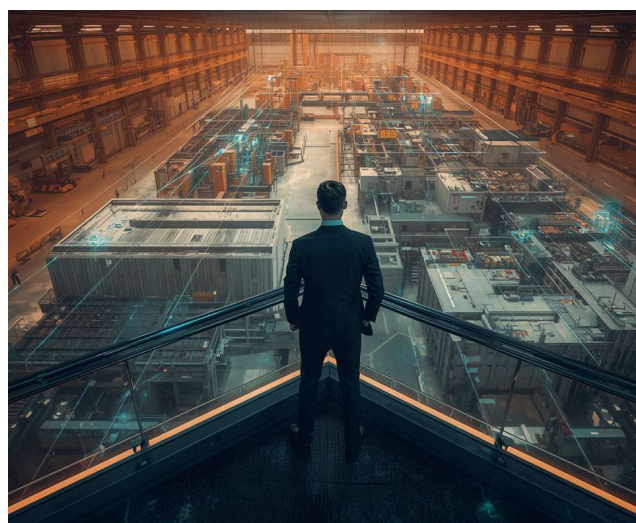
Hay sectores donde la empresa es, literalmente, una red repartida por todo el territorio. El acueducto es un ejemplo perfecto: miles de kilómetros de tuberías, estaciones, sensores y equipos de campo distribuidos por toda la ciudad y sus alrededores. Lo mismo sucede con la energía eléctrica o el transporte de combustibles.

La paradoja es que, aunque la infraestructura ya está repartida por todo el territorio, muchas veces la protección sigue concentrada en pocas oficinas centrales. Es como tener cientos de puertas en distintos barrios, pero un solo vigilante sentado en el centro de la ciudad.

Repensar esa protección con la lógica de la malla significa darle a cada punto —cada planta, cada estación, cada equipo en la calle— la capacidad de detectar problemas, de comunicarse de manera segura, de tomar pequeñas decisiones sin esperar autorización y de coordinarse con los puntos vecinos. No hay una bóveda que blindar: hay un tejido que sostener.

El nuevo perfil del que cuida la empresa

Si esta idea se toma en serio, el trabajo del responsable de seguridad cambia por completo. Ya no será el jefe de una fortaleza, sino algo más parecido al tejedor de una red. Su tarea principal no será acumular herramientas en una oficina, sino repartirlas con inteligencia por toda la organización. No será controlar la información desde un solo punto, sino asegurarse de que fluya por varios caminos y llegue a tiempo a quien la necesita. No será proteger un núcleo, sino cuidar que el tejido completo no se rompa.



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



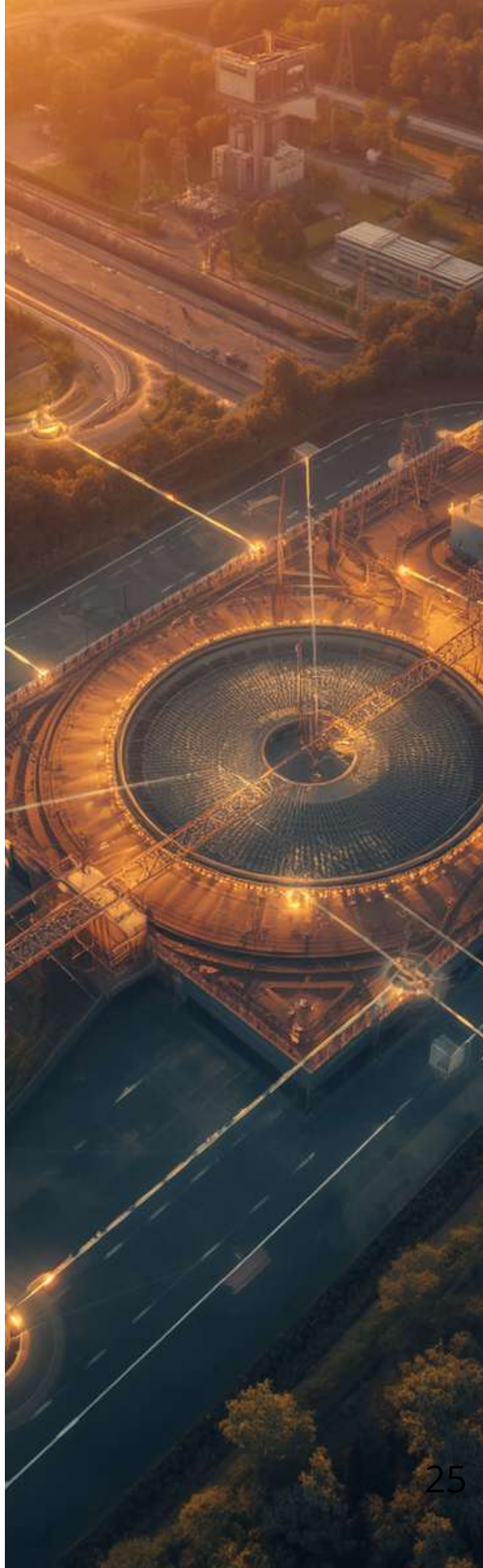
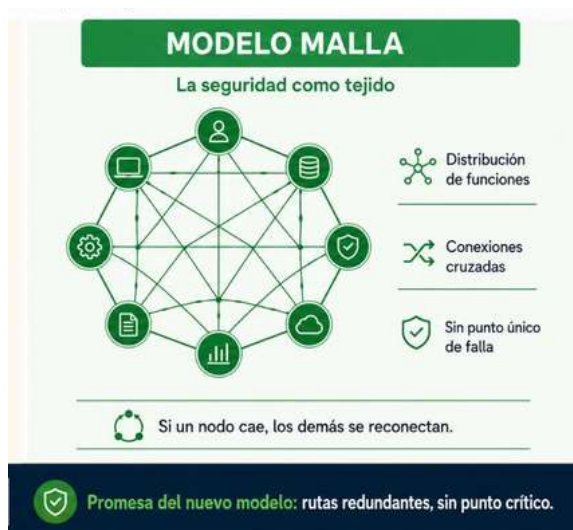
Innovación
tecnológica

Este cambio pide nuevas habilidades: saber leer cómo se conectan las cosas entre sí, anticipar lo que puede venir, hacer que el conocimiento circule cuando hace falta y entender que la transparencia interna no es un lujo político, sino una herramienta de seguridad.

La red en malla no es solo una forma de conectar computadores. Es una manera de organizar la resistencia frente a peligros que también aprendieron a moverse sin un centro. Adoptarla no significa renunciar al orden: significa cambiarlo. Menos jerarquía vertical, más coordinación entre muchos puntos. Menos control desde arriba, más confianza bien medida entre iguales. La seguridad del futuro no se defenderá en el centro, porque ya no habrá un centro que defender. Se defenderá en la red, o no se defenderá.

Seguridad: castillo vs. malla.

Dos arquitecturas de protección, dos lógicas de resiliencia.





Seguridad
Privada

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



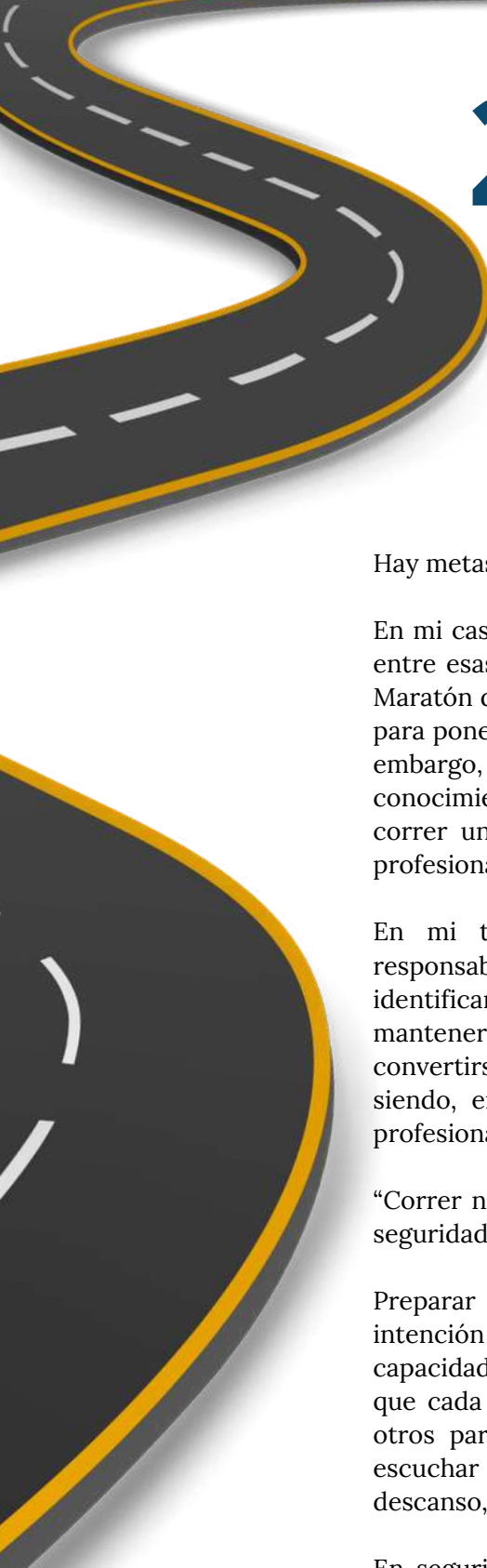
Calle 143 #46-09
Bogotá, Colombia



601 744 25 10



director.comercial@pph.com.co



21 kilómetros

cuando correr también es aprender a
gestionar el riesgo

Yinna Marcela Gutiérrez Orjuela

Hay metas que empiezan mucho antes de la línea de partida.

En mi caso, comenzó varios años atrás, cuando decidí recorrer kilómetros y, entre esas decisiones, prepararme para correr los 21 kilómetros de la Media Maratón de Bogotá. Al principio lo vi como un reto personal, una oportunidad para poner a prueba mi resistencia física y mental, así como mi disciplina. Sin embargo, mientras avanzaba en los entrenamientos y profundizaba en el conocimiento de este deporte, que hoy llamo “un arte más”, descubrí que correr una media maratón tenía muchas más similitudes con mi ejercicio profesional de las que inicialmente imaginaba.

En mi trabajo como Jefe de Seguridad Física, buena parte de mi responsabilidad está relacionada con anticiparme a diferentes escenarios: identificar riesgos, establecer controles, planear, hacer seguimiento, mantener la constancia y tomar decisiones antes de que una situación pueda convertirse en una emergencia. Prepararme para 21 kilómetros terminó siendo, en cierta forma, un ejercicio práctico de esos mismos principios profesionales.

“Correr no empieza cuando se da la señal de salida. De la misma manera, la seguridad no empieza cuando ocurre un incidente.”

Preparar una media maratón exige planeación. No basta con tener la intención de correr 21 kilómetros; es necesario construir progresivamente la capacidad y la experiencia para hacerlo. Durante esta preparación aprendí que cada entrenamiento tenía un propósito: algunos días eran para correr, otros para fortalecer, otros para recuperar y algunos, simplemente, para escuchar mi cuerpo. También tuve que revisar la alimentación, hidratación, descanso, ritmo y, sobre todo, la capacidad de recuperación.

En seguridad física ocurre algo similar. Una operación segura no depende exclusivamente de reaccionar correctamente frente a un evento; depende de todo aquello que se haya planeado con anterioridad y de la preparación frente a los escenarios que puedan presentarse durante las diferentes operaciones de seguridad: identificación de amenazas, reconocimiento de vulnerabilidades, establecimiento de medidas de prevención, estructuración de protocolos, verificación de capacidades de respuesta y claridad sobre quién debe tomar decisiones.

Por tanto, en ambos escenarios, la improvisación puede ser costosa. Un entrenamiento mal planificado puede terminar en una lesión o, en casos extremos, comprometiendo la vida; una medida de seguridad mal diseñada puede generar una afectación operativa, económica o incluso humana. Por eso, tanto en la carrera como en mi trabajo, he aprendido a valorar una palabra que parece sencilla, pero que tiene un enorme significado: anticipación.

Uno de los aprendizajes más importantes de correr distancias largas es entender que el cuerpo y la mente son una máquina de enviar señales que, con profesionalismo y serenidad, debemos aprender a escuchar.

En algunos entrenamientos aparece el cansancio, la pesadez en las piernas, la dificultad para mantener el ritmo o incluso la sensación de que respirar se hace más difícil. En esos momentos, una primera reacción puede ser continuar como si nada estuviera pasando. Sin embargo, aprender a reconocer esas señales también hace parte de la preparación.

En seguridad física sucede exactamente lo mismo. Los riesgos no siempre aparecen de manera evidente. Muchas veces existen señales previas: comportamientos inusuales, cambios en el entorno, información sobre situaciones de orden público, fallas tecnológicas, vulnerabilidades en una instalación o cualquier circunstancia que pueda afectar la continuidad de una operación.

“El reto está en identificar esas señales a tiempo.”

En mi experiencia profesional, las alertas tempranas son una herramienta fundamental. No se trata solamente de reaccionar ante una situación crítica, sino de observar, analizar y comunicar oportunamente para que las decisiones puedan tomarse antes de que el riesgo se materialice.

Durante esta carrera de 21 kilómetros aprendí que no todas las decisiones tienen que tomarse con la misma velocidad. Hay momentos para acelerar y momentos para conservar energía; momentos para avanzar y otros para ajustar la estrategia.

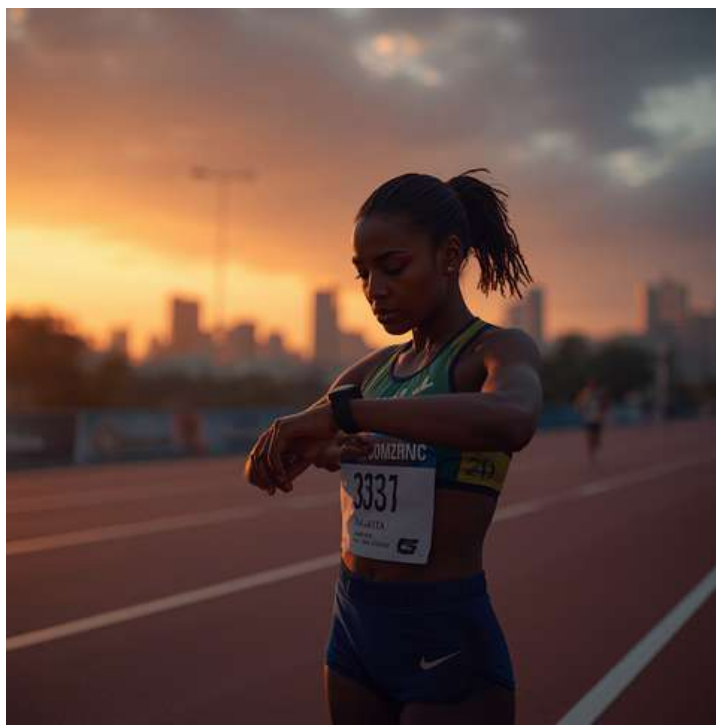
“La seguridad requiere exactamente este mismo equilibrio.”

Ninguna carrera está completamente libre de riesgos. Puede aparecer el desgaste mental “el enemigo número uno (1) del runner” o muscular, y es allí donde adquiere valor el arte de saber escuchar el cuerpo y conocer bien la estrategia, también puede presentarse una condición climática inesperada, como ocurrió durante la carrera: en el parque Simón Bolívar un clima lluvioso y bastante frío, poco antes de iniciar los rayos del sol bogotano y por la calle 92, encontrarse nuevamente con la lluvia y algo de viento. En ese momento surge la pregunta: ¿estamos preparados? Y la respuesta fue clara: ya habíamos entrenado con estos factores, ¡lo podemos hacer!

Lo mismo ocurre en las organizaciones, la gestión del riesgo no significa pretender que nunca ocurrirá un incidente. Significa desarrollar la capacidad para reducir la probabilidad de que suceda, disminuir sus consecuencias y tener preparada una respuesta adecuada, manteniendo siempre la capacidad de reacción y el constante entrenamiento mental y operacional.

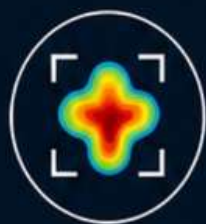
Por lo anterior, es pertinente hablar de mitigación del riesgo en ambos escenarios, en mi trabajo, esta visión implica pensar permanentemente en controles preventivos, protocolos de actuación, sistemas tecnológicos, vigilancia, coordinación con diferentes actores y capacidad de respuesta frente a situaciones críticas.

En la carrera, mis mecanismos de mitigación fueron diferentes, pero obedecían a la misma lógica: entrenar progresivamente, fortalecer, descansar, alimentarme adecuadamente, conocer mis límites y tener una estrategia para afrontar los 21 kilómetros.



¿SABE REALMENTE QUÉ ESTÁ PASANDO EN SUS TIENDAS?

Nuestra analítica convierte
el video en información



MAPAS DE CALOR

Identifique las zonas
con mayor interacción.



TIEMPO DE PERMANENCIA

Conozca cuánto tiempo
permanece cada cliente
en las diferentes áreas.



ANÁLISIS DE COMPORTAMIENTOS

Detecte merodeo y conductas
inusuales antes de que
representen un riesgo.



Solicite una asesoría
para su operación

 314 297 7321



**SECURITY
SHOPS**

“La seguridad requiere exactamente este mismo equilibrio.”

Ninguna carrera está completamente libre de riesgos. Puede aparecer el desgaste mental “el enemigo número uno (1) del runner” o muscular, y es allí donde adquiere valor el arte de saber escuchar el cuerpo y conocer bien la estrategia, también puede presentarse una condición climática inesperada, como ocurrió durante la carrera: en el parque Simón Bolívar un clima lluvioso y bastante frío, poco antes de iniciar los rayos del sol bogotano y por la calle 92, encontrarse nuevamente con la lluvia y algo de viento. En ese momento surge la pregunta: ¿estamos preparados? Y la respuesta fue clara: ya habíamos entrenado con estos factores, ¡lo podemos hacer!

Lo mismo ocurre en las organizaciones, la gestión del riesgo no significa pretender que nunca ocurrirá un incidente. Significa desarrollar la capacidad para reducir la probabilidad de que suceda, disminuir sus consecuencias y tener preparada una respuesta adecuada, manteniendo siempre la capacidad de reacción y el constante entrenamiento mental y operacional.

Por lo anterior, es pertinente hablar de mitigación del riesgo en ambos escenarios, en mi trabajo, esta visión implica pensar permanentemente en controles preventivos, protocolos de actuación, sistemas tecnológicos, vigilancia, coordinación con diferentes actores y capacidad de respuesta frente a situaciones críticas.

En la carrera, mis mecanismos de mitigación fueron diferentes, pero obedecían a la misma lógica: entrenar progresivamente, fortalecer, descansar, alimentarme adecuadamente, conocer mis límites y tener una estrategia para afrontar los 21 kilómetros.

Y allí encontré una reflexión que también aplica a mi trabajo, la seguridad física, como el running, no siempre se trata de ir más rápido, muchas veces se trata de saber cuándo avanzar, cuándo reducir el ritmo, cuándo cambiar la estrategia y cuándo detenerse para evitar un riesgo mayor. Los 21 kilómetros me recordaron que detrás de cada resultado hay planeación, disciplina, prevención y capacidad de respuesta.

En la carrera, la recompensa fue cruzar la meta. En mi ejercicio profesional, la satisfacción está en saber que una buena gestión de seguridad puede contribuir a que miles de personas desarrollen su trabajo, que una operación pueda continuar y que una organización esté mejor preparada para enfrentar escenarios inesperados.

Quizás por eso hoy veo los 21 kilómetros de una manera diferente, no fueron solamente una prueba deportiva, fueron 21 kilómetros de planeación, gestión del riesgo, toma de decisiones, resiliencia y aprendizaje.

Y, sobre todo, una confirmación personal de que tanto en la vida como en la seguridad, llegar a la meta no depende únicamente de la fuerza para avanzar, sino de la capacidad de prepararnos para todo aquello que pueda aparecer en el camino.;

¡Gracias Running!





BUSINESS ALLIANCE FOR SECURE COMMERCE



1996 - 2026

12° Congreso Mundial

Septiembre 1-2, 2026 | Miami

12° Congreso Mundial

Septiembre 1-2, 2026

Hyatt Regency Brickell
Miami, FL.

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

Costos por participación

Early Bird

Hasta junio 15 de 2026

Miembros BASC*: USD \$580.00

Entrada General (No BASC): USD \$580.00

Audidores Internacionales BASC: USD \$650.00

Registro Regular

Desde junio 16 hasta agosto 31 de 2026

Miembros BASC*: USD \$620.00

Audidores Internacionales BASC: USD \$620.00

Entrada General (No BASC): USD \$670.00

Tarifa especial para acompañantes**: USD \$ 300.00

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



@CongresoMundialBASC_
@BASCGlobalConference

Contáctenos para inscripción:

Teléfono: +573102527801

E-mail: asistente.direccion@basc.org.co

*Miembros BASC: Empresas afiliadas y/o certificadas BASC, miembros de Juntas Directivas BASC, y colaboradores BASC.

**Aplica para conyuge e hijos.

INCENDIOS DE AUTOS ELÉCTRICOS

El riesgo invisible está en el humo



HERNÁN DOMÍNGUEZ

Cuando una batería de un vehículo eléctrico entra en fuga térmica, el peligro no se limita a las llamas.

Antes de aproximarse, las brigadas industriales y los bomberos deben considerar otro riesgo menos visible: la liberación de gases tóxicos, inflamables y asfixiantes que pueden afectar tanto a los ocupantes como a quienes intervienen en la emergencia.

Una investigación publicada en Fire Safety Journal analizó dos incendios a escala real en vehículos eléctricos. Los resultados dejan una advertencia importante:

La atmósfera puede volverse peligrosa cerca del vehículo mucho antes de que el humo tóxico ingrese de manera significativa al habitáculo.

¿Qué investigó el estudio?

Los investigadores provocaron la fuga térmica mediante la penetración de una celda en la batería de tracción de dos vehículos eléctricos idénticos. Los vehículos tenían las ventanillas y puertas cerradas y el sistema de ventilación apagado. Las pruebas se realizaron al aire libre y se midieron gases en tres puntos:

- Zona respiratoria del conductor.
- Zona respiratoria del pasajero trasero derecho.
- Pasarruedas trasero derecho, próximo a la celda afectada.

Entre las sustancias analizadas se encontraban:

- Fluoruro de hidrógeno —HF—.
- Cianuro de hidrógeno —HCN—.
- Monóxido y dióxido de carbono.
- Acetileno e hidrocarburos.
- Carbonatos orgánicos provenientes del electrolito.
- Concentración de oxígeno.
- La presencia y combinación de estas sustancias puede producir irritación, dificultad respiratoria, desorientación, pérdida de coordinación e incapacidad.

El humo no necesariamente ingresa de inmediato al habitáculo

En las pruebas, los gases liberados inicialmente encontraron vías de salida hacia el exterior. Sin embargo, a medida que avanzó el incendio, el calor y el daño generaron nuevas rutas de propagación.

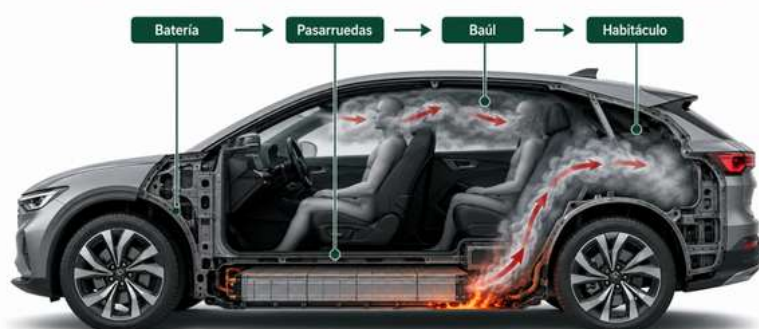
En estos vehículos, una de las principales vías observadas fue:

Batería → pasarruedas trasero → baúl → asientos traseros → zona del conductor.

El calentamiento del pasarruedas y de los componentes próximos permitió que el fuego y los gases alcanzaran el baúl. Desde allí, el humo se propagó al habitáculo.

- Esta ruta no debe considerarse universal. Puede cambiar según:
- Modelo y arquitectura del vehículo.
- Ubicación de la primera celda afectada.
- Integridad de la carcasa de la batería.
- Daños provocados por una colisión.
- Sistemas de sellado y ventilación.
- Lugar donde se encuentre estacionado el vehículo

UNA POSIBLE RUTA DEL HUMO TÓXICO



Ruta observada en los ensayos del informe. Puede variar según vehículo y daño.

HERNÁN DOMÍNGUEZ

El dato más importante para los primeros respondientes

El estudio utilizó el concepto de dosis efectiva fraccional —FED— definido en la norma ISO 13571 para estimar la posible discapacidad causada por gases asfixiantes y por la disminución del oxígeno. Se adoptó un valor FED de 0,3 como umbral conservador de afectación significativa. En los ensayos, ese nivel se alcanzó cerca del pasarruedas trasero derecho en:

- Ensayo 1: 2 minutos y 34 segundos.
- Ensayo 2: 3 minutos y 25 segundos.
- Estos resultados no establecen un “tiempo seguro” universal. Pero muestran que la atmósfera próxima al vehículo puede deteriorarse desde los primeros minutos.

Para el primer respondiente, esto significa que acercarse a inspeccionar el vehículo sin protección respiratoria, permanecer cerca del pasarruedas o inclinarse sobre el baúl puede generar una exposición peligrosa, incluso cuando todavía no existe un incendio generalizado.

EL RIESGO PUEDE APARECER MUY TEMPRANO

ENSAYO 1

2 min 34 s



ENSAYO 2

3 min 25 s



! Umbral FED 0,3 cerca del pasarruedas trasero derecho

! Datos indicativos de dos ensayos al aire libre. No son tiempos universales.
Fuente: Rappolter et al., Fire Safety Journal 182 (2020), 104717.

HERNÁN DOMÍNGUEZ

¿Qué sucede dentro del vehículo?

Los dos automóviles eran idénticos, pero el desarrollo de los incendios fue muy diferente.

En uno de los ensayos, el humo ingresó de manera importante al habitáculo alrededor de los 14,5 minutos. En el otro, lo hizo mucho más tarde.

Sin embargo, una vez producido el ingreso significativo del humo, las condiciones se deterioraron rápidamente. En ambos ensayos se observó:

- Aumento brusco del monóxido y dióxido de carbono.
- Disminución severa del oxígeno.
- Presencia de HCN, HF y otros compuestos tóxicos.
- Posible pérdida de orientación y capacidad motora.
- Reducción crítica de la capacidad de autoevacuación.

Un punto especialmente relevante es que, después de aparecer las primeras llamas en el pasarruedas, el oxígeno del habitáculo descendió de aproximadamente 20 % a 5 % en solo 4,5 minutos en ambos ensayos.

La ausencia inicial de humo en el interior, por lo tanto, no garantiza que la situación permanezca estable.

PTEE

PROGRAMA DE TRANSPARENCIA Y ÉTICA EMPRESARIAL

En Huella Gestión ayudamos a tu empresa a diseñar, implementar y evaluar tu PTEE, dando cumplimiento a la **Ley 2195 de 2022** y fortaleciendo una cultura de transparencia, ética e integridad.



PREVENIMOS RIESGOS DE
**CORRUPCIÓN, SOBORNO
Y CONFLICTOS DE INTERÉS.**
PROMOVEMOS NEGOCIOS
ÉTICOS Y SOSTENIBLES.



BENEFICIOS DE IMPLEMENTAR TU PTEE



REDUCE RIESGOS
LEGALES Y
REPUTACIONALES



PREVIENE ACTOS
DE CORRUPCIÓN
Y SOBORNO



FORTALECE LA CULTURA
DE INTEGRIDAD Y
BUEN GOBIERNO



CUMPLE CON LA
NORMATIVA VIGENTE
(LEY 2195 DE 2022)



GENERA CONFIANZA
CON CLIENTES,
ALIADOS E INVERSIONISTAS



¡CONTÁCTANOS HOY!
DISEÑAMOS E IMPLEMENTAMOS
TU PTEE PARA UNA GESTIÓN
ÉTICA Y TRANSPARENTE.



+57 315-511-1916



servicioalcliente@huellalogistica.com



www.huellalogistica.com.co

Cinco recomendaciones para el personal de seguridad, las brigadas y los bomberos

1. Identificar el sistema de propulsión

El personal interviniente debe confirmar si se trata de un vehículo eléctrico, híbrido o convencional. También debe consultar, cuando esté disponible, la guía de respuesta de emergencia del fabricante.

2. Controlar la aproximación

Siempre que el escenario lo permita, la aproximación debe realizarse desde una posición favorable respecto del viento y evitando permanecer innecesariamente cerca de la parte inferior, el pasarruedas o el baúl.

El humo de color claro tampoco debe interpretarse como inofensivo.

3. Utilizar protección respiratoria

El personal que ingrese en la zona potencialmente contaminada debe utilizar el nivel de protección respiratoria establecido por el procedimiento y el sistema de comando.

En operaciones de extinción, rescate, revisión o remoción con atmósfera no caracterizada, un respirador con filtro no sustituye al equipo de respiración autónoma de presión positiva.

4. Limitar la exposición

La organización debe establecer zonas de trabajo, controlar el acceso y reducir la cantidad de personas expuestas. Bomberos, brigadistas, policías, operadores de grúa y personal de mantenimiento pueden quedar dentro de la trayectoria del humo.

5. Prever monitoreo, descontaminación y seguimiento

La desaparición de las llamas no significa que el riesgo haya terminado. Deben contemplarse:

- Monitoreo atmosférico acorde con la evaluación del incidente.
- Posibilidad de reignición.
- Descontaminación de equipos y ropa.
- Manejo seguro del agua y los residuos contaminados.
- Evaluación médica ante síntomas o exposición significativa.
- Transporte y almacenamiento temporal del vehículo dañado.

ANTES DE ACERCARSE



1. Identificar el vehículo y la batería



2. Trabajar a barlovento cuando sea posible



3. Usar protección respiratoria adecuada



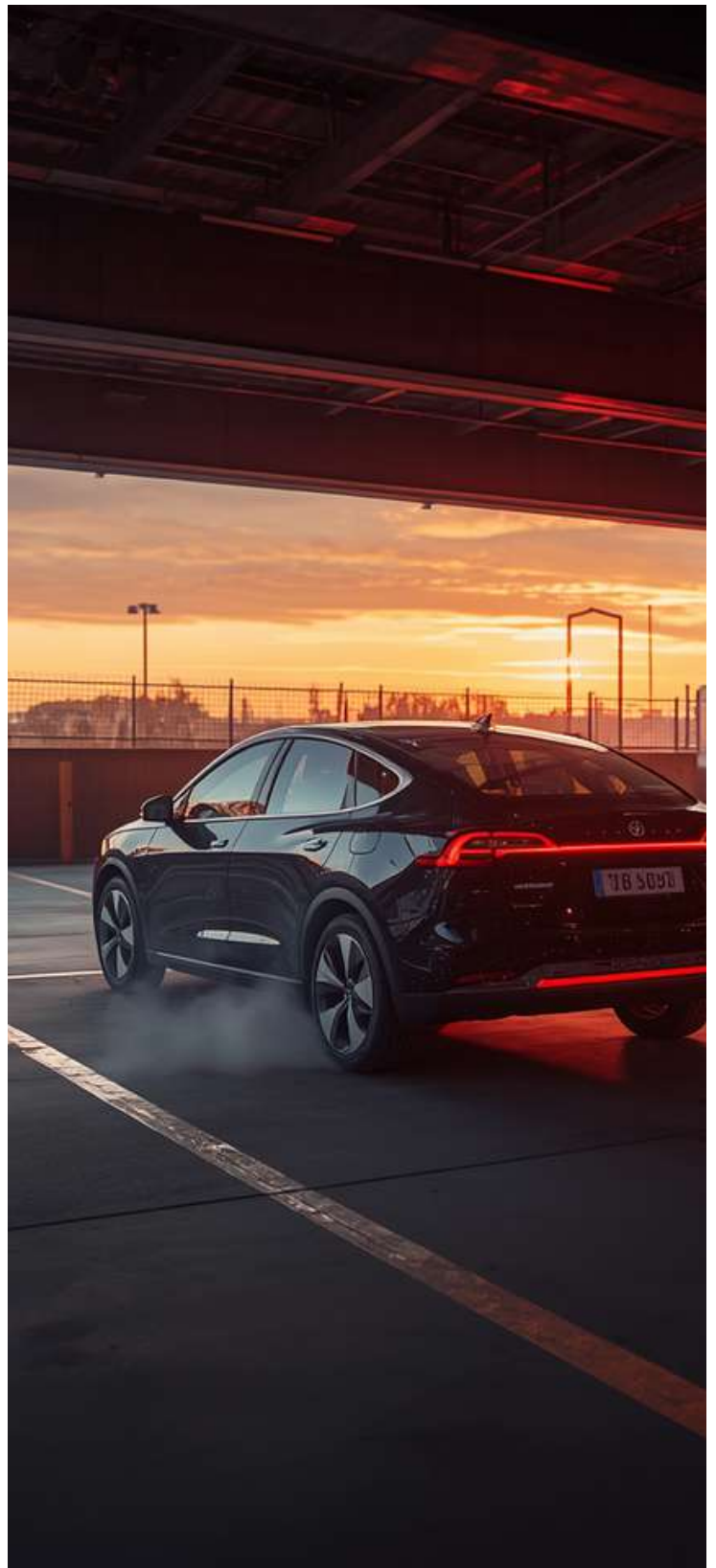
4. Controlar la zona y limitar exposiciones



5. Prever monitoreo y descontaminación



Integrar estas medidas al procedimiento y al sistema de comando local.



¿Están preparados nuestros planes de emergencia?

Muchas organizaciones ya incorporaron vehículos eléctricos, cargadores o flotas electrificadas. Sin embargo, sus planes de emergencia continúan describiendo únicamente procedimientos para vehículos convencionales.

Un protocolo actualizado debería responder, como mínimo, estas preguntas:

- ¿Cómo identificará la brigada el tipo de vehículo?
- ¿Quién ordenará la evacuación y el aislamiento?
- ¿Qué protección respiratoria estará disponible?
- ¿Cómo se coordinará la respuesta con los bomberos?
- ¿Dónde permanecerá el vehículo después del incidente?
- ¿Cómo se manejarán una posible reignición y la contaminación?
- ¿Los operadores de grúa y seguridad conocen estos riesgos?
- ¿Se ha realizado un simulacro específico?

El problema no se resuelve agregando una página genérica sobre baterías. Es necesario revisar escenarios, recursos, responsabilidades, capacitación y coordinación externa.

Los incendios de vehículos eléctricos no deben evaluarse solamente por la altura de las llamas.

La generación de gases puede comenzar desde los primeros momentos de una falla crítica. Su trayectoria puede variar y las condiciones pueden cambiar rápidamente.

Para las brigadas y los bomberos, la principal enseñanza es clara:

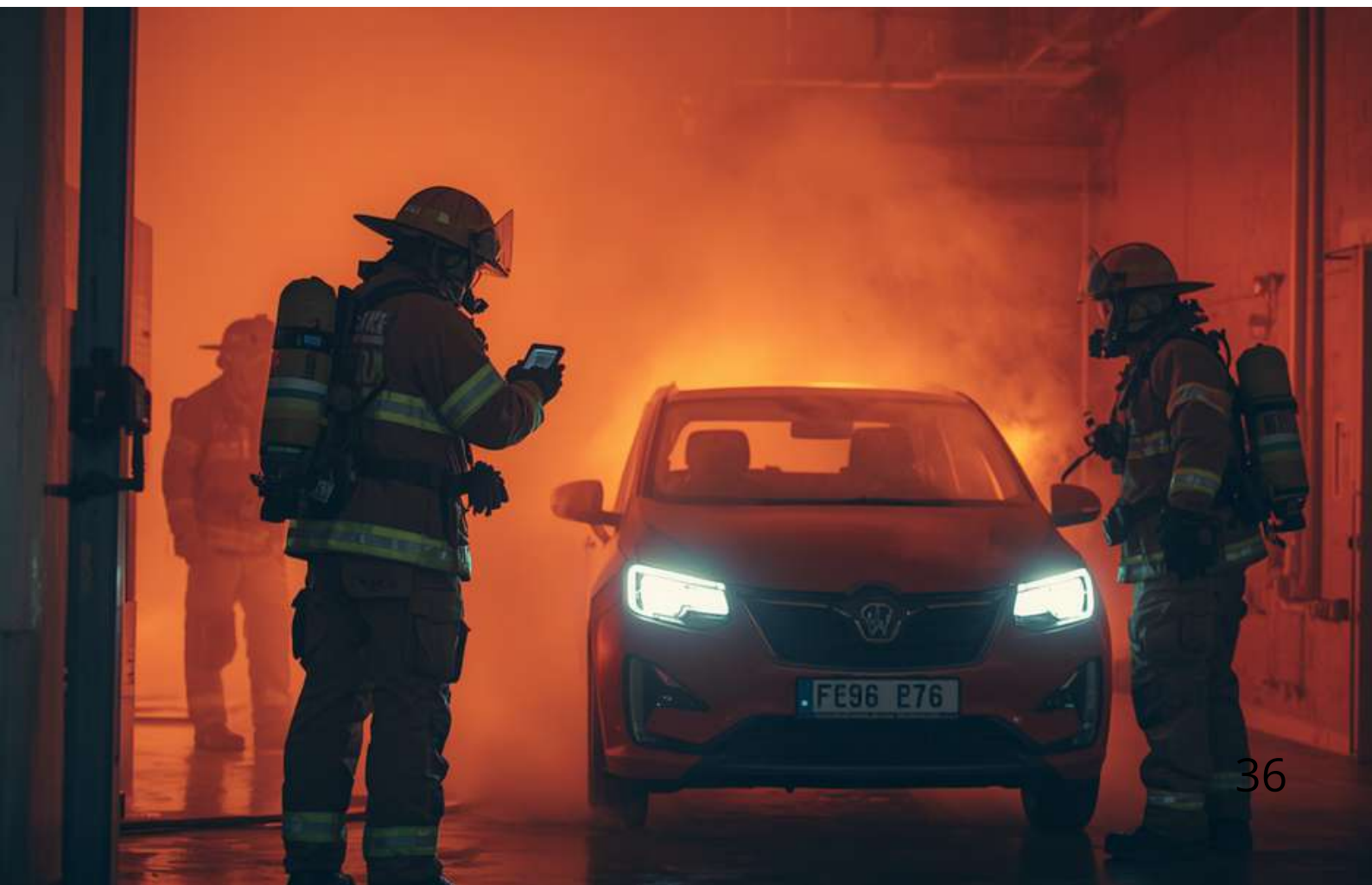
Si no se ha caracterizado la atmósfera, el humo debe considerarse peligroso y la aproximación debe realizarse con protección, control y un procedimiento previamente definido.

Las empresas no necesitan improvisar durante el incidente. Necesitan integrar este riesgo antes de que ocurra.

Fuente y limitaciones

Fuente principal: Tim Rappsilber, Simone Krüger, Tina Raspe, Rudolf Recló y Hans-Georg Schweiger, "Toxic gas emission in electric vehicles: What a battery fire means for occupant safety", Fire Safety Journal, volumen 162, 2026, artículo 104717.

El estudio comprende dos ensayos al aire libre, realizados con el mismo modelo de vehículo, alto estado de carga, fuga térmica inducida por penetración, puertas y ventanillas cerradas y ventilación apagada. Sus tiempos son indicativos y no deben extrapolarse directamente a todos los vehículos, colisiones, estacionamientos cerrados o intervenciones reales.





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

INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y GEOPOLÍTICA: UNA CONVERGENCIA ESTRATÉGICA INEVITABLE

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



Durante décadas, la seguridad nacional se interpretó principalmente desde una lógica tradicional: defensa del territorio, capacidades militares y sistemas de alianzas. Sin embargo, el siglo XXI ha introducido una transformación estructural que obliga a replantear estos pilares. Hoy, el poder no se mide únicamente en términos físicos, sino también en la capacidad de procesar información, desarrollar algoritmos y controlar infraestructuras digitales.

En este nuevo escenario, la inteligencia artificial (IA), la ciberseguridad y la geopolítica han dejado de ser campos independientes para integrarse en un mismo eje estratégico. Esta convergencia redefine la manera en que los Estados compiten, gestionan riesgos y proyectan influencia a nivel global.

Para comprender esta transformación, es fundamental precisar los conceptos. La inteligencia artificial puede definirse como “el estudio de agentes que reciben percepciones de su entorno y realizan acciones que maximizan sus posibilidades de éxito” (Russell y Norvig, 2021). Esta formulación, ampliamente aceptada en la comunidad académica, permite entender la IA no solo como una herramienta tecnológica, sino como un sistema de toma de decisiones automatizado con impacto directo en múltiples ámbitos, entre ellos la seguridad.

En la práctica, la IA funciona como un multiplicador de capacidades. Desde sistemas de vigilancia predictiva hasta el análisis de grandes volúmenes de información, los algoritmos permiten anticipar amenazas, optimizar procesos y respaldar decisiones de alto nivel. No obstante, este avance también plantea interrogantes importantes. Como advierte Bostrom (2014), el desarrollo de sistemas altamente autónomos conlleva riesgos que van desde sesgos algorítmicos hasta la opacidad en la toma de decisiones, factores que pueden debilitar la gobernanza y la estabilidad institucional.

En paralelo, la ciberseguridad ha dejado de ser una cuestión meramente técnica para convertirse en un componente esencial de la seguridad nacional. Según Singer y Friedman (2014), el ciberespacio se ha consolidado como un nuevo dominio de conflicto en el que actores estatales y no estatales compiten por el acceso, el control y la influencia. En este sentido, los ciberataques ya no son hechos aislados, sino instrumentos estratégicos capaces de afectar infraestructuras críticas, sistemas financieros y servicios esenciales para la población.



Este cambio implica que la seguridad ya no depende solo de la defensa física, sino también de la resiliencia digital. Proteger redes, bases de datos y sistemas operativos pasa a ser una prioridad, ya que su vulnerabilidad puede generar consecuencias tan graves como las de un ataque convencional, aunque con menor visibilidad y mayor dificultad para identificar a su responsable.

Desde la mirada geopolítica, esta interacción está reconfigurando el equilibrio de poder mundial. Como señala Kissinger (2021), la inteligencia artificial no solo transforma la economía, sino que altera la forma en que los Estados ejercen su influencia y toman decisiones estratégicas. Hoy la competencia ya no se limita al control territorial, sino que se extiende al dominio tecnológico.

En este contexto surge el concepto de soberanía digital, entendido como la facultad de un Estado de ejercer control sobre sus propios datos, infraestructuras y tecnologías críticas (Floridi, 2020). Esta noción es hoy un requisito indispensable para mantener la autonomía estratégica, especialmente cuando la dependencia externa en materia tecnológica puede convertirse en una forma de vulnerabilidad geopolítica.

También es necesario reconocer la irrupción de nuevos actores en la escena internacional. Empresas tecnológicas, plataformas digitales y organismos especializados manejan hoy niveles de influencia que superan las fronteras tradicionales del poder estatal. Como explica Nye (2010), esta realidad confirma que el poder en el siglo XXI es cada vez más difuso y multidimensional.

Para países como la República Dominicana y otras naciones en desarrollo, este escenario presenta una doble cara. Por un lado, implica riesgos asociados a la falta de preparación en materia de ciberseguridad y gobernanza tecnológica. Por otro, abre oportunidades concretas para fortalecer capacidades locales, formar talento especializado y posicionarse mejor en la economía global.

La clave no está simplemente en adoptar nuevas tecnologías, sino en integrarlas dentro de una visión de Estado. Esto requiere invertir en educación, actualizar los marcos normativos, fomentar la cooperación entre el sector público y el privado, y diseñar políticas que unan innovación y seguridad.

En definitiva, la convergencia entre inteligencia artificial, ciberseguridad y geopolítica no es una tendencia futura, sino una realidad que ya está en marcha. Ignorarla no solo afecta la competitividad de un país, sino que pone en riesgo su seguridad y su capacidad de adaptación.

Estamos ante una nueva forma de orden mundial, donde los datos, los algoritmos y la resiliencia digital son tan determinantes como los recursos tradicionales. Entender esta dinámica ya no es una opción académica: es una necesidad para quienes toman decisiones tanto en el sector público como en el privado.



1ER CONGRESO SST 5.0

INNOVACIÓN, IA Y EL FUTURO
DE LA SEGURIDAD EMPRESARIAL

“

NO ES UN EVENTO.
ES DONDE SE DEFINE
EL LIDERAZGO
DEL MAÑANA.



5 Y 6
AGOSTO 2026



BARRANQUILLA
COLOMBIA



AISOHMEX, A.C.



POTENCIALIZANDO
EL ALGORITMO HUMANO



CONOCIMIENTO
APLICADO



IA Y
TECNOLOGÍA



TENDENCIAS
GLOBALES



PRODUCTIVIDAD
Y RESULTADOS



CULTURA
Y SEGURIDAD

www.capitanhseq.com

La Seguridad Corporativa Comienza Antes de la Crisis

- Lo que Toda Empresa Debe Tener Bajo Control.

Por Eduardo E. Hurtado – MBA, CPP.

Los entornos empresariales son cada vez más complejo, globalizado y expuesto a amenazas multidimensionales, la seguridad corporativa ha evolucionado desde una función reactiva orientada a responder incidentes hacia una disciplina estratégica que contribuye directamente a la continuidad del negocio, la resiliencia organizacional y la protección de los activos corporativos. Las empresas enfrentan diariamente riesgos relacionados con el fraude, la corrupción, el crimen organizado, amenazas internas, conflictos laborales, incumplimientos regulatorios, ciberataques y eventos geopolíticos que pueden comprometer seriamente sus operaciones y su reputación. Ante esta realidad, existen **tres pilares** fundamentales que permiten construir un programa de seguridad corporativa robusto y sostenible, ellos son la **debida diligencia, el cumplimiento normativo mediante políticas y procedimientos, y el análisis y gestión de riesgos**. Estos elementos no deben ser vistos como procesos independientes, sino como componentes integrados de un sistema de gobernanza que permite identificar amenazas, establecer controles adecuados y garantizar una toma de decisiones informada. Sin embargo, para que estos mecanismos sean verdaderamente efectivos, es imprescindible que exista una coordinación permanente con los departamentos de Recursos Humanos (RR. HH.) y Legal, quienes aportan criterios laborales, regulatorios y éticos fundamentales para asegurar que las medidas de seguridad cumplan con la legislación vigente y respeten los derechos de los trabajadores y las partes interesadas. Posteriormente, todas las iniciativas relevantes deben ser revisadas y aprobadas por el equipo directivo, garantizando así el compromiso organizacional y la alineación con los objetivos estratégicos de la empresa.

La Debida Diligencia es La Primera Línea de Defensa

En pocas palabras, es una de las herramientas más importantes para mantener una empresa segura. Se trata de investigar, revisar y validar información sobre personas, proveedores, contratistas, socios comerciales u otros terceros antes de iniciar cualquier relación laboral o comercial con ellos. El objetivo es sencillo, identificar posibles riesgos antes de que se conviertan en problemas que puedan afectar a la empresa en aspectos financieros, operativos, legales o de reputación. Cuando se realiza correctamente, la debida diligencia ayuda a detectar antecedentes penales o comportamientos cuestionables, identificar posibles conflictos de interés, evaluar riesgos asociados con corrupción o sobornos y verificar que los proveedores tengan la capacidad técnica y financiera para cumplir con sus compromisos. Además, permite confirmar que terceros cumplen con la normativa aplicable, protege la imagen de la organización y reduce los riesgos asociados a alianzas estratégicas y relaciones comerciales. En el entorno empresarial actual, donde las cadenas de suministro son cada vez más extensas y complejas, los riesgos ya no provienen únicamente de los empleados internos. Muchas veces, una empresa puede verse tan afectada por las acciones de un proveedor o contratista como por las de su propio personal. Si un socio comercial se ve involucrado en actividades ilícitas, prácticas laborales inadecuadas o casos de corrupción, la organización que mantiene vínculos con él también puede sufrir consecuencias importantes, incluyendo daños reputacionales, pérdidas económicas, investigaciones regulatorias e incluso la pérdida de oportunidades de negocio. Por esta razón, la debida diligencia no debe verse como un simple requisito administrativo, sino como una medida preventiva que permite tomar decisiones informadas, proteger los intereses de la empresa y fortalecer la seguridad corporativa en todos los niveles.



Cuando una organización decide no realizar un proceso adecuado de debida diligencia, se expone a una serie de riesgos que pueden tener consecuencias significativas para el negocio. Entre ellos se encuentra la posibilidad de contratar personal con antecedentes o comportamientos incompatibles con cargos de confianza, así como establecer relaciones comerciales con proveedores o contratistas involucrados en actividades ilegales o poco éticas. Asimismo, la falta de verificaciones previas puede derivar en pérdidas económicas ocasionadas por fraudes, incumplimientos contractuales o malas prácticas corporativas. A esto se suman los daños reputacionales, que en muchos casos tardan años en recuperarse y pueden afectar la confianza de clientes, inversionistas y otras partes interesadas. Además, la organización puede enfrentar investigaciones regulatorias, sanciones gubernamentales e incluso litigios civiles o penales derivados de la vinculación con terceros de alto riesgo e incluso de contratación negligente. No son pocos los casos donde la ausencia de controles adecuados sobre proveedores y socios comerciales ha resultado en multas millonarias, pérdida de contratos estratégicos y un deterioro considerable de la credibilidad y confianza que sustentan el éxito de cualquier organización.

El papel de Recursos Humanos y Legal

Este proceso de debida diligencia debe llevarse a cabo en estrecha coordinación con Recursos Humanos y el departamento Legal. RH participa verificando credenciales, historial laboral, referencias profesionales y cumplimiento de requisitos relacionados con la contratación de personal. Por su parte, el departamento Legal asegura que las verificaciones cumplan las normativas de privacidad, protección de datos y legislación laboral aplicable, evitando posibles reclamaciones o incumplimientos regulatorios.



Cumplimiento Normativo es la Base de la Disciplina Organizacional

Un programa de seguridad no puede depender exclusivamente de la experiencia o criterio individual de los empleados. La organización necesita establecer lineamientos claros, documentados y formalmente aprobados para garantizar una actuación consistente en todos los niveles. Aquí es donde adquieren relevancia las políticas, procedimientos, estándares y protocolos corporativos. El cumplimiento normativo representa la capacidad de una organización para operar de acuerdo con leyes, regulaciones, normativas internas y expectativas éticas aplicables a su actividad. Dentro de la función de seguridad, esto incluye aspectos como:

- Control de acceso físico.
- Investigaciones internas.
- Protección de información sensible.
- Gestión de incidentes.
- Seguridad en viajes.
- Gestión de crisis.
- Protección ejecutiva.
- Seguridad de contratistas y visitantes.
- Protecciones de privacidad y datos personales.

Las políticas establecen las reglas generales y los principios que orientan la forma en que una organización debe actuar, mientras que los procedimientos detallan paso a paso cómo deben ejecutarse las actividades para cumplir con esos lineamientos. Cuando una empresa cuenta con políticas y procedimientos sólidos, obtiene múltiples beneficios que impactan directamente en su seguridad y eficiencia operativa. En primer lugar, permiten la estandarización de los procesos, asegurando que todos los empleados actúen bajo los mismos criterios sin importar su ubicación geográfica o nivel jerárquico. Asimismo, contribuyen a la reducción de errores, ya que la documentación formal de los procesos disminuye la improvisación y reduce la probabilidad de cometer fallas que puedan afectar la operación o generar incidentes de seguridad. Desde el punto de vista legal, proporcionan una importante protección jurídica, al demostrar que la organización ha implementado controles razonables para prevenir conductas inapropiadas, riesgos operativos o incumplimientos normativos. Además, facilitan el desarrollo de auditorías internas y externas, ya que permiten evidenciar de manera clara la existencia y aplicación de controles organizacionales. Finalmente, fortalecen la cultura corporativa, transmitiendo expectativas claras sobre los comportamientos esperados, las responsabilidades de cada empleado y el compromiso de la organización con el cumplimiento, la ética y la seguridad.

LAS EMPRESAS MÁS FUERTES NO SOLO CUIDAN RESULTADOS... CUIDAN A SU GENTE

En **Grupo SST Caribe** trabajamos por entornos laborales más seguros, saludables y humanos.

Porque cuando el bienestar se convierte en prioridad, también crecen:

- La productividad
- El compromiso
- El desempeño
- La cultura organizacional

Construimos bienestar que impulsa organizaciones.

Grupo SST Caribe



@grupossstcaribe

Consecuencias de la ausencia de políticas y procedimientos

Cuando una organización no cuenta con políticas y procedimientos claros, documentados y comunicados a sus empleados, se incrementa significativamente la probabilidad de que surjan problemas operativos y de seguridad. Adicionalmente, la ausencia de reglas definidas dificulta la asignación de responsabilidades individuales, ya que los empleados pueden argumentar que desconocían las expectativas o los requisitos establecidos por la organización. Uno de los mayores desafíos surge cuando ocurre un incidente de seguridad y la empresa intenta aplicar medidas correctivas o disciplinarias sin contar con políticas previamente establecidas. Resulta complejo exigir el cumplimiento de una norma que nunca fue formalmente creada, comunicada o explicada al personal. En estos casos, las acciones disciplinarias pueden ser cuestionadas desde el punto de vista laboral o legal, especialmente si no existe evidencia de que los empleados conocían las reglas o habían recibido capacitación sobre ellas. En otras palabras, es difícil sancionar una conducta cuando no existían directrices claras que indicaran qué era aceptable y qué no dentro de la organización. Por esta razón, las políticas y procedimientos no solo sirven para orientar las actividades diarias, sino también para proporcionar un marco de referencia que permita gestionar incidentes de manera justa, consistente y legalmente defendible. De hecho, muchas investigaciones realizadas después de eventos corporativos relevantes concluyen que el problema no fue necesariamente la falta de recursos o tecnología, sino la inexistencia de procedimientos claramente definidos, la falta de comunicación de las reglas o una implementación deficiente de los controles establecidos. Como resultado, la organización puede enfrentar pérdidas económicas, daños reputacionales y una disminución en la confianza de clientes, empleados, inversionistas y demás partes interesadas.

Análisis y Gestión de Riesgos, La Herramienta Estratégica para la Toma de Decisiones

La gestión moderna de la seguridad corporativa está basada en un principio fundamental, las decisiones deben tomarse en función de los riesgos identificados y no únicamente como reacción a los problemas cuando estos ya han ocurrido. Esto significa que los recursos, las inversiones y los controles de seguridad deben priorizarse de acuerdo con las amenazas reales que enfrenta la organización. Para lograrlo, es necesario realizar análisis de riesgos que permitan identificar amenazas, evaluar vulnerabilidades y determinar el impacto potencial que determinados eventos podrían tener sobre las operaciones, las personas, los activos y la reputación de la empresa. Este proceso es especialmente importante porque las organizaciones operan en entornos dinámicos donde los riesgos evolucionan constantemente debido a cambios tecnológicos, políticos, económicos, sociales y regulatorios. Un análisis de riesgos adecuado proporciona a la alta dirección una visión clara de las áreas más vulnerables del negocio y facilita la toma de decisiones informadas sobre las medidas necesarias para reducir o mitigar dichos riesgos.

Por el contrario, cuando una organización carece de un programa estructurado de gestión de riesgos, queda expuesta a una amplia variedad de problemas que pueden afectar seriamente su desempeño y continuidad operativa. Entre las consecuencias más comunes se encuentran la aparición de crisis inesperadas, interrupciones prolongadas de las operaciones, incidentes y accidentes de seguridad, pérdidas económicas significativas, daños a la reputación corporativa, incumplimientos regulatorios, demandas legales y afectaciones directas tanto para los empleados como para los clientes. En muchos casos, las empresas descubren sus principales vulnerabilidades únicamente después de sufrir un evento grave, cuando los daños ya se han materializado. Lamentablemente, en estas situaciones los costos de recuperación, corrección y reconstrucción de la confianza suelen ser considerablemente mayores que la inversión que habría sido necesaria para prevenir el problema mediante una adecuada identificación, evaluación y gestión de riesgos. Por esta razón, una gestión de riesgos efectiva no debe considerarse un gasto, sino una inversión estratégica que fortalece la resiliencia organizacional y contribuye a la sostenibilidad del negocio a largo plazo. La gestión de riesgos no busca eliminar todas las amenazas, algo prácticamente imposible, sino reducir la probabilidad de ocurrencia y minimizar el impacto cuando los eventos se materializan. Este enfoque permite adoptar una postura preventiva en lugar de reactiva, fortaleciendo la capacidad de adaptación y recuperación de la organización. En definitiva, la seguridad corporativa ya no debe considerarse únicamente una función operativa. Hoy representa una herramienta estratégica de gobernanza que protege personas, activos, información y reputación, permitiendo que las organizaciones alcancen sus objetivos de negocio de manera segura, sostenible y responsable.

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



Sin recursos para fortalecer las FF AA.

Por: Hugo Acero Velásquez

El gobierno de Abelardo De La Espriella no contará con recursos suficientes para cumplir muchas de las promesas que hizo durante la campaña presidencial. El déficit fiscal, los graves problemas de la salud, del sector energético y de seguridad, solo podrán ser resueltos si se cuenta con recursos frescos, hoy difíciles de conseguir.

En el caso de la seguridad, antes de finalizar el gobierno de Gustavo Petro el Ejército y Planeación Nacional ponen en evidencia el alto déficit que se tiene para fortalecer esta fuerza, sin contar las necesidades del resto de la Fuerza Pública. Adicional a esto, gobierno saliente deja una serie de compromisos por más de 36 billones de pesos que se van a pagar con vigencias futuras, es decir, el nuevo gobierno va a encontrar presupuestos de inversión ya comprometidos y sin considerar si lo que se va a adquirir con esos recursos, es lo que se requiere para enfrentar los problemas de violencia y delincuencia actuales.

En qué van a invertir 13 billones de pesos.

El gobierno, a través del CONPES 4187, titulado “Declaración de importancia estratégica de los proyectos de inversión asociados al programa de fortalecimiento de las capacidades de la Fuerza Pública para afrontar los inminentes riesgos a la seguridad pública del país”, aprobó el 27 de marzo de este año recursos por 13 billones de pesos financiados con vigencias futuras a 8 años. Este CONPES que legalmente debe ser público, hoy es reservado y en la página del DNP solo aparece su portada y un comunicado de prensa.

Saber qué se va a adquirir con este CONPES es fundamental por dos motivos. El primero, los actores que ejercen violencia y delincuencia en el país, cambiaron, ya no hay guerrillas que quieran tomarse el poder o los paramilitares que “defiendan al Estado democrático”, eso se acabó, lo que queda desde 2016 es crimen organizado nacional y transnacional que manejan las grandes rentas del narcotráfico, la minería ilegal, el contrabando, la trata de personas, entre otras actividades criminales.



Lo segundo, hoy el Estado tiene una asimetría financiera y táctica desigual frente al crimen organizado actual. Mientras la Fuerza Pública gasta millones de dólares en tecnologías tradicionales como helicópteros y aviones de superioridad estratégica cuyo costo operativo es enorme, sin desconocer que pueden ser necesarios, los Grupos Armados Organizados (GAO) neutralizan estos activos operando en grupos de 3 a 4 personas utilizando drones comerciales de entre 500 y 1,500 USD. Esta disparidad ha hecho que la infraestructura militar y policial sea «porosa» ante ataques verticales. Por otro lado, hoy la Fuerza Pública intenta interceptar líneas telefónicas, mientras los criminales usan mensajería encriptada y tecnologías como internet satelital Starlin imposible de interceptar eficazmente con los equipos que tiene el Estado.

De acuerdo a una presentación extraoficial que me facilitaron del Consejo Superior de Política Fiscal -CONFIS-, titulada “Vigencias Futuras Excepcionales para la Seguridad Pública”, los 13 billones se distribuirán de la siguiente manera:

2. RESUMEN EJECUTIVO POR FUERZA / INSTITUCIÓN

Fuerza / Institución	Nº Proy.	Total 2027–2034	Part.	Vigencia pico
Ejército Nacional	6	COP 5.73 Billones	44.1 %	2031
Armada Nacional	8	COP 3.38 Billones	26.0 %	2031
Fuerza Aeroespacial	1	COP 1.57 Billones	12.0 %	2027–2030
Policía Nacional	4	COP 2.33 Billones	17.9 %	2031
GRAN TOTAL	19	COP 13.00 Billones	100 %	2031

* 2031 concentra la mayor inversión (~COP 3.0 Billones, 23 % del total), por maduración de contratos plurianuales.

Estos recursos, se destinarán principalmente, en el caso del Ejército, 5,2 billones para modernizar la flota de aeronaves, renovar armamento individual, equipos de protección del personal y actualizar las comunicaciones y sistemas de información; la Armada va a invertir 2,9 billones principalmente en la modernización de los buques, lanchas, patrulleras, aeronaves, armamento; la Policía invertirá los 2,33 billones en adquirir y mantener aeronaves, renovar el parque automotor, armamento y videovigilancia y finalmente la Fuerza Aeroespacial utilizará los 1,7 billones en renovar la flota de combate, transporte y entrenamiento de la FAC.

La pregunta que surge después de leer la información, hasta ahora conocida es ¿Si lo que se va adquirir con los 13 billones de pesos es lo que realmente requiere la Fuerza Pública en su conjunto, para enfrentar esta nueva criminalidad organizada nacional y transnacional que opera en nuestro país y en la región? Pareciera que la distribución de recursos respondió más bien al largo listado de necesidades que cada Fuerza presentó, sin que haya habido un trabajo coordinado de inversión estratégica conjunta para enfrentar el nuevo escenario creciente de violencia y delincuencia, generado por la criminalidad organizada.

El problema no es solo estratégico y táctico, es también económico, en la medida en que son tantas las necesidades y tan pocos los recursos, que hay que concentrarlos en la adquisición de equipos especializados y en el fortalecimiento de unidades conjuntas, que marquen la diferencia y recuperen la capacidad de combate y garantía de seguridad de la Fuerza Pública, frente a la criminalidad actual.



Compra de 17 aviones de combate suecos Saab JAS 39 Gripen

El 14 de noviembre del año pasado se firmó el contrato entre el Gobierno de Colombia y la empresa sueca Saab para la compra de 17 aviones Gripen, catalogados como lo último en tecnología, los cuales reemplazarán a la antigua flota de aviones Kfir de la Fuerza Aeroespacial Colombiana (FAC).

El valor aproximado de este contrato es de 16,7 billones de pesos (unos 3.600 millones de dólares). De acuerdo con la Contraloría General de la Nación el esquema de pago del Gobierno con la empresa sueca SAAB se estructuró en un anticipo (40 %) pagadero en seis cuotas entre 2026 y 2031. El saldo excedente del 60 % se desembolsará contra entrega de las aeronaves entre 2028 y 2032, es decir que más del 70% del valor de este contrato, tendrá que ser desembolsado por el gobierno de Abelardo De La Espriella[1].

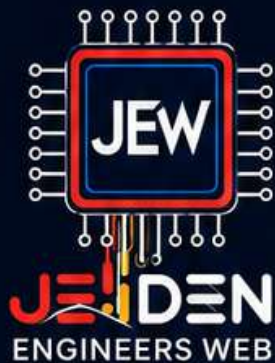
Y los drones en camino

El gobierno afanado por los pésimos resultados de la seguridad en todo el territorio y por la amenaza creciente del uso de drones con explosivos por parte de los grupos armados ilegales, presionó la compra rápida de un escudo antidrones por \$6,2 billones, que se financiará a mediano plazo por el mecanismo de vigencias futuras para asegurar el presupuesto total.

Este proyecto inició con una primera fase de \$1 billón, que se comenzó a ejecutar a finales del año pasado con la adquisición, por parte del Ministerio de Defensa, de sistemas de contramedidas antidrón (C-UAS) por un valor de 25,3 millones de dólares con la compañía estadounidense Dedrone Tactical. Estos equipos están destinados a la vigilancia y protección de las bases del Ejército y la Fuerza Aeroespacial frente al uso de drones con explosivos por parte de grupos armados ilegales. En la actualidad se gestiona otro contrato de similares características por más de 800 mil millones de pesos, con empresas de EE UU y de la India.

La pregunta que surge frente a este proyecto de inversión es ¿Se van a invertir más de 6 billones de pesos en sistemas de defensa antidrones o es necesario utilizar parte de estos recursos para pasar a la ofensiva con drones armados, para enfrentar a los grupos armados ilegales que hoy utilizan drones con explosivos, que le han quitado a la Fuerza Pública el monopolio casi absoluto del espacio aéreo?

[1] La Opinión. "Contraloría revela detalles del multimillonario contrato de los 17 aviones Gripen" Enero de 2026. <https://laopinion.co/colombia/contraloria-revela-detalles-del-multimillonario-contrato-de-los-17-aviones-gripen>



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

Frente a esta pregunta, el Derecho Internacional Humanitario (DIH) no solo responde con un rotundo Sí, sino que revela una paradoja crucial: en el contexto de la guerra asimétrica colombiana, el uso de drones de ataque sería, en muchos casos, la opción militar más ética y precisa disponible.

Lejos de ser “robots asesinos” indiscriminados, los drones, operados bajo una doctrina estricta, refuerzan los pilares del DIH de distinción, proporcionalidad y precaución de una manera que las armas convencionales a menudo no pueden. En términos de distinción, un dron ofrece una vigilancia persistente. Permite a un operador observar un objetivo durante horas, asegurando la identificación positiva de que es un combatiente legítimo y no un civil. Es la diferencia entre disparar a coordenadas en un mapa con un mortero y apuntar con certeza a un blanco verificado.

En relación con la proporcionalidad, el dron utiliza un bisturí quirúrgico, mientras que otros usan un mazo. Permite el uso de municiones pequeñas y precisas para neutralizar una amenaza específica sin causar el devastador daño colateral de una bomba aérea o el fuego de artillería.

Frente a la precaución, la capacidad de un dron para abortar un ataque en el último segundo si un civil entra en escena, es una salvaguarda que casi ningún otro sistema de armas ofrece. Reduce el riesgo para los no combatientes y para las propias tropas, y así evita asaltos frontales de alto riesgo.

El enemigo ya está usando esta tecnología sin restricción alguna ética ni legal. La vacilación estatal, no sería una muestra de superioridad moral; podría interpretarse como una renuncia a la responsabilidad estatal, de proteger a los ciudadanos y a nuestros soldados y policías.

Estos son algunos de los compromisos adquiridos por 36 billones de pesos por el gobierno actual, sin tener en cuenta la construcción de la nueva sede del Ministerio de Defensa, que se tendrá que realizar en algún momento. Inversiones todas, que el nuevo gobierno, a excepción del contrato de los aviones Gripen, podrá reorientar o tomar decisiones de fondo de acuerdo con los recursos disponibles y con base en los requerimientos técnicos y humanos para enfrentar el crimen organizado nacional y transnacional que opera en nuestro territorio y a nivel regional. Hoy, el verdadero obstáculo no es la ley ni la tecnología, es la falta de recursos, de visión, comprensión de los problemas de violencia y delincuencia actuales y la parálisis en la toma de decisiones en el liderazgo político, militar y policial.





FERIA INTERNACIONAL
DE SEGURIDAD

26 AL **28**
AGOSTO 2026
›CORFERIAS‹

INTEGRACIÓN DE TECNOLOGÍAS GLOBALES

**UN SOLO LUGAR PARA DECISIONES
ESTRATÉGICAS EN SEGURIDAD**



Conocimiento experto



Tecnología integrada



Networking especializado

REGÍSTRESE AQUÍ



**MÁS INFORMACIÓN
EN SECURITYFAIRCOLOMBIA.COM**



PLAN

FRENO

Seguridad que nos mueve

En la Dirección de Tránsito y Transporte trabajamos por la seguridad vial de los conductores de servicio de **carga** y **transporte de pasajeros**.

Conductores de transporte de pasajeros: #NoMasExcusasEnLaVía



Revise y mantenga en óptimas condiciones el **sistema de frenos** de su vehículo.



Un buen freno puede **salvar** muchas **vidas**.



Revise periódicamente pastillas, bandas, discos, líquido de frenos y sistema de aire.



Realice el mantenimiento preventivo en talleres autorizados.



Al conducir, mantenga la distancia de seguridad y evite maniobras bruscas.



Su responsabilidad protege su vida, la de sus pasajeros y la de los demás.

frene, revise y continúe su viaje. La prevención es la mejor ruta para llegar seguro a su destino.





Comprometidos con un Transporte Seguro

En la terminal de transporte trabajamos juntos
por la **seguridad** de conductores, pasajeros
y todos los actores viales.



#NoMasExcusasEnLaVía



Cada viaje comienza con un **compromiso**:
conducir con **responsabilidad** para llegar seguros a destino.





¡Viaje seguro, elija transporte legal!



✓ **Compre sus tiquetes** únicamente en las terminales de transporte o canales autorizados.



✓ **Verifique** que el vehículo pertenezca a una empresa legalmente habilitada.



✓ **No acepte** ofertas de transporte realizadas en la calle o por personas no autorizadas.



✓ **Llegue con anticipación** a la terminal para organizar su viaje de manera segura.



✓ **Proteja su vida** y la de su familia utilizando siempre transporte formal.



#NoMasExcusasEnLaVía

