VENEZUELA, MARZO DE 2026 - AÑO 1 - NÚMERO 2

SEGURIDAD en acción VENEZUELA

CÓMO TU FORMA DE VER EL MUNDO DEFINE TU SEGURIDAD

PAG. 20-23

LA SEGURIDAD PATRIMONIAL DEL SIGLO XXI

PAG. 4-7

CUANDO EL BIT SE CONVIERTE EN ÁTOMO

PAG. 39-40

HASTA QUE PUNTO PUEDE INCOMODARNOS LA TECNOLOGÍA?

PAG. 11-13

Adolfo M. Gelder

EDITORIAL

Resiliencia y Estrategia en un entorno en cambio

Bienvenidos a esta segunda edición de Seguridad en Acción Venezuela. Tras el éxito de nuestro lanzamiento, regresamos con el firme compromiso de seguir profesionalizando la cultura de la seguridad en nuestro país, bajo el respaldo regional de nuestra casa matriz en Bolivia y nuestra red LATAM.

Este primer trimestre del 2026 nos ha recordado que la seguridad no es un estado estático, sino un proceso dinámico de adaptación. Los sucesos del pasado sábado 3 de enero marcaron una pauta importante en la dinámica nacional; en estas páginas, analizamos lo ocurrido no desde la noticia, sino desde la lección aprendida, ofreciendo recomendaciones de seguridad situacional diseñados específicamente para el entorno venezolano actual, donde la prevención es nuestra mejor herramienta de defensa.

Mirando hacia el futuro inmediato, nos preparamos para el asueto de Semana Santa. En esta edición, compartimos una guía exhaustiva de recomendaciones para que tanto ciudadanos como empresas aseguren sus activos y su integridad durante los primeros días de abril. La seguridad en vacaciones no es un lujo, es una planificación estratégica.

Además, en nuestro afán por cubrir los pilares de la seguridad integral, presentamos secciones especializadas en: Seguridad Laboral e Industrial: Estrategias para mitigar riesgos en la operatividad diaria, garantizando que el talento humano sea siempre el recurso más protegido.

Seguridad Informática: Un balance del primer trimestre en materia de ciberamenazas. En un mundo hiperconectado, la blindaje digital es la base de la continuidad de cualquier negocio en 2026.

Esta edición es una invitación a pasar del diagnóstico a la acción. Los invito a profundizar en cada artículo, a debatir las ideas y, sobre todo, a implementar estos conocimientos en sus organizaciones y hogares.

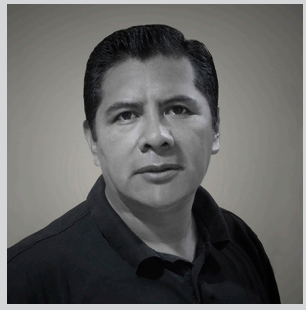
Desde Venezuela, con visión latinoamericana, seguimos construyendo un entorno más seguro para todos.

¡Bienvenidos a la acción!

STAFF

HUMBERTO COPA G.
DIRECTOR GENERAL

LUCIEL RIOS CAMACHO,
COORDINADORA ACADÉMICA Y OPERATIVA



DAVID CORONEL CLAURE
EDICIÓN Y PRENSA

Seguridad en Acción VENEZUELA es una revista especializada en seguridad integral, abordando temas de seguridad corporativa, industrial, electrónica, cibernética y personal.

CONTENIDO

LA SEGURIDAD PATRIMONIAL DEL SIGLO XXI

Despertando antes del amanecer

En el vertiginoso tablero de juego que es el mundo de hoy, la seguridad patrimonial ya no puede darse el lujo de ser el "bombero" que llega solo cuando las llamas consumen el edificio. ¡No! La seguridad del siglo XXI es el estratega que predice dónde y cómo podría encenderse el fuego, y lo evita. Es una disciplina proactiva, un vigía constante que no espera la tormenta, sino que lee el viento para anticiparla. Esta metamorfosis crucial se logra tejiendo hilos de sabiduría antigua con la agudeza moderna: desde la conciencia situacional hasta las lecciones del Rinoceronte Gris y el Cisne Negro, pasando por la Teoría del Lastre Organizacional y las sempiternas enseñanzas de Sun Tzu. Juntas, estas ideas nos permiten construir un escudo impenetrable, hecho de previsión y no de reacción.

Conciencia Situacional:

El Sexto Sentido de la Protección

Imagina que eres un capitán en medio del mar, la conciencia situacional es la capacidad que tienes de leer el clima, las corrientes, la profundidad y hasta el estado de ánimo de tu tripulación. En el mundo de la seguridad patrimonial, es ese "sexto sentido" que te permite no solo ver lo que pasa, sino entender por qué. Va más allá de las cámaras y los sensores; es la inteligencia que te dice si esa pequeña anomalía en el sistema de repente se volverá un problema gigante, o si un cambio en el vecindario podría traer nuevas amenazas.

UN EQUIPO CON BUENA CONCIENCIA SITUACIONAL

Es como un ajedrecista que piensa varias jugadas por delante.

Pueden:

- **Oler el peligro**
  Detectar patrones, captar señales débiles y adelantarse a posibles incidentes antes de que se materialicen.
- **Ajustar la brújula**
  Cambiar de rumbo en tiempo real cuando las condiciones lo exigen, manteniendo la seguridad siempre afinada.
- **Decidir en caliente y con cabeza fría**
  Actuar con rapidez y precisión, minimizando el daño cuando lo inevitable ocurre.

El Rinoceronte Gris y el Cisne Negro:

Preparados para lo Obvio y lo Inaudito

Cuando hablamos de riesgos, es vital diferenciar entre lo que sabemos que viene y lo que nos toma por sorpresa.

El Rinoceronte Gris: El Elefante en la Sala que Nadie Quiere Ver.
Un rinoceronte gris es un evento muy probable con un gran impacto que se descarta o se pasa por alto, tal vez porque no lo estamos tomando lo suficientemente en serio. El término fue acuñado por la autora de «The Gray Rhino», Michele Wucker, para referirse a un peligro que es obvio, visible y nos afecta directamente.

Piensa en ese riesgo enorme, con el que ya convives y que, en el fondo, sabes que te va a embestir. Es un rinoceronte gris. Este podría ser un sistema de seguridad anticuado, una brecha de ciberseguridad conocida que se ha pospuesto por "prioridades" o el aumento de la delincuencia en la zona que, por alguna razón, no se ha abordado con la seriedad que merece. Ser proactivo aquí significa no esperar a que el rinoceronte cargue, es ponerle barreras, desviar su camino, es actuar antes de que cause estragos. Es realizar acciones de mitigación y anulación de daños en base sobre lo que ya sabemos.

El Cisne Negro: La Sorpresa Monumental.
La teoría del cisne negro, Fue desarrollada por el filósofo e investigador libanés Nassim Taleb. Es la teoría que nos habla de ese evento que, hasta que sucede, parece imposible de suceder. Un cisne ne-

gro es algo tan improbable y con un impacto tan descomunal que, cuando ocurre, nos hace exclamar: "¿Quién lo hubiera imaginado?". Solo después, en retrospectiva, intentamos construir una explicación lógica. En seguridad, podría ser un ciberataque de proporciones bíblicas nunca antes visto, o el robo de una información ultra-secreta por un método tan ingenioso que desafía toda imaginación. Dado que no podemos predecirlos, la proactividad aquí no es evitarlos, sino construir una organización a prueba de golpes. Es como tener un "plan B" para tu "plan B", asegurándote de que tu negocio pueda seguir funcionando incluso si el mundo se pone patas arriba. Se trata de ser flexible, de aprender de cada tropiezo y de tener la piel dura.

La Teoría del Lastre (Organizacional): Limpiando la Casa para que Siga Brillando

Aquí entra una idea poderosa que nace de mis experiencias en el sector gubernamental, así como privado y que he comprobado y afianzado en el ámbito de la seguridad privada, llegando a postularla desde entonces como; la Teoría del "Lastre"(Organizacional), Imaginemos una embarcación que navega hacia su destino; si esta embarcación lleva demasiado peso muerto —objetos que no aportan ni contribuyen a la navegación—, su velocidad disminuye, su estabilidad se compromete y su capacidad de maniobra se reduce. En una organización, este peso muerto se manifiesta en aquellas personas que, sin importar su cargo o posición, no suman sino que restan.

La Teoría del" Lastre"(Organizacional), postula que en toda organización existen individuos o grupos cuya presencia y comportamiento actúan como un peso muerto que ralentiza, obstaculiza o incluso hunde el desempeño colectivo. Estos "lastres" no contribuyen al logro de los objetivos comunes, sino que restan valor mediante la falta de compromiso, resistencia al cambio, bajo rendimiento, deslealtad o sabotaje activo o pasivo. Al igual que un barco cargado con peso innecesario pierde velocidad y maniobrabilidad, una organización con lastres internos enfrenta dificultades para avanzar, innovar y mantener estándares de seguridad y eficiencia.
Identificar a este "Lastre"(Organizacional), manejarlo con firmeza y justicia es vital. No solo son un riesgo directo (pueden robar, filtrar información), sino que su presencia es como una enfermedad silenciosa que carcome la moral y la confianza del equipo. Una seguridad proactiva mira hacia adentro con la misma atención que mira hacia afuera, esto significa tener controles internos claros, fomentar una cultura de ética, lealtad y una gestión que se atreva a tomar decisiones difíciles cuando la seguridad de la organización está en juego.

El Arte de la Guerra de Sun Tzu:

Estrategia milenaria para la seguridad moderna

Las palabras de Sun Tzu, escritas hace milenios, resuenan con una claridad asombrosa en la seguridad patrimonial del siglo XXI. Es el "manual" definitivo para ser más zorro que conejo:
"Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca saldrás derrotado".

Esta es la columna vertebral. Significa entender a fondo a quiénes intentan dañarte (los ciberdelincuentes, los ladrones, la competencia desleal) y, a la vez, conocer al milímetro tus propias fortalezas y, sobre todo, tus debilidades. Solo así sabrás dónde poner tus defensas.

"La excelencia suprema consiste en romper la resistencia del enemigo sin luchar".

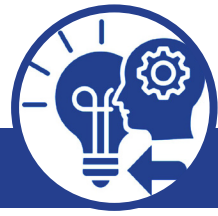
¿No es esto la prevención en su máxima expresión? La meta no es atrapar al ladrón, sino hacer que tu empresa sea un objetivo tan difícil que el ladrón ni se acerque. Una buena disuasión, un sistema de alarma impecable, una presencia de seguridad visible y una reputación de "intocable".

"La velocidad es la esencia de la guerra".

En seguridad, cada segundo cuenta. Si algo pasa, ¿qué tan rápido puedes detectarlo y qué tan ágil eres para responder? Los planes de contingencia deben ser tan flexibles como un bailarín y la capacidad de reacción, casi instantánea.

"Todo el arte de la guerra se basa en el engaño".
No se trata de mentir, sino de ser impredecible y astuto. Variar tus rutinas de seguridad, implementar medidas que confundan a los posibles atacantes, o simplemente hacer que tus defensas parezcan más robustas de lo que esperan.

"Victorioso es aquel que sabe cuándo luchar y cuándo no luchar".
Esto se traduce en ser inteligente con tus inversiones en seguridad. No se trata de gastar sin medida, sino de proteger lo más valioso de la manera más eficiente, enfocándose en los riesgos que tendrían un mayor impacto si se materializan.



La Gran Sinfonía de la Proactividad

Una vez que; logramos que todas estas ideas se conjuguen y bailen juntas, la seguridad patrimonial se transforma en una sinfonía de anticipación y resiliencia.

Afinar el radar.
Desarrollar esa conciencia situacional a través de la inteligencia, el monitoreo constante y una cultura donde todos son "ojos y oídos"

Domar los "Rinocerontes Grises".
Identificar y neutralizar esas amenazas obvias y conocidas antes de que causen un desastre dentro de la organización. Es arreglar el techo antes de que llueva a cántaros.

Blindarse contra los "Cisnes Negros".
Construir una organización con músculos para resistir lo inesperado. Tener planes de respaldo, sistemas flexibles y la capacidad de reinventarse cuando el panorama cambia radicalmente.

Limpiar la casa del "Lastre".
Asegurarse de que cada pieza de tu organización suma, identificando y gestionando a quienes restan o representan un riesgo interno.

Jugar como Sun Tzu.
Planificar con astucia, disuadir con inteligencia, conocer cada rincón de tu campo de batalla y actuar con la rapidez y la sabiduría de un maestro estratega.

Al ensamblar estas piezas, la seguridad patrimonial se eleva de ser un gasto necesario a convertirse en un motor de valor, un guardián silencioso que protege no solo los activos, sino la continuidad, la reputación y el futuro de la organización. Porque la verdadera seguridad no se trata de apagar incendios; se trata de evitar que se enciendan.

My.Marcos Carrillo Castillo
Oficial retirado del Ejército de Venezuela.

Consultor Estratégico en Seguridad y Protección Patrimonial.

El sesgo que debilita nuestra capacidad de reaccionar:

Cuando el peligro se vuelve rutina

¨Las personas no huyen de la realidad, se adaptan a ellas cuando no encuentran como cambiarla"

Sigmund Freud.

La sirena de la ambulancia, ni un grito lo que alertó a la comunidad.

Fue el silencio.

Las luces seguían encendidas, las puertas cerradas, la vida continuaba. Nadie salió. Nadie preguntó. Nadie llamó. No porque no hubiera ocurrido algo, sino porque ya no parecía urgente.

En muchos entornos sociales actuales, la inseguridad no siempre se presenta como un hecho excepcional. A veces ocurre algo más complejo y peligroso: se vuelve parte de la rutina. Cuando esto sucede, no solo se transforma el contexto, también cambia la conducta de las personas y su forma de responder ante el riesgo.

Este fenómeno no responde a la indiferencia ni a la falta de valores. Está profundamente ligado a cómo el ser humano se adapta psicológica y conductualmente a la exposición constante al peligro.

Frente a este escenario: se presentan los casos particulares donde la repetición de situaciones de riesgo —robos, amenazas, violencia, estafas o hechos irregulares— va perdiendo impacto emocional con el tiempo. Aquello que antes generaba alarma inmediata comienza a percibirse como algo "normal".

Expresiones como: "sigue de largo que no es tu problema", "mejor no involucrarse", "eso pasa siempre" o "no vale la pena alertar" se incorporan de forma natural al discurso cotidiano. Esta normalización no surge de una decisión consciente, sino de un proceso de adaptación.

El problema es que adaptarse al peligro no lo elimina. Solo reduce la capacidad de detectarlo y responder a tiempo.

Por qué ocurre el sesgo de normalización del riesgo:

Desde una mirada jurídica y conductual, este fenómeno puede explicarse a través del sesgo de normalización del riesgo. En términos simples, ocurre cuando la mente, para protegerse del desgaste emocional constante, deja de percibir como urgente aquello que se repite con frecuencia.

El ser humano no está diseñado para vivir en estado permanente de alerta. Ante la exposición prolongada al peligro, el cerebro ajusta sus mecanismos de respuesta para poder seguir funcionando. El riesgo continúa existiendo, pero deja de activar una reacción inmediata.

Este sesgo genera una falsa sensación de control: la persona cree que domina la situación porque logra convivir con ella, cuando en realidad ha reducido su capacidad de respuesta y autoprotección.
lo que revela este fenómeno en la conducta social es que la normalización del riesgo no es un problema individual aislado. Es un fenómeno colectivo que impacta directamente en la seguridad ciudadana y en la eficacia de cualquier sistema de prevención.

Cuando el peligro deja de ser percibido como tal:

1. Se debilita la denuncia.
2. Se reduce la alerta comunitaria.
3. Se incrementa la vulnerabilidad de quienes están más expuestos.
4. Se consolida la idea de que "no hay nada que hacer".

Desde una perspectiva jurídica, este proceso erosiona la corresponsabilidad social. La seguridad deja de entenderse como un derecho que requiere participación activa y se transforma en una carga que cada persona gestiona en soledad.

El impacto en la conducta cotidiana:

Este sesgo se manifiesta en conductas aparentemente pequeñas, pero con efectos acumulativos importantes:

1. No alertar ante situaciones sospechosas.
2. Evitar intervenir incluso cuando alguien necesita ayuda.
3. No denunciar por considerar que el esfuerzo será inútil.
4. Ajustar la vida diaria al peligro en lugar de reducirlo.

Estas respuestas no nacen del desinterés, sino del agotamiento emocional. Sin embargo, el resultado es el mismo: mayor exposición al riesgo y menor capacidad de prevención.

La seguridad no depende únicamente de normas o instituciones. También depende de cómo las personas perciben el peligro y deciden actuar frente a él.

El ser humano no está diseñado para vivir en estado permanente de alerta.

RECOMENDACIONES
CLARAS Y APLICABLES

Hablar de sesgos son aquellos que deben ir acompañado de propuestas realistas que permitan recuperar la capacidad de respuesta sin generar miedo excesivo.

PARA LA CIUDADANÍA:

Identificar cuándo una situación peligrosa ha sido normalizada.

Recuperar pequeñas alertas cotidianas sin caer en la paranoia.

Fortalecer la comunicación básica entre vecinos y entornos cercanos.

Educar en prevención desde el hogar, con información clara y adecuada a cada edad.

PARA EL ENTORNO COMUNITARIO E INSTITUCIONAL:

Hay que Promover mensajes constantes y comprensibles sobre prevención, también se debe Enfocar la seguridad desde la conducta y no solo desde la norma.

Generar confianza para que la denuncia vuelva a percibirse como una herramienta útil. La prevención comienza cuando el riesgo vuelve a ser reconocido como tal.

El mayor peligro no es el miedo, El mayor peligro es acostumbrarse a él.

Cuando el riesgo deja de incomodarnos, dejamos de protegernos. Recuperar la capacidad de reacción no implica vivir en alerta permanente, sino volver a mirar aquello que habíamos dejado de ver.

La seguridad comienza cuando la normalidad deja de justificar el peligro.

Un estudio sobre conducta social y riesgo asevera que cuando ese se vuelve cotidiano, deja de percibirse como amenaza y debilita nuestra capacidad de reaccionar.

Abogado
Leila Castillo
Perfilación criminal y análisis conductual aplicado a la seguridad ciudadana.

¿HASTA QUE PUNTO PUEDE INCOMODARNOS

LA TECNOLOGIA?

LA RESISTENCIA AL CAMBIO ES LA RESISTENCIA A LA PROPIA EVOLUCION, FLUYE CON LA TRANSFORMACION

No tenemos que esperar a que suceda una crisis en el departamento ya sea un robo de datos, que se infecten las computadoras con un virus que dañe la información, podemos hacer los cambios antes de que sucedan estos inconvenientes o como la frase de Deepak Chopra “Todos los grandes cambios están precedidos por el caos “

La primera gran amenaza que enfrenta la seguridad en el departamento de RRHH es la resistencia al cambio, en todas las empresas siempre encontramos gente de todas las edades integrando nuestro maravilloso talento humano que es el alma de toda organización por mucho tiempo no representaba ningún problema ya que se impartían capacitaciones informales o formales para gran cantidad de personas sin necesidad de una gran inversión y sin requerir ayuda externa; que pasa en el momento que los procesos deben cambiar y no solo la manera en que se realizan, nos referimos a integrar tecnología en dichos procesos, en la mayoría de

los casos se encuentran con una pared a la que llamamos RESISTENCIA AL CAMBIO y con las famosas frases que la acompañan:

- “No tenemos tiempo”
- ” No tenemos suficiente ayuda“
- “Déjame pensarlo“
- “Es un cambio muy radical“

CAPACITAR PARA EVOLUCIONAR

Y mi favorita “Siempre se ha hecho así”, la primera vez que escuche esta frase estaba en mis veintes y me lo dijo una compañera que tenía más de treinta años en una institución, a lo que le respondí porque siempre se haya hecho así no quiere decir que este bien o que no lo podemos mejorar, pero les adelanto que labore seis años con ella y nunca cambio sus actividades o aprendió algo nuevo, ignorando las sugerencias de sus compañeros para aprender otros procesos y ascender a otro cargo.

El cambio asusta y te saca de tu área de confort, pero es necesario para evolucionar, para adaptarse a la sociedad y para ser independiente desde manejar el internet, manejar un teléfono inteligente, y se entiende para las personas que no nacimos con la tecnología es a veces abrumador, pero se debe hacer de la manera apropiada, sin dejar o ignorar a las personas.
Como debemos hacer para que las personas se adapten a los cambios de la tecnología sin levantar un muro que no les permita aprender y así evolucionar en su carrera y favorecer los ideales de la empresa o de la institución, capacitando al personal sobre la tecnología que adoptara la empresa para los procesos de manera muy profesional sin descartar al personal que ya posee la empresa , capacitarlos no solo en tecnología sino los peligros que conlleva esa el uso de la tecnología en la empresa, cursos sobre el buen uso de las pc o laptop que usan en su área laboral, podría decirse que en el 80 por ciento de las empresas venezolanas no entrenan a su personal cuando empiezan en un puesto dentro de la organización desde a que

La verdadera ignorancia no es la ausencia de conocimientos sino el hecho de rehusarse a adquirirlos

se dedican, su misión, visión, objetivos solo le entrega una serie de documentación el primer día lo llenan, lo entregan y a trabajar, y después los jefes porque no son lideres se quejan de que le preguntan al empleado a que se dedican y no saben como lo van a saber si nunca la organización se preocupo por integrar a esa persona al talento humano de la empresa, de allí parte toda la idea desde la capacitación hasta el buen uso de los equipos es por falta de capacitación. Se debe entrenar al personal desde el principio no solo cuando se implementa un nuevo sistema en la organización para que se alinee con los objetivos de la empresa, pero es todo lo contrario quieren que la persona ya ingrese con la experiencia en los sistemas y totalmente formada para no invertir en ella, para disfrutar de los frutos tienes que sembrar primero. Parte de la capacitación debe ser cursos de cómo usar los equipos no utilizar pendrive en la pc o en la laptop ya que pueden contener virus e infectar y dañar los archivos, mantener siempre respaldo de la información, poseer discos extraíbles para las bases de datos mas importantes y los archivos mantenerlos con claves confidenciales e igual que la computadora mantenerla con las claves personales ya que toda la información del departamento es primordial e importante y muy tentadora para los cibercriminales que se aprovecharan de las vulnerabilidades de la organización para sacar provecho monetario.

Desiree da Silva

Tendencias y Evolución de los Delitos contra la Propiedad

EN EL ÁMBITO CORPORATIVO EN LATINOAMÉRICA

(Análisis 2025)

El año 2025 ha confirmado una transformación profunda en el panorama de riesgos patrimoniales para las corporaciones en los países de habla hispana. La convergencia de factores económicos volátiles, avances tecnológicos exponenciales y la sofisticación del crimen organizado ha redefinido las amenazas contra los activos tangibles e intangibles de las empresas. Este artículo presenta un análisis integral de las tendencias observadas, ofrece una reseña comparativa entre las principales economías de la región, evalúa los niveles de riesgo, enumera los delitos predominantes y propone un marco estratégico basado en tecnología, talento humano y gestión preventiva para construir una seguridad corporativa resiliente.

1. Reseña Comparativa entre Países: Un Mosaico de Riesgos

El impacto de los delitos contra la propiedad corporativa no es homogéneo en la región. Las diferencias en marcos legales, capacidades de investigación, penetración tecnológica y contextos socioeconómicos crean escenarios distintos.

- **México y Colombia:** Enfrentan los niveles más altos de riesgo convergente. Predominan los delitos de extorsión a gran escala, secuestro y Robo de carga en corredores logísticos y robo de hidrocarburos/mercancías con presunta connivencia de actores internos. La influencia del crimen organizado transnacional eleva la violencia y la complejidad de los ataques.

- **Argentina y Chile:** Presentan un perfil de riesgo alto en delitos financieros y cibernéticos, pero moderado en delitos físicos violentos. En Argentina, el fraude interno, la falsificación documental y el robo de metales preciosos (especialmente cobre) son predominantes.
- **Chile** muestra una alta tasa de robos en cadenas de retail y farmacéuticas, junto con un crecimiento significativo del fraude corporativo y el robo de información intelectual.
- **España:** Si bien con índices generales de delincuencia menor, sufre un alto impacto por delitos de "cuello blanco": fraude bursátil, malversación de fondos, corrupción privada y espionaje industrial. Es el país de la región con mayor incidencia de ciberdelitos sofisticados contra la propiedad intelectual.
- **Perú y Ecuador:** Riesgo medio-alto, focalizado en la minería ilegal que afecta a concesiones corporativas, el robo de concentrados minerales y el asalto a camiones de transporte de valores. La corrupción en puertos y aduanas es un factor agravante común.
- **Centroamérica (Guatemala, Honduras, El Salvador):** Riesgo alto por extorsión a PYMEs y corporaciones, y robo de carga en tránsito. Los avances en seguridad ciudadana no se han traducido plenamente en una reducción del riesgo corporativo patrimonial.

2. Niveles de Riesgo Analizados (2025)

- **Riesgo Crítico (Alta Probabilidad / Alto Impacto):** Robo de carga en tránsito (México, Colombia, Centroamérica); Fraude interno y malversación (toda la región); Ciberataques para extorsión (Ransomware) y robo de datos.
- **Riesgo Alto (Media Probabilidad / Alto Impacto):** Extorsión y secuestro virtual de ejecutivos; Sabotaje industrial y robo de maquinaria; Hurto en centros de distribución (Retail).
- **Riesgo Medio (Alta Probabilidad / Impacto Medio):** Robo hormiga y peculado por empleados; Falsificación de productos; Daños a la propiedad por conflictos sociales.
- **Riesgo Emergente (Probabilidad en Crecimiento):** Fraude con Inteligencia Artificial (deepfakes "falsedades profundas" son archivos de vídeo, imagen o voz manipulados mediante un software de inteligencia artificial, para autorizaciones fraudulentas); Robo de materiales críticos para la transición energética (litio, tierras raras); Criptodelitos para lavar activos provenientes del robo corporativo.

3. Principales Delitos Contra la Propiedad en el Ámbito Corporativo (2025)

1. Fraude Interno y Malversación de Fondos: Sigue siendo el delito de mayor impacto económico. Incluye esquemas de facturación falsa, desvío de pagos y apropiación indebida de activos.

2. Robo de Carga y Cadena de Suministro: Desde el asalto a camiones hasta el contrabando en puertos. La falta de visibilidad en "la última milla" es la principal vulnerabilidad.

3. Ciberdelitos Patrimoniales: Ransomware (secuestro de datos y sistemas), Fraude del CEO/BEC (suplantación para transferencias fraudulentas) y robo de Propiedad Intelectual y datos sensibles.

4. Extorsión y Secuestro Virtual: Amenazas contra directivos o ataques DDoS (Denegación de Servicio Distribuido) es un ciberataque que satura un servidor, sitio web o red con tráfico masivo desde múltiples fuentes) a sistemas productivos para exigir pagos en criptomonedas.

5. Hurto en Establecimientos Comerciales y Retail: Organizado por bandas que atacan inventarios de alto valor.

6. Sabotaje y Robo de Activos Productivos: Robo de cableado de cobre, maquinaria y componentes tecnológicos para su reventa.

7. Falsificación y Piratería: Afecta marcas, productos farmacéuticos y software, erosionando ingresos y reputación.

4. La Tecnología como Medio de Mitigación

La tecnología ha dejado de ser solo una barrera para convertirse en un facilitador de inteligencia predictiva y respuesta ágil.

- **Inteligencia Artificial y Machine Learning:** Análisis predictivo de patrones delictivos en la cadena de suministro. Detección de anomalías en transacciones financieras para identificar fraude en tiempo real.
- **Plataformas de IoT (Internet de las Cosas) y Sensores:** Geolocalización y monitorización en tiempo real de contenedores y camiones. Sensores en perímetros que diferencian amenazas de falsas alarmas.
- **Ciberseguridad Avanzada:** Soluciones de Zero-Trust, EDR (Detección y Respuesta en Endpoints) y SOAR (Orquestación, Automatización y Respuesta de Seguridad) para contener ciberataques rápidamente.
- **Analítica de Video con IA:** Cámaras que reconocen comportamientos sospechosos (ej.: merodeo, vehículos recurrentes), objetos abandonados o desvíos de ruta en almacenes.
- **Blockchain para la Cadena de Custodia:** Trazabilidad inmutable de mercancías desde el origen hasta el consumidor final, reduciendo el espacio para el fraude y el desvío.

5. El Talento Humano de la Seguridad Integral y su Gestión

La tecnología es inútil sin el capital humano capacitado para interpretarla y actuar.

- **Perfiles Demandados:** Ya no solo vigilantes. Se buscan Analistas de Riesgo, Investigadores Corporativos Digitales, Gestores de Continuidad del Negocio, Especialistas en Ciber-Física (que unen OT y IT) y Profesionales en Inteligencia de Amenazas.
- **Formación Continua:** En ciber-higiene, respuesta a incidentes y legislación local.
- **Cultura de Seguridad:** Involucrar a todos los empleados como el primer eslabón de la defensa (reporte de incidentes, phishing).
- **Integración Departamental:** La seguridad física, la ciberseguridad, el cumplimiento normativo (compliance) y los recursos humanos deben trabajar en equipos multidisciplinares.
- **Bienestar y Ética:** Proteger al personal de seguridad de la corrupción y el burnout (estado de agotamiento físico, emocional y mental causado por estrés laboral crónico), fomentando un entorno ético.

6. Medidas Preventivas Integrales

1. Evaluación de Riesgo Dinámica: Realizar auditorías periódicas que consideren el contexto cambiante.

2. Protección por Capas (Defensa en Profundidad): Combinar medidas perimetrales, control de accesos (biométrico), vigilancia activa, ciberseguridad y procedimientos de respuesta.

3. Plan de Continuidad del Negocio y Recuperación ante Desastres: Tener protocolos probados para recuperar operaciones tras un incidente grave (ej.: ataque ransomware, robo masivo).

4. Due Diligence y Controles Internos: Verificación exhaustiva de empleados, socios y proveedores. Separación de funciones y dobles firmas para transacciones críticas.

5. Cooperación Público-Privada: Participar en cámaras sectoriales de seguridad e intercambiar información de inteligencia (anónima) con autoridades competentes.

7. Países Más Afectados en 2025 (Ranking por Impacto Agregado)

1. México: Por volumen, violencia y diversidad de delitos (carga, extorsión, fraude, ciberataques).

2. Colombia: Por la sofisticación del crimen organizado en logística y la alta tasa de extorsión empresarial.

3. Argentina: Por la magnitud económica del fraude corporativo y los delitos financieros.

4. España: Por el alto valor de los activos intelectuales y financieros atacados mediante ciberdelitos y fraudes complejos.

5. Chile: Por la creciente ola de robos violentos a retail y el aumento sostenido del cibercrimen.

8. Recomendaciones Estratégicas

- **Adoptar un Enfoque de "Seguridad Convergente":** Integrar físico, lógico y humano en una única gobernanza.
- **Invertir en Inteligencia, no solo en Reacción:** Destinar recursos a plataformas de analítica predictiva y monitoreo de amenazas.
- **Priorizar la Protección de Datos:** Considerar los datos como el activo más crítico. Implementar cifrado y copias de seguridad inalterables.

- **Desarrollar un Programa Robusto de Ética y Cumplimiento:** Es la barrera más eficaz contra el fraude interno.
- **Realizar Simulacros Regulares:** Ensayar la respuesta ante un secuestro de carga, un ciberataque masivo o una investigación fraudulenta.

Conclusión

El año 2025 ha dejado claro que la seguridad corporativa patrimonial exige una evolución desde la protección estática hacia la resiliencia dinámica. Los delitos son cada vez más híbridos, explotando la fisura entre lo físico y lo digital. El éxito no radicará únicamente en adquirir la tecnología más avanzada, sino en la capacidad de las organizaciones para integrar capacidades, fomentar una cultura de seguridad consciente y desarrollar un talento humano capaz de anticiparse y adaptarse. Aquellas empresas que entiendan la seguridad como un facilitador estratégico de la continuidad del negocio, y no como un mero gasto operativo, serán las que mejor protejan su patrimonio en el complejo panorama latinoamericano.

Bibliografía Consultada

- Foro Económico Mundial (WEF). (2025). Global Risks Report 2025. Ginebra: WEF.
- Control Risks. (2025). RiskMap 2025: Análisis para Latinoamérica. Londres: Control Risks.
- Asociación Latinoamericana de Seguridad (ALAS). (2025). Informe Anual de Tendencias Delictivas Corporativas.
- PwC. (2025). Global Economic Crime and Fraud Survey 2025: Latin America Findings.
- Europol. (2025). Internet Organised Crime Threat Assessment (IOCTA) 2025.
- Institutos Nacionales de Estadística y Seguridad Pública de México (INEGI), Colombia (Policía Nacional), Argentina (Ministerio de Seguridad), España (Ministerio del Interior). Datos públicos y reportes sectoriales 2024-2025.
- ASIS International. (2024). Manual de Protección de Activos Empresariales. Edición revisada.

Dr. Tovar Cartaya John R., CPO

Consultor en Seguridad Integral

La Seguridad nace en tu mente

Cómo tu forma de ver el mundo define tu seguridad

DOS MUNDOS EN UN MISMO LUGAR

Imagina por un momento a Ricardo, un padre de familia, caminando por un parque urbano al atardecer. Lleva a su hijo de la mano y, mientras respira el aire fresco, sus ojos buscan el banco donde solía sentarse con su propio abuelo. Para Ricardo, ese parque es un "espacio de posibilidad": ve juegos, ve recuerdos, ve un atajo conveniente para llegar a casa y cenar. Su cuerpo está relajado, su respiración es pausada. En su mundo, en ese momento, no hay peligro.

A solo diez metros de distancia camina Elena. Ella fue víctima de un robo en esa misma zona hace seis meses. Aunque la luz es la misma y el viento sopla igual para ambos, Elena no ve un parque; ve un "laberinto de amenazas". Donde Ricardo ve un arbusto decorativo, Elena ve un punto ciego donde alguien podría esconderse. Donde Ricardo ve un atajo, ella ve una trampa sin salida. Su corazón late rápido, sus manos sudan y su atención está fragmentada. Ambos están en el mismo espacio físico, bajo las mismas leyes de la física, pero habitan mundos de riesgo radicalmente distintos.

Esta historia, que podría ser la de cualquiera de nosotros, nos revela una verdad profunda que a menudo ignoramos: la seguridad no está solo "allá afuera", en los objetos, en las rejas o en las personas que nos rodean. La seguridad —y el riesgo— viven en la conversación interna entre lo que sucede y quién está mirando. Esta es la esencia de unir la rigurosidad técnica de la seguridad con la profundidad humana del coaching ontológico.

De los muros a la mente

Para entender por qué este enfoque es revolucionario, debemos mirar un poco hacia atrás. Durante décadas, la industria de la seguridad y la gestión de riesgos se trató como una ingeniería de "muros y candados". La lógica era simple y mecánica: si quieres estar seguro, construye muros más altos, instala cámaras con mejor resolución y contrata guardias más fuertes. Era una seguridad reactiva, basada en el miedo y la fuerza bruta.

Sin embargo, la historia nos ha enseñado lecciones costosas y dolorosas. Grandes tragedias, desde el hundimiento del Titanic hasta fallos modernos en seguridad corporativa o aviación, rara vez ocurrieron porque la tecnología fallara. El Titanic no se hundió solo por un iceberg; se hundió por el juicio de arrogancia de creer que era "insumergible", lo que llevó a sus capitanes a ignorar las advertencias y a no llevar suficientes botes salvavidas. El fallo técnico fue consecuencia de un fallo en la observación humana.

En el mundo moderno, la norma internacional ISO 31000 llegó para cambiar este paradigma. En su evolución, dejó de ver el riesgo solo como "evitar cosas malas" y pasó a definirlo como el "efecto de la incertidumbre sobre los objetivos".
Aquí es donde entra el factor humano de lleno. La incertidumbre no es un dato numérico que puedas meter en una hoja de cálculo; es una sensación, una interpretación. Y los seres humanos no somos cámaras de video que graban la realidad de forma neutra. Somos seres lingüísticos, emocionales y biológicos.

Un dato alarmante que los expertos en seguridad integral manejamos es que más del 80% de los incidentes de seguridad (ya sea un robo en casa, un accidente laboral o un fraude digital) tienen un componente raíz de error humano basado en una percepción errónea. No es que la amenaza fuera invisible; es que nuestra mente decidió, inconscientemente, que "eso no podía pasar aquí".

¿Por qué no vemos lo que está frente a nosotros?

Desde el Coaching Ontológico, partimos de una premisa que puede sonar extraña al principio, pero que es liberadora: "No vemos las cosas como son, sino como somos nosotros".
Nuestro cerebro es una máquina biológica diseñada para la eficiencia. Para no colapsar con tanta información (millones de bits de colores, sonidos, distancias), crea "atajos" mentales y filtros. En seguridad, esto es crítico. Si tú crees (tienes el juicio arraigado) de que tu barrio es "tranquilo", tu cerebro literalmente filtrará y borrará las señales de peligro para confirmar esa creencia y mantenerte en calma. Verás a un desconocido merodeando y pensarás: "Debe estar esperando a alguien", en lugar de pensar: "Está evaluando las casas".
Al aplicar el coaching a la seguridad, desglosamos tres distinciones fundamentales que transforman nuestra capacidad de protección:

1. La trampa de la interpretación

La mayoría de las personas vive su seguridad basada en juicios, no en hechos, y eso es sumamente peligroso.

- El Hecho: Es algo comprobable y medible. Ejemplo: "La cerradura de la puerta principal no tiene pasador de seguridad" o "Esta calle no tiene alumbrado público".
- El Juicio: Es la opinión que tenemos sobre el hecho. Ejemplo: "No pasa nada, aquí todos nos conocemos" o "Es solo un tramo corto, no es peligroso".

El riesgo se materializa cuando confundimos nuestro juicio de comodidad con el hecho de seguridad. El delincuente no ataca tus juicios (lo buena persona que eres o lo tranquilo que es el barrio); el delincuente explota los hechos (la ventana abierta, la distracción con el celular). El coaching nos invita a limpiar nuestros lentes y preguntar constantemente: ¿Estoy realmente seguro o simplemente estoy cómodo?

2. La ceguera cognitiva y la transparencia

Vivimos la mayor parte del día en "transparencia", es decir, en piloto automático. Cuando conduces a casa, a veces llegas y no recuerdas los últimos cinco kilómetros. Eso es transparencia. En seguridad, la transparencia es el enemigo silencioso.
Hay riesgos que no vemos simplemente porque no tenemos la "distinción" para verlos. Un transportista experimentado mira una calle estrecha y ve un "embudo de riesgo"; un conductor novato solo ve "una calle angosta". El objetivo de este análisis es sacarte de la transparencia. La seguridad requiere un estado de presencia. No se trata de vivir en paranoia, sino de estar "aquí y ahora". Cuando estás presente, rompes la ceguera y empiezas a ver lo que antes era invisible.

3. La Emoción define la Acción

El miedo paraliza, pero la serenidad alerta salva vidas. Si gestionas tu seguridad desde el miedo constante (paranoia), terminarás agotado y cometerás errores por estrés. Si la gestionas desde la resignación ("si me va a tocar, me va a tocar"), te vuelves una presa fácil porque dejas de actuar.

El estado ideal es la Ambición de Cuidado: "Me cuido porque me valoro, no porque tengo miedo". Desde esta emoción, tus ojos se abren y tu capacidad de respuesta mejora biológicamente. Tu cuerpo está listo para actuar, no para huir despavorido.

Seguridad para la Vida Diaria
No necesitas ser un experto en artes marciales ni tener un doctorado en gestión de riesgos para elevar drásticamente tu nivel de seguridad. Solo necesitas cambiar tu observador.

El ejercicio del "Visitante Extraño"
Muchas veces, la familiaridad nos ciega. Nos acostumbramos tanto a nuestro entorno que dejamos de verlo. Esa puerta del patio que cierra mal ya no es un riesgo, es "una maña de la casa". Una vez al mes, sal de tu casa y vuelve a entrar, pero jugando un rol: imagina que eres alguien que ha olvidado las llaves y necesita entrar sin ser visto. Mira tu casa con esos ojos ajenos.
De pronto, notarás que ese arbusto alto tapa la visión de la ventana, o que la luz de la entrada está quemada, facilitando el acceso. Al cambiar el observador (de dueño a intruso), las vulnerabilidades saltan a la vista. Arregla esos detalles; la seguridad es 90% prevención y mantenimiento.

Romper la "Burbuja Digital"
Hoy en día, el mayor facilitador de asaltos en la vía pública es el celular. No solo porque es un objeto de valor, sino porque genera una "ceguera atencional" absoluta.
Practica la "Transición Consciente". Al salir de la universidad, del trabajo o del metro, guarda el teléfono por 3 minutos. Levanta la cabeza. Mira las manos de las personas. Los ojos pueden engañar, pero las manos ejecutan la acción. Si caminas observando el entorno, envías un mensaje corporal de "estoy alerta", lo cual disuade a muchos oportunistas que buscan víctimas distraídas (en transparencia). El delincuente busca facilidad, no resistencia.

El peligro de la "Llegada"
Estadísticamente, una gran cantidad de robos de vehículos y asaltos ocurren en la puerta de casa o del destino final. ¿Por qué? Porque el conductor piensa: "Ya llegué". Ese juicio relaja el cuerpo y baja la guardia antes de tiempo.

Mantén el "Juicio de Alerta" hasta que estés dentro de la zona segura. Al llegar a casa, antes de meter el coche o bajarte, haz un escaneo de 360 grados (espejos y entorno). Si ves algo que no te cuadra (un juicio de intuición), no te detengas, da una vuelta más. Confía en tu intuición; es biología pura queriendo protegerte.

Del "No es mi problema" a la "Red de Cuidado"
El aislamiento es el mejor amigo de la inseguridad. Un barrio donde los vecinos no se hablan es un "buffet" para la delincuencia. El juicio de "no es mi problema" es el mayor riesgo sistémico. Creen un grupo de comunicación (WhatsApp o similar) pero con reglas claras: solo para seguridad y emergencias (sin memes ni política).
Conocer al vecino es seguridad estratégica. Saber que el auto del vecino de enfrente no suele estar ahí a esa hora te permite detectar anomalías. La seguridad integral es coordinación de acciones. Una comunidad que se mira y se saluda es una comunidad vigilada naturalmente.

Tú eres el sistema
La gestión del riesgo empieza en la mente y termina en la acción. Podemos llenar nuestras ciudades de cámaras y nuestras casas de alarmas de última generación, pero la tecnología es solo una herramienta inerte sin un ser humano consciente detrás. Tú eres el sistema operativo de tu propia seguridad.
Si cambias la forma en que observas tus miedos (reconociéndolos sin dejarte dominar) y tus certezas (cuestionando si estás seguro o solo confiado), cambiarás tu capacidad de proteger lo que más amas. La seguridad integral no es un destino utópico donde "nunca pasa nada malo". Eso no existe. La seguridad real es la habilidad de estar preparados para gestionar la incertidumbre, con una actitud de cuidado, presencia y solidaridad.

"No podemos controlar el viento ni las olas (las amenazas externas), pero sí podemos ajustar nuestras velas y, sobre todo, entrenar al capitán que las observa (nuestra consciencia)."

Elías Cabeza
Lic. En criminalística
Militar retirado de la Fuerza
Aérea Venezolana

La Investigación Corporativa en la Venezuela de 2026:

Estrategia y Resiliencia

En el complejo ecosistema empresarial venezolano de 2026, la investigación corporativa ha experimentado una metamorfosis definitiva. Lo que antes se percibía como una actividad reactiva, limitada a auditorías contables básicas para resolver problemas puntuales, se ha transformado en el sistema nervioso central de las compañías que operan en el país. En un entorno marcado por la volatilidad cambiaria, la reconfiguración de sectores industriales y una apertura económica selectiva, investigar no es solo una medida de control, sino el motor que permite a las organizaciones nacionales y multinacionales navegar la incertidumbre.

Hoy, la investigación corporativa en Venezuela abarca un espectro sin precedentes: desde la auditoría de ética interna en empresas que manejan flujos mixtos de divisas, hasta el uso de inteligencia artificial para predecir movimientos de una competencia que se reinventa constantemente. En este paradigma, la información veraz es el activo más escaso y valioso; es la base para la resiliencia operativa y la protección de la reputación en un mercado hiperconectado.

1. Clasificación de la Investigación: Las Dos Vertientes en Venezuela

Para comprender cómo operan las empresas líderes en el país, debemos dividir la investigación en dos grandes categorías funcionales: la estratégica y la de cumplimiento (compliance).

A. La Vertiente Estratégica: Crecimiento en un Mercado en Transformación

Esta rama está orientada a identificar nichos de oportunidad dentro de la economía venezolana. Con la entrada de nuevos actores internacionales y el surgimiento de marcas locales robustas, la Inteligencia de Mercado es vital. Las empresas ya no solo miran sus ventas, sino que investigan la capacidad de consumo real de los distintos estratos de la población y el origen de los productos que inundan los anaqueles. La investigación de riesgos

geopolíticos también es crucial aquí: las empresas analizan constantemente el panorama de las sanciones internacionales y las licencias de operación, ya que cualquier cambio en la política exterior de socios clave puede alterar el suministro de insumos o el acceso a sistemas de pago globales.

B. La Vertiente Forense y de Cumplimiento: Protección en un Entorno Dual

En Venezuela, donde conviven el bolívar y el dólar, y donde el marco legal es altamente dinámico, la investigación forense se enfoca en la preservación de activos.

Investigación Forense e Interna: Se activa para detectar fraudes financieros y fugas de inventario, problemas críticos en un contexto de alta rotación de personal. La sofisticación de los delitos corporativos exige que estas investigaciones utilicen herramientas de análisis de datos para encontrar patrones sospechosos en las transacciones multimoneda que el ojo humano pasaría por alto.

Debida Diligencia (Due Diligence): Este proceso es el "escudo" de las empresas en Venezuela. Antes de cualquier alianza o adquisición, se realiza una radiografía exhaustiva de los socios comerciales para garantizar que no existan vínculos con actividades ilícitas o personas sancionadas, lo cual podría contaminar la operación global de la compañía.

2. Metodologías Modernas: El Ciclo de Inteligencia Adaptado

La metodología de investigación en el país ha dejado de ser empírica para volverse técnica, adoptando el ciclo de inteligencia para filtrar el "ruido" informativo típico del entorno venezolano:

Planificación: Se definen las preguntas críticas: ¿Es este proveedor confiable? ¿Cuál es el origen real de sus fondos? ¿Cómo afectará la nueva Ley de Economía Circular nuestras operaciones en el interior del país?

Recopilación: En Venezuela, esto implica un reto mayor. Se utilizan fuentes abiertas (OSINT), pero también se depende de la verificación en campo, ya que los registros públicos pueden estar desactualizados o ser de difícil acceso.

Procesamiento y Análisis: Los datos se cruzan con las realidades del mercado local. El análisis ya no solo describe la inflación pasada, sino que busca predecir la disponibilidad de combustible o energía para el próximo trimestre.

Difusión: Los resultados se entregan a las juntas directivas como insights accionables, permitiendo que las empresas decidan, por ejemplo, si deben adelantar compras de materia prima o diversificar sus proveedores logísticos.

3. Tendencias Disruptivas en el 2026 Venezolano
IA Democratizada y Monitoreo de Precios

La inteligencia artificial ha llegado a los departamentos de marketing venezolanos. Las empresas usan agentes de IA para rastrear los precios en "bodegones", cadenas de supermercados y marketplaces digitales en tiempo real. Esta democratización permite que incluso las medianas empresas (PYMES) realicen investigaciones competitivas que antes eran exclusivas de grandes corporaciones, ajustando sus estrategias de precios diariamente si es necesario.

El Giro hacia el Compliance Ético y ESG

A pesar de los desafíos económicos, la investigación corporativa en Venezuela ha puesto el foco en los criterios Ambientales, Sociales y de Gobernanza (ESG). Las empresas que buscan financiamiento internacional o exportar sus productos deben investigar su propia cadena de valor para asegurar el cumplimiento de estándares éticos y ambientales. En 2026, no investigar el impacto ambiental de una planta en Carabobo o Zulia puede cerrar las puertas a mercados europeos o norteamericanos.

Resiliencia ante Fallas de Infraestructura

Una tendencia única en el contexto local es la investigación preventiva de infraestructura. Las empresas investigan y monitorean constantemente el estado de las redes eléctricas y de conectividad en las distintas regiones del país para activar planes de contingencia. La investigación corporativa aquí se convierte en logística pura: saber dónde y cuándo habrá una interrupción permite a la empresa seguir operando mientras la competencia se detiene.

4. La Importancia Crítica de la Investigación

En la Venezuela de 2026, la velocidad de la información en redes sociales como X o TikTok es absoluta. Una investigación deficiente que no detecte una mala práctica de un empleado o un problema de calidad en un producto puede desencadenar una crisis de reputación viral que destruya años de construcción de marca en pocas horas.
Por el contrario, las organizaciones que dominan la investigación corporativa obtienen una ventaja estratégica inmensa. Pueden innovar con menor riesgo, contratar talento con mayor confianza en un mercado laboral complejo y reaccionar con agilidad ante los cambios regulatorios del Estado.

CONCLUSIÓN

La investigación corporativa en Venezuela ha dejado de ser una carga administrativa para convertirse en la brújula que guía a las empresas en un mar de incertidumbres. En un país donde los datos oficiales a veces son escasos y el mercado es profundamente dinámico, la capacidad de investigar de manera ética, tecnológica y profunda es la diferencia entre la quiebra y el liderazgo. Aquellas empresas venezolanas que integren estos procesos en su cultura organizacional no solo estarán protegiendo su patrimonio, sino construyendo un futuro sólido basado en la transparencia y la inteligencia real del mercado.

David González
Consultor

SEGURIDAD PRIVADA EN VENEZUELA

El eje estratégico de la transición hacia la inversión global.

El panorama venezolano ha dado un giro irreversible. A partir de los eventos suscitados desde el 3 de enero de 2026, la transición hacia la democracia trae consigo una transformación económica sin precedentes. Con la llegada de inversión extranjera y el retorno de empresas globales, la seguridad deja de ser un gasto operativo para convertirse en el activo estratégico más crítico del país, ya que, sin seguridad jurídica y física, no hay inversión sostenible y es evidente el atraso al que fue sometido todo el pais y los sectores de su sociedad, durante más de dos décadas transición de la democracia al autoritarismo.

Sin embargo, el nuevo horizonte que se vislumbra al final del túnel ubica a la industria de la seguridad privada en Venezuela en una encrucijada crítica. Este escenario debe ser analizado con rigor por aquellos empresarios resilientes que, pese a la severa crisis nacional, lograron sostener sus operaciones. Durante años, el sector fue víctima de modelos de gestión puramente reactivos y de una erosión institucional que permeó las estructuras corporativas, dejando un vacío de liderazgo evidente. Para quienes dominamos la materia, esta desidia es palpable a simple vista: se manifiesta en la figura del vigilante en la calle y en una desconexión profunda entre la operatividad táctica y la visión gerencial de alto nivel que hoy exigen las corporaciones internacionales.

Para que las empresas locales sean competitivas frente a la exigencia internacional, la profesionalización debe ser el eje central. No se trata solo de

contratar personal; se trata de formar líderes bajo estatutos claros y certificaciones estandarizadas. En este contexto, la capacitación y la mejora continua, se vuelven indispensables para tender puentes entre la necesidad del inversor y la capacidad de respuesta local.

Las empresas de seguridad venezolanas ya no pueden permitirse ser solo "proveedoras de servicios de vigilancia". La realidad actual y lo que se vislumbra para el pais, exige una urgente actualización en temas de gestión empresarial, porque el líder de seguridad del 2026, debe hablar el lenguaje de la alta gerencia, entender de mitigación de riesgos financieros, saber gestionar crisis y dominar estándares internacionales de cumplimiento (compliance), además de conocer y poner en práctica el importante tema de las relaciones publicas, para transmitir todos esos conocimientos a su entorno y garantizar unas operaciones que conlleven al éxito de la empresa.

La seguridad es, en esencia, "confianza". Y la confianza se construye con conocimiento y ética. La transformación que vive Venezuela requiere que los empresarios del sector abandonen las viejas prácticas de un sistema que buscaba socavar la institucionalidad para abrazar un modelo basado en la excelencia pedagógica y la formación continua. Solo mediante una gestión empresarial moderna, transparente y con avales de expertos internacionales, la seguridad venezolana podrá ser la garantía que el desarrollo económico del país, necesita.

El Espejismo del Pasado: "De la Dignidad a la Desidia"

Para entender hacia dónde debemos proyectar el sector, es imperativo recordar de dónde venimos. En el año 2001, mientras me desempeñaba como funcionario de Seguridad Pública en el estado Táchira, fui designado para apoyar en el transporte de valores a una reconocida empresa privada que, lamentablemente, desapareció tras la crisis. Recuerdo como si fuese hace un par de dias, que, al conversar con algunos de los empleados, descubrí que sus salarios casi triplicaban mi sueldo como Guardia Nacional. En aquel entonces, la seguridad privada gozaba de tal respeto y solidez, que muchos militares activos veíamos en ese sector una alternativa de retiro digna y profesional.

Esa realidad fue sepultada por una crisis impuesta. Lo que heredamos fue una estructura de abandono: hoy, la responsabilidad de proteger activos recae mayoritariamente en personas de la tercera edad la mayoría con problemas de salud, debido a su edad, empujadas por la necesidad a trabajar en condiciones de explotación laboral. Operan sin armamento reglamentario, sin capacitación técnica, carentes de liderazgo y bajo una precariedad legal absoluta que desprotege tanto al trabajador como al cliente."

Esta erosión alcanzó su punto más crítico en el área de la Protección Ejecutiva. Tras el desarme impuesto a la sociedad civil mediante leyes restrictivas durante la transición política al autoritarismo, se produjo un éxodo masivo de talento técnico. Los pocos escoltas que habíamos en el pais, al vernos imposibilitados para ejercer nuestra labor con legalidad y seguridad, nos sumamos a los más de 8 millones de compatriotas en la diáspora. Muchos de estos especialistas probablemente no regresaremos, dejando un vacío de capacidades difícil de llenar.

Ante la posible llegada de nuevas inversiones extranjeras, los empresarios demandarán esquemas de protección ejecutiva, vehículos blindados y logística de seguridad de estándar internacional. No podemos esperar a que la demanda nos atropelle; es urgente profundizar en el entrenamiento especializado y promover transformaciones jurídicas que permitan profesionalizar nuevamente el sector. Debemos preparar a una nueva generación de agentes que cubra el espacio de los que ya no están, garantizando que Venezuela sea un destino seguro para el capital y el desarrollo, por lo tanto, INSEAL está preparada, para contribuir en ello.

La Radiografía de una Crisis: “HABLÓ EL SARGENTO MAYOR”

Toda esta degradación sistémica es el resultado directo de la erosión de principios que analizo profundamente en mi libro: “HABLÓ EL SARGENTO MAYOR: Ante los antivalores de la humanidad” (disponible globalmente en Amazon desde 2019). Bajo esta óptica, me atrevo a sostener que en Venezuela se impuso una “seguridad de fachada” como norma; un modelo amparado por monopolios vinculados a quienes, durante más de 26 años, condujeron al país hacia su actual debacle institucional. Sin embargo, para pesar de esas estructuras cerradas, el panorama está por cambiar. La realidad actual demanda un nuevo orden en el empresariado del sector: una transición desde la desidia hacia la profesionalización ética, donde la seguridad deje de ser un simulacro y recupere su esencia como cimiento elemental de la sociedad.

Un síntoma de esta enfermedad moral que carcome la profesión en el rubro de la seguridad en Venezuela, lo viví recientemente con un joven familiar quien fue contratado por una empresa de seguridad sin filtros ni verificación de antecedentes penales. Le entregaron un uniforme y lo enviaron directo al servicio sin capacitación alguna. A los tres días, el chico abandonó el puesto de trabajo por apatía y aburrimiento, prefiriendo entregar el uniforme y quedarse desempleado y esa situación, me hizo deducir que quienes lo contrataron, no utilizaron estrategias de motivación, basadas en las características esenciales de liderazgo, que deben tener los gerentes y supervisores de cualquier empresa de seguridad en el mundo. Cuando no hay selección ni liderazgo, no hay compromiso; solo hay un hombre uniformado esperando que el tiempo pase, para cobrar su bajo salario, sufragar los gastos de su hogar y volver a la misma rutina, que se convierte en un círculo vicioso.

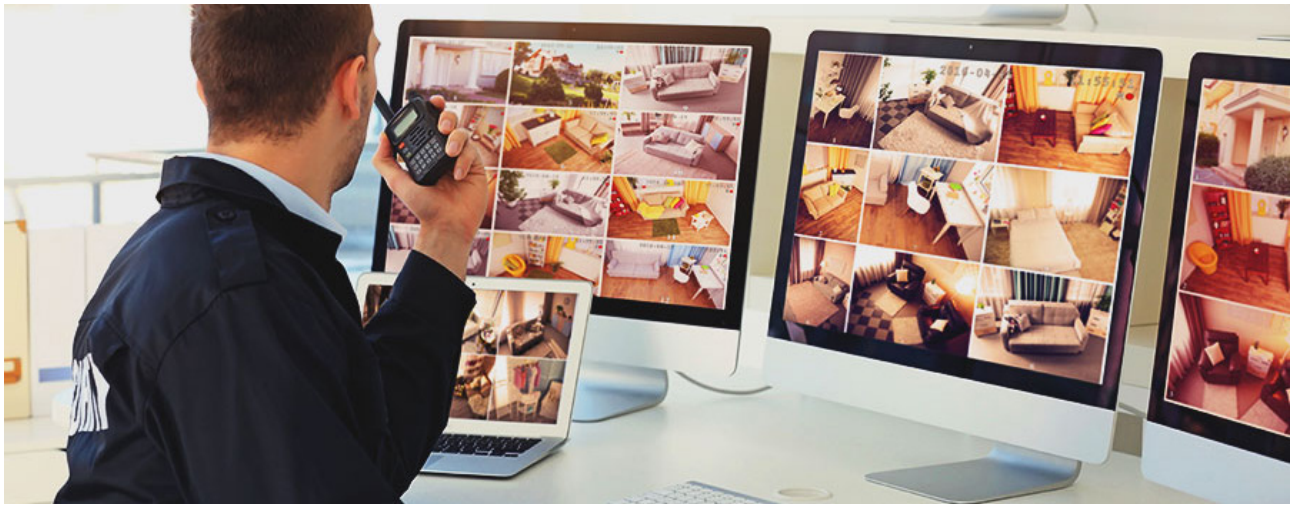
Esta desconexión operativa es apenas el reflejo de una herida más profunda: el colapso del Estado de Derecho frente a la siembra sistemática de antivalores. Como explico en mi obra, la seguridad ciudadana y la seguridad privada no son compartimentos estancos; ambas se nutren del mismo tejido social. En Venezuela, la erosión de la institucionalidad ha borrado la frontera entre el orden y la anarquía, permitiendo que la corrupción y el facilismo sustituyan a la disciplina y el honor. Cuando el Estado deja de garantizar justicia y el mérito es reemplazado por la lealtad política, la seguridad pública se desvirtúa y la privada se degrada en esa experiencia real que mencioné anteriormente. Sin un marco legal sólido que castigue el antivalor y premie la ética, nos quedamos con instituciones vacías de contenido, donde la falta de propósito es la consecuencia natural de una sociedad a la que se le arrebató el sentido del deber y el respeto por la ley, por tal motivo, es pertinente que el empresariado venezolano, entienda la necesidad de incluir en los programas de capacitación de su personal, el tema del liderazgo ético y rescate de los valores que aprendimos desde niños y que algunos hemos dejado de poner en práctica, por cuestiones de rutina o simplemente por permitir en nosotros características negativas como el EGOCENTRISMO, que es un mal que llevamos con nosotros, muchos profesionales de seguridad y que no hemos podido superar.

La Cúspide de la Improvisación: "El Vacío de Liderazgo Gerencial"

Sin embargo, la crisis más alarmante no está en la base de las empresas, que es su capital humano o su razón de ser (vigilantes), sino en la gerencia. Hace aproximadamente cinco meses, en INSEAL, fuimos contactados desde México para coordinar un servicio de vehículos blindados con la finalidad de proteger a un grupo de ejecutivos de una reconocida multinacional, que viajarían desde el exterior, a las ciudades venezolanas de Valencia, Maracay y Maracaibo.

Al contactar a una empresa de "seguridad" local, quedé sorprendido, cuando al conversar vía telefónica con una dama quien se identificó como la Gerente de Ventas de una empresa de seguridad, me di cuenta que desconocía en su totalidad, que significaban los niveles de blindaje automotriz. Que alguien en un cargo de decisión ignore los estándares técnicos de Protección Ejecutiva es una negligencia técnica inaceptable. Este es el resultado de operar en una nación donde el "contacto político" o la necesidad de tener alguien en el puesto sin que esté preparado (a) para tal fin, vale más que el conocimiento profesional que se requiere, porque ni tienen la iniciativa de capacitarlos sobre el tema del cargo que les ofrecen.

En tal sentido, desde los Estados Unidos de América, hemos estado preparando robustos programas virtuales de capacitación y mejora continua, convertidos en diplomados en Gestión de la Seguridad, con la participación de instructores especialistas de renombre internacional y dejarlos disponibles al público en nuestros portales web, para que aquellos profesionales interesados en pasar al siguiente nivel en sus carreras, se capaciten cómodamente bajo la modalidad asincrónica y sobre todo adaptándolos a la economía actual del pais, de una manera muy accesible, para que esto no represente un impedimento en el interesado.



INSEAL: El Aliado adecuado, para las empresas de la Nueva Venezuela

En INSEAL USA, nos hemos estado preparando para este momento. En nuestra gama de servicios a nivel internacional, no solo ofrecemos capacitación técnica de vanguardia para elevar el nivel de los gerentes y guardias de vigilancia de cualquier empresa de seguridad, sino que contamos con instituciones aliadas y las plataformas adecuadas, para permitir que los profesionales venezolanos accedan a cursos intensivos, licenciaturas en Criminología y Seguridad Pública, en modo virtual. Además, hemos estandarizado certificaciones como "PRIVATE SECURITY OFFICER INSEAL" (Oficial de Seguridad Privada Inseal) y "AGENTE DE PROTECCION EJECUTIVA INSEAL", además, estamos esperando el gran momento de tener el camino libre para establecernos como empresa de seguridad en Venezuela y poder ofrecer todos nuestros servicios, con el objeto de generar empleos y de esa manera, contribuir con el desarrollo de esa gran nación de América Latina como lo es Venezuela, la cual, con el apoyo de los Estados Unidos de América, está destinada a convertirse en una gran potencia económica.

Además, estamos consolidando una base de datos de profesionales líderes de la seguridad pública (ex policías y militares retirados) con trayectoria ética que se quedaron en el pais y otros que regresaran luego de la apertura económica, para capacitarlos, entrenarlos, adaptarlos a los nuevos estándares y reinsertarlos a ser parte de la solución en el campo de la seguridad privada y la protección ejecutiva.

Venezuela pasa de la oscuridad a la competitividad global. La seguridad en esta nueva era no será cuestión de azar, sino de profesionalismo y estándares internacionales. Invitamos al empresariado a actualizarse y a los profesionales a unirse a nuestra comunidad de mejora continua. Es momento de que la ética y la formación técnica sean el cimiento de nuestra nación.

Nota del Autor:
Para más información sobre INSEAL, puedes visitar nuestro portal web: www.inseal.us y conocer más sobre nuestra visión.

Dicxon Ruiz Quintana
Director de Operaciones de INSEAL-USA,
Texas - Houston 26/01/2026.

ASESORES Y CONSULTORES C.A.

SEPREVYPRO

Seguridad, Prevención y Protección

LA AGENDA EJECUTIVA DE SEGURIDAD INTEGRAL

ES MI HERRAMIENTA PARA RENDIR MI GESTIÓN

UTILIDAD DE LA AGENDA

- Produce un esquema de trabajo organizado con fundamentos técnicos.
- Es tener la organización a la mano para analizar, evaluar y dar la debida respuesta administrativa y operativa en cada caso.

BENEFICIOS ASOCIADOS

- Gestión coherente.
- Trabajo en equipo.
- Conocimientos en sistema integral de seguridad.
- Estandariza los procesos.
- Planificación metódica.

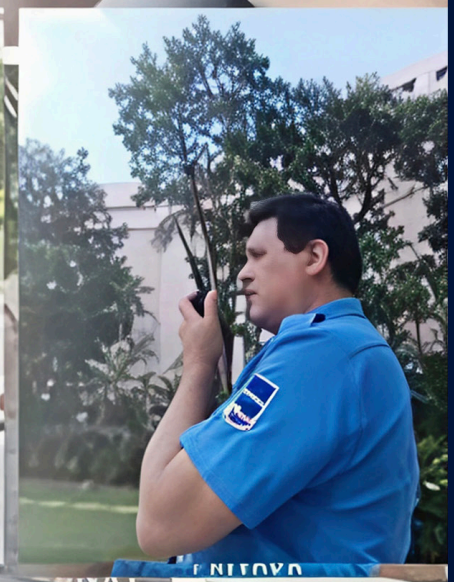
VALORES

- Conlleva a la sincronía en los procesos de seguridad.
- Produce la organización de información a la mano.
- Promueve una mística de trabajo basado en el tecnicismo de la seguridad.

INFORMACIÓN

seprevypro@gmail.com
seprevypro@hotmail.com
WhatsApp: 0426 511 88 99

HALCONES DE VALENCIA C.A.



Conoce
NUESTROS SERVICIOS

- Sistemas de alarmas y CCTV.
- Control de acceso.
- Biometricos.
- Seguridad Residencial.
- Seguridad Comercial.
- Seguridad Empresarial.

halconesValencia@gmail.com
+58 414 496 96 50
+ 58 412 408 80 51

Ciudad de Valencia
Estado Carabobo Venezuela

La IA Transforma la Seguridad CCTV en 2026

En el vertiginoso mundo de la tecnología, pocos avances han impactado la seguridad como la fusión de la Inteligencia Artificial (IA) con los sistemas de Circuito Cerrado de Televisión (CCTV). Lo que antes era una simple herramienta de grabación, hoy se ha convertido en un centinela inteligente, capaz de predecir, analizar y reaccionar con una eficiencia sin precedentes. En 2026, esta integración ha alcanzado nuevas cotas, redefiniendo el concepto de vigilancia y protección.

Más Allá de la Grabación: Análisis Predictivo y Detección Proactiva

El cambio más significativo no es solo la capacidad de ver, sino de comprender. Los sistemas CCTV impulsados por IA de hoy no solo graban eventos, sino que los analizan en tiempo real para identificar patrones y anomalías. La visión por computadora avanzada permite detectar comportamientos sospechosos, objetos abandonados, intrusiones en zonas restringidas e incluso predecir posibles incidentes antes de que ocurran. Esto se traduce en una reducción drástica de las falsas alarmas y una mayor agilidad en la respuesta. Los operadores de seguridad ya no están abrumados por horas de metraje, sino que reciben alertas contextualizadas y priorizadas, permitiéndoles enfocar su atención donde más se necesita.

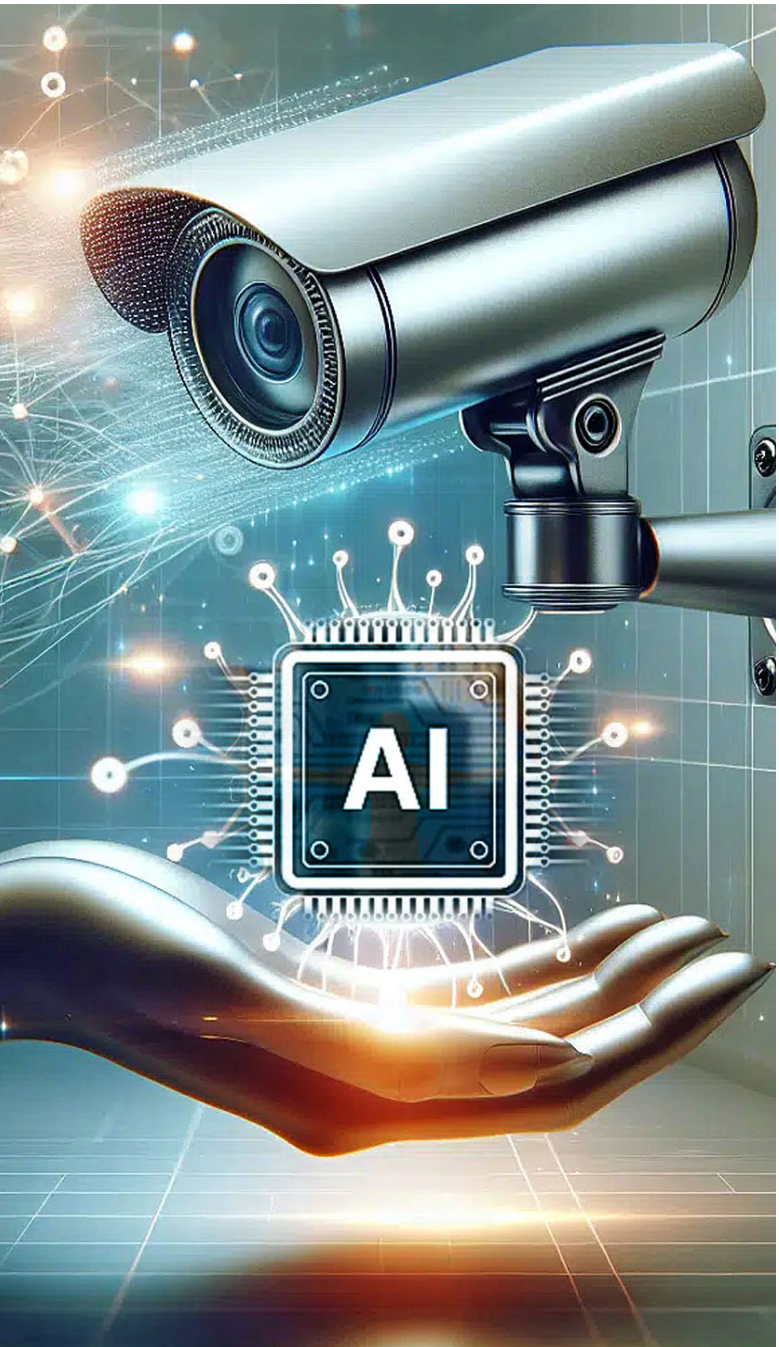
Reconocimiento Facial y de Objetos: Identificación Precisa y Gestión Eficiente

La IA ha perfeccionado el reconocimiento facial, que ahora es capaz de identificar personas con una precisión asombrosa, incluso en condiciones de poca luz o con obstrucciones parciales. Esto es invaluable para el control de acceso, la búsqueda de personas desaparecidas o la identificación de individuos de interés en grandes multitudes.

El Salto Cuantitativo de 2026: De la Vigilancia a la Inteligencia Contextual

En este 2026, la integración de la Inteligencia Artificial en el CCTV ha dejado de ser un "complemento" para convertirse en el núcleo del sistema. La infraestructura ha mutado, pasando de servidores centralizados a una red distribuida de nodos inteligentes.

1. Edge AI: Procesamiento en la Propia Cámara
Una de las mayores mejoras de este año es la consolidación del Edge Computing. Ya no es necesario enviar terabytes de video a la nube para que sean analizados. Las cámaras de 2026 cuentan con chips NPU (Unidades de Procesamiento Neuronal) integrados que procesan la metadata localmente.



Ventaja: Reducción del latencia a milisegundos y ahorro masivo en ancho de banda.

Impacto: La cámara puede tomar decisiones autónomas, como activar un cierre de emergencia o emitir una alerta sonora, sin depender de una conexión a internet estable.

2. IA Multimodal y Fusión de Sensores
El CCTV moderno ya no solo "ve". Gracias a la IA multimodal, los sistemas combinan video de alta definición con:

Analítica de Audio: Identificación de disparos, rotura de cristales o gritos de auxilio, diferenciándolos del ruido ambiental urbano.

Imagen Térmica de Nueva Generación: Capacidad de detectar variaciones de temperatura corporal para prevención de incendios o monitoreo de salud en espacios públicos.

Radar y LiDAR: Integrados en la misma unidad de CCTV para medir distancias exactas y velocidades, permitiendo un seguimiento 3D preciso incluso en oscuridad total o niebla densa.

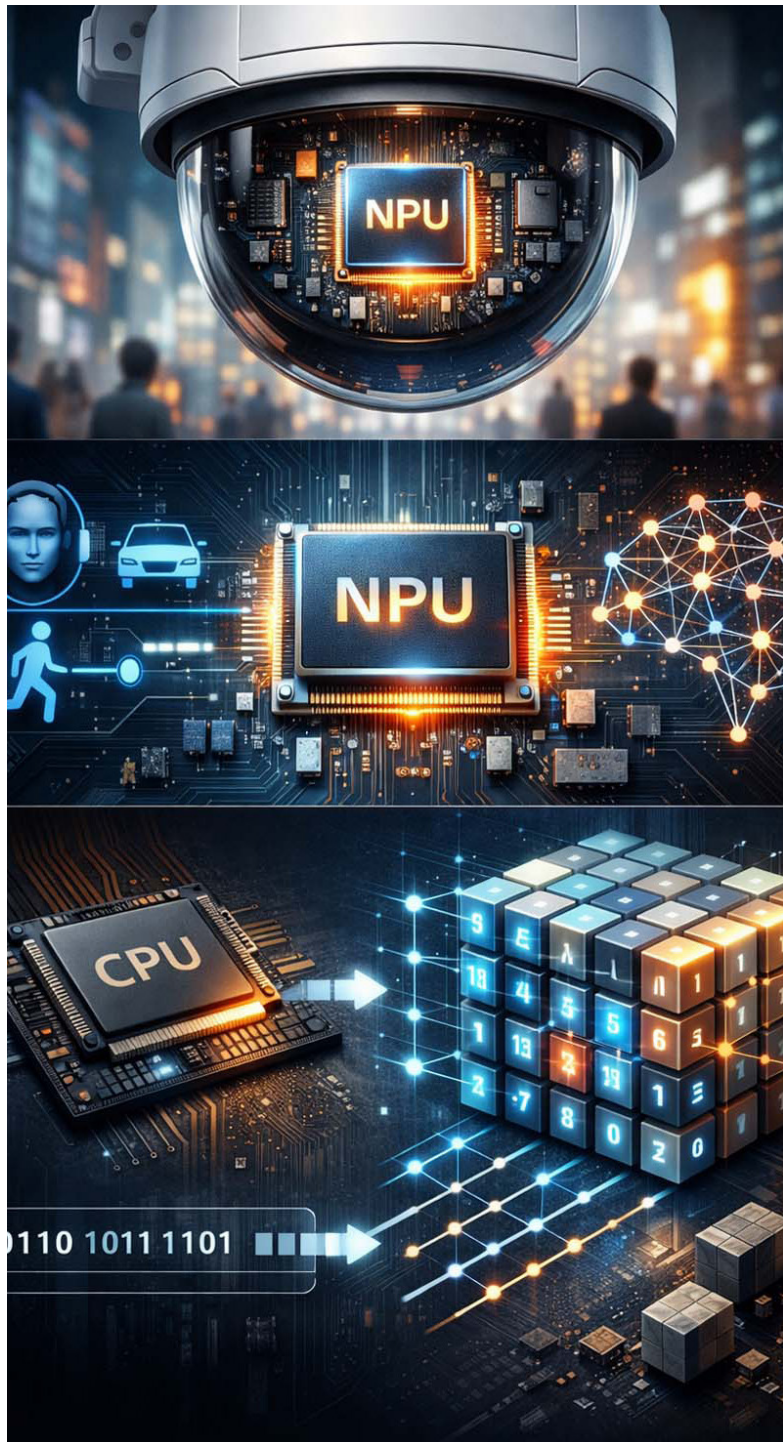
3. La Ética y la "Privacidad por Diseño"
Ante el avance de la IA, 2026 es el año de la regulación estricta. Los sistemas líderes ahora integran anonimización dinámica. La IA difumina

automáticamente los rostros y placas vehiculares en el flujo de video en vivo, y solo permite el acceso a los datos originales bajo protocolos de seguridad estrictos o mediante una orden digital autorizada.

"La seguridad ya no se mide por cuántas cámaras tienes, sino por la capacidad de tu IA para interpretar el entorno respetando la libertad individual."

El Motor de la Vigilancia Moderna: ¿Qué es una NPU?

A diferencia de las CPUs convencionales (diseñadas para tareas generales) o las GPUs (optimizadas para gráficos), la NPU es un microprocesador diseñado específicamente para acelerar algoritmos de aprendizaje profundo (Deep Learning). En el contexto del CCTV de 2026, la NPU es el componente que permite que el análisis ocurra dentro de la propia carcasa de la cámara.



Arquitectura y Funcionamiento
El funcionamiento de una NPU se basa en la computación en paralelo masiva. Mientras que una CPU procesa tareas de forma secuencial, la NPU está estructurada para realizar miles de operaciones matemáticas simultáneas (específicamente multiplicaciones y acumulaciones de matrices), que son la base de las redes neuronales.

CARACTERÍSTICAS CLAVE EN 2026:

Eficiencia Energética: Las NPUs actuales logran un rendimiento de hasta 10-15 TOPS (Trillones de Operaciones por Segundo) consumiendo apenas unos pocos vatios. Esto evita que las cámaras se sobrecalienten a pesar de procesar video en 4K a 60 fps en tiempo real.

Optimización de Capas de Red: Están diseñadas para ejecutar capas de convolución (el "ojo" de la IA que detecta bordes y formas) y capas de atención (que permiten a la IA enfocarse en un objeto específico ignorando el movimiento de las hojas de un árbol).

EL FLUJO DE TRABAJO EN EL DISPOSITIVO (ON-DEVICE WORKFLOW)

Cuando un haz de luz entra por el lente, la NPU interviene en milisegundos.

Pre-procesado: Limpieza de ruido digital y ajuste de contraste mediante IA.

Extracción de Características: La NPU identifica patrones (un rostro, un arma, una matrícula).

Inferencia: El sistema toma una decisión basada en los patrones. Por ejemplo: "Este objeto es un humano y su trayectoria indica que va a saltar la valla".

Generación de Metadata: En lugar de enviar el video completo al servidor, la cámara envía un pequeño paquete de datos con la alerta y las coordenadas del evento.

¿Por qué es vital para el CCTV actual?

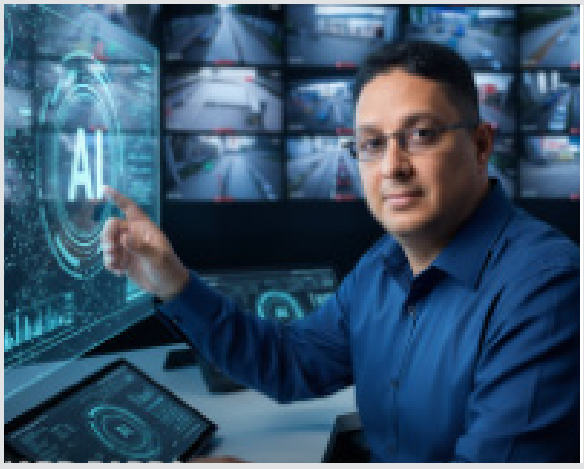
Sin la NPU, la analítica avanzada dependería de una conexión constante a un servidor potente. En 2026, la "Inteligencia en el Borde" garantizada por estos chips significa que, incluso si un atacante corta los cables de red, la cámara puede seguir analizando la escena localmente, activar alarmas sonoras y almacenar la evidencia crítica de forma autónoma.

Dato Técnico: Las cámaras de gama alta en 2026 ya integran NPUs de tercera generación con arquitectura de 7 nanómetros, lo que permite que una sola cámara rastree hasta 200 objetos simultáneamente sin degradar la calidad de la imagen.

Conclusión: El Futuro es Autónomo

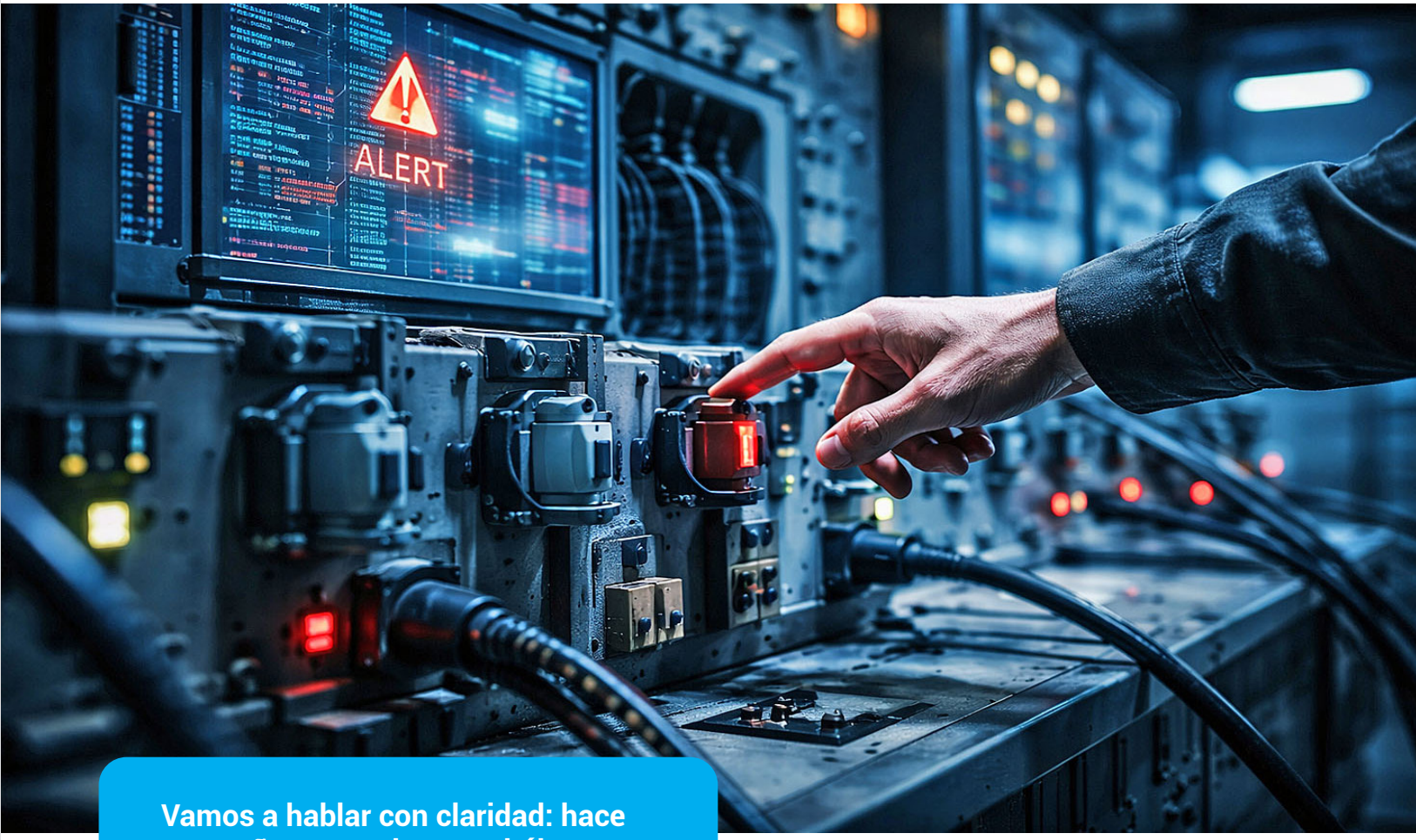
La integración de la IA en CCTV este año ha transformado las ciudades en "Smart Cities" más seguras. Hemos pasado de ser espectadores de lo que ocurrió a gestores en tiempo real de lo que está sucediendo. El siguiente paso, que ya empezamos a vislumbrar, es la colaboración total entre enjambres de drones de vigilancia y cámaras fijas, orquestados por una sola mente sintética.

Mi Trayectoria en Seguridad Tecnológica



Richard Parra
Un profesional con 24 años de trayectoria en el sector de la seguridad tecnológica. Mi especialización principal se centra en el diseño, implementación y gestión de sistemas de CCTV (Circuito Cerrado de Televisión) de alta complejidad.
A lo largo de mi carrera, me he consolidado como un referente en la gestión de proyectos a gran escala con integración de Inteligencia Artificial (IA) y en la gestión de proyectos de seguridad complejos. Mi compromiso es inquebrantable en la optimización de la vigilancia y la protección de activos mediante la implementación de soluciones de vanguardia.

Cuando el Bit
SE CONVIERTE EN ÁTOMO



Vamos a hablar con claridad: hace unos años, cuando escuchábamos la palabra "Ciberseguridad", pensábamos en un muchacho con capucha metido en un sótano oscuro allá en Europa o China, tratando de robarse una clave de banco. Pero si algo nos ha enseñado este primer trimestre de 2026 —y especialmente el susto que pasamos el sábado 3 de enero— es que ese cuento cambió. Ahora, el problema es aquí, es ahora y, lo más importante, ya no se queda solo "dentro de la computadora".

El 3 de enero: Un balde de agua fría

No nos digamos mentiras. Lo que pasó ese sábado de enero en Venezuela no fue solo un "problema técnico". Fue la prueba de que, si alguien quiere echarle una broma al país, ya no necesita un tanque de guerra; le basta con saber dónde darle click a los sistemas que controlan nuestra luz y nuestras comunicaciones.

Ese día entendimos que la ciberseguridad es, literalmente, seguridad nacional. Si se cae la red, se para el comercio, se quedan mudos los teléfonos y, peor aún, se nos complica la logística de seguridad física. En este 2026, si no proteges tus redes, es-

tás dejando la puerta de tu empresa (y de tu casa) abierta de par en par.

El "Cibercrimen" se puso botas y salió a la calle

Este es el punto que más me preocupa y del que quiero que hablemos en esta edición: el delincuente ya no solo quiere tu clave, quiere tu dirección.

En Venezuela estamos viendo una tendencia peligrosa. Hackean la base de datos de una cadena de farmacias o de una aplicación de delivery, y nosotros pensamos: "Bueno, no tengo dinero en esa cuenta, no importa". ¡Error! En esa base de datos está tu nombre, tu teléfono, qué compras, dónde vives y a qué hora pides comida.

Esa información digital se la venden a las bandas que operan en la calle. Entonces, el delincuente que te intercepta ya sabe quién eres y qué tienes. El mensaje es contundente: Un descuido digital hoy es un riesgo físico mañana. El bit se convirtió en átomo; el código se convirtió en amenaza real.

La Inteligencia Artificial: ¿Ayuda o dolor de cabeza?

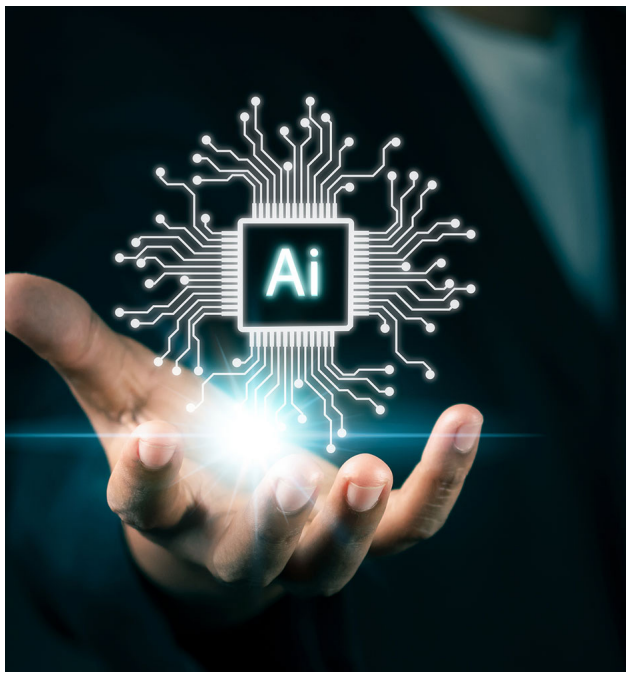
La IA en este 2026 está haciendo cosas increíbles, pero los "malos" también la están usando. ¿Te han llamado últimamente con la voz exacta de un familiar o de tu jefe pidiéndote un favor urgente o una transferencia porque "están en una emergencia"?

Ojo con eso. Ya no puedes confiar ciegamente en lo que escuchas o ves en una pantalla. Los deepfakes están a la orden del día. Mi recomendación: Vuelve a lo básico. Crea claves familiares o corporativas, palabras secretas que solo tú y tu equipo conozcan. En un mundo de IA, la desconfianza inteligente es tu mejor defensa.

Seguridad en el trabajo: No es solo usar el casco

A mis amigos de seguridad industrial y laboral les digo: ya no basta con que el trabajador use las botas y el casco. Si ese trabajador conecta su teléfono personal cargado de virus al puerto USB de una máquina de la planta, puede parar la producción entera.

Este primer trimestre ha sido movido para las industrias venezolanas. La "convergencia" significa que el sistema que controla la temperatura de una cava o la presión de una tubería está pegado a internet. Si alguien entra ahí, el daño es físico, es costoso y es peligroso. La seguridad laboral en 2026 empieza por la higiene digital de cada empleado.



¿Qué nos toca hacer el resto del año?

No quiero que lean esto y se asusten, quiero que se activen. En Venezuela somos expertos en resolver, pero en seguridad es mejor prever.

Para este primer trimestre y lo que viene en Semana Santa, les dejo tres consejos:

Cero confianza (Zero Trust): No asumas que porque alguien te escribe de un número conocido, es esa persona. Verifica.

Limpia tu rastro: Deja de poner tanta información de tu rutina en redes sociales. Al delincuente del 2026 le encanta tu Instagram para planificar su próximo golpe físico.

Actualízate o te actualizan: Si tu software es del 2020, estás trabajando con las puertas abiertas. Invierte un poquito en actualizar tus sistemas; te va a salir mucho más barato que pagar un rescate o perder la mercancía.

Adolfo M. Gelder

BLINDA TU PYME:
MÁS SEGURIDAD, MEJORES FINANZAS
OPERACIONES EFICIENTES

Transformamos tu riesgo en crecimiento
Estrategia, Ciberseguridad y Rentabilidad

Finanzas

Organización y control para tu tesorería

Ciberseguridad

Protección avanzada contra amenazas digitales

Organización y Métodos

Procesos eficientes y reducción de riesgos internos

S&S
Consultores Corporativos

S&S CONSULTORES CORPORATIVOS

Agenda tu auditoria de seguridad informática gratuita

CAPACITACIÓN Y CONSULTORIA ESTRATEGICA DE SEGURIDAD

Carrillo & Consultores Asociados

NUESTROS SERVICIOS

- Capacitación del personal de Seguridad Privada
- Analisis y gestión de riesgos Bajo metodologia RBI

- Estudios de Seguridad y vulnerabilidad Corporativa
- Diseño de manuales de procedimientos y protocolos

- Capacitación tecnica en Seguridad y protecccón ejecutiva

WEB:https://carrilloconsultores.webnode.com.ve
+58 424 398 6498
marcos.carrilloc@gmail.com
@carrilloconsultores.ve
+ 58 424 398 6498 / 426 218 2158

"LAS BUENAS PRÁCTICAS DE SEGURIDAD Y LA IMPORTANCIA DE LA CAPACITACIÓN"

La evolución urbana de Caracas ha consolidado los centros comerciales como espacios multifuncionales que trascienden la simple función de compra, convirtiéndose en puntos neurálgicos de encuentro social, esparcimiento y actividad económica. Estos complejos, que van desde el icónico Sámbil Caracas hasta opciones más especializadas como el Tolón Fashion Mall, reflejan un comportamiento del consumidor y una dinámica de mercado particulares en el contexto venezolano actual.

El objetivo principal de estas líneas, es indagar para generar información relevante sobre estos espacios, analizándolos como termómetros de la realidad socioeconómica de la capital. La visita a centros comerciales de la gran caracas permitió recopilar datos de primera mano sobre: Flujo, perfil de los visitantes y personal que labora y presta servicios, en especial la seguridad privada y la vigilancia.

Desde esta perspectiva, se realiza un estudio sobre las prácticas de seguridad física en centros comerciales, con el objetivo de identificar áreas de mejora y fortalecer la protección tanto para visitantes como para el personal.

La seguridad privada, en un estado democrático moderno como el de nuestro país, es muy compleja, pues abarca múltiples factores, por lo tanto, para dar respuesta adecuadas a las demandas de la sociedad venezolana y en éste caso específico, como lo son los ciudadanos que visitan y hacen vida en los centros comerciales, comerciantes y dueños de locales e incluso personal gerencial y dueños de centro comerciales. Siendo las cosas así, resulta claro que surgen varias premisas y si las contextualizamos a través de interrogantes, posiblemente podamos construir un temario de diagnóstico de seguridad. De este modo se pueden priorizar las acciones que incidan directa e inmediatamente en las buenas prácticas en seguridad.

Para dar con esa respuesta adecuada, en cuanto al servicio óptimo en un centro comercial, se describen algunas incógnitas que, si se toman en consideración, de seguro abarcará esos factores que influirán en el servicio que satisfaga a la sociedad.

A TÍTULO ILUSTRATIVO, INTERROGAREMOS LAS SIGUIENTES PREMISAS:

¿Cómo es la aproximación? Consiste en indagar conocimientos generales del centro comercial; historicidad, estructura organizacional, tipos de visitantes, ubicación, productos de comercialización y estructura de seguridad entre otros.

¿Cuáles son las características del personal de seguridad? Imprescindible saber cómo es la forma de supervisión, del liderazgo, la presencia del trabajador, educación y decoro, si el hacer cotidiano del ejercicio de vigilancia está basado en el ejemplo y la moral, perfil del personal y evaluación del conocimiento, dominio y manejo teórico-práctico de la seguridad física.

¿Cuál es la función de la seguridad? La seguridad debería estar al servicio de los objetivos de la empresa o centro comercial, la ejecución de la seguridad no obstaculiza el funcionamiento de los procesos. Su actividad es flexible, el producto de su función es la prevención y protección, los roles del personal deben estar bien definidos.

¿Cómo es la inducción en la seguridad? El objeto y función de la seguridad está clara, se toma en cuenta el ambiente operacional de todos los departamentos del centro comercial, los aspectos legales, organigrama gerencial, normas, procesos, procedimientos y recuentos de casos.

¿Cómo es el ambiente operacional? Se refiere al entorno que rodea a la empresa, el lugar donde tiene las oficinas, áreas críticas, almacenes, orientación del personal obrero y administrativo, características de las empresas del sector que hacen vida en el centro comercial y o afines. Ubicación de la problemática del país en asuntos de seguridad, índices delictuales, los acontecimientos de orden público, los modus operandis que existen en incidentes o eventos no deseados, comunicación efectiva con otras gerencias para el seguimiento de casos, en fin, una gestión interfuncional.

¿Existen políticas de seguridad? Es el norte ético-jurídico que orienta la función de seguridad, en ella deben estar contemplados asuntos como la prohibición de hacer actos en contra de la ley. Esta permite la cultura de la seguridad.

¿Hay fundamentos legales de seguridad? Es el ejercicio regulado por las leyes, normas, reglamentos, manuales de funciones, manuales de emergencias, etc. En tal sentido hay que conocerlos, comprenderlos y cumplirlos, de allí se genera la responsabilidad penal, civil y administrativa.

¿Cómo se concibe la seguridad empresarial? Es el conjunto de políticas, normas, procesos que se tienen, se crean y establecen en un servicio de un centro comercial para prevenir y proteger de eventos o incidentes no deseados, que afecten el objetivo comercial del servicio.

¿Cuál es el objeto de estudio de la seguridad? Realizar un gran diagnóstico de todo lo que concierne, afecta, influye en al servicio de seguridad de la empresa. Hacerlo desde una perspectiva integral tomando en cuenta los tres medios que la cons-

tituyen; medios humanos, medios técnicos y medios organizativos. El estudio analiza los riesgos y la forma de disminuirlos básicamente, describe las amenazas, evalúa los riesgos, enfocado en los activos de la empresa como lo son las personas, bienes materiales, infraestructura y procesos.

EL POR QUÉ DE LA CAPACITACIÓN

En tal sentido, de la realidad que se vive en un centro comercial, el servicio de vigilancia forma parte del equipo de seguridad, es de gran significancia debido a que son la personas que tienen contacto directo con el conglomerado de ciudadanos que hacen vida en los citados espacios, por ende, consideramos que es de carácter exclusivo y obligatorio poseer conocimientos básicos unificados del ejercicio de la seguridad física. Por consiguiente, se realizó una indagación al personal de vigilancia, esto con el fin de verificar y abordar la necesidad que surge cuando hay diferencia entre lo que una persona debería saber para desempeñar una tarea, y lo que sabe realmente.

La forma de interactuar con los entrevistados fue de la siguiente manera. "Su experiencia y perspectivas como oficial de seguridad son muy valiosas para nosotros. ¿Podría dedicarnos unos breves minutos para responder algunas preguntas sobre su formación y conocimientos en seguridad? La información que nos proporcione será tratada de forma confidencial y anónima, y los resultados solo se utilizarán con fines estadísticos para el informe general. Agradecemos mucho su colaboración."

Estando de acuerdo los entrevistados y respondiendo las siguientes preguntas.

1. ¿Qué entienden por el significado de sistema?
2. ¿Qué entienden por el significado de seguridad?
3. ¿Qué entienden por el significado de prevención?
4. ¿Qué entienden por el significado de protección?
5. ¿Cuál sería el fin último de la seguridad en tu trabajo?
6. ¿Cómo pueden definir el significado de sistema integral de seguridad?

En atención al interrogatorio realizado, refiere la importancia que tuvo la intencionalidad de concebir un impacto a los entrevistados de despertar y avivar, una realidad que surge, cuando hay diferencia entre lo que un oficial de vigilancia debería saber para desempeñar una tarea, y lo que sabe realmente. Obteniendo unos resultados y hallazgos notables, y preocupante en las secciones dedicadas a generalidades de protocolos de seguridad; las respuestas de los participantes no fueron adecuadas y carecieron de sintonía con las expectativas y estándares requeridos, revelando una posible brecha en la comprensión o aplicación de las directrices de seguridad.

Es allí donde el pensamiento cobra valor, e indiscutiblemente se tiene que reflexionar, cuestionar y partiendo de la necesidad imperiosa de crear espacios para capacitar al personal de vigilancia, siendo ellos considerados en el servicio de seguridad en un centro comercial, como las cuatro patas de la mesa, ósea por el rol que desempeñan en contacto directo con la colectividad, teniendo ésta una expectativa de optima atención.

Se hace necesario contar con espacios concretos para profundizar una mirada y recorridos que tengo en mi intuición, ya que, como profesional de la materia, abre paso al camino del conocimiento, teniendo la posibilidad de originar contenidos conceptuales, procedimentales y actitudinales, que identifiquen la búsqueda de soluciones a tal situación como lo es la concientización de las buenas prácticas de seguridad.

Por lo tanto, como empresario de seguridad, como profesional que contrata servicio de vigilancia y como cliente que requiere ese digno servicio, exige la capacitación idónea del personal en cada área, única forma de transformar y mejorar la labor de vigilancia.

“La educación, prevención y protección es la tríada fundamental en la Seguridad”

Luis Silva Ascanio.

Lic. en Educación. Profesor Universitario, con énfasis en Prevención del Delito y Ciencia Penitenciaria. T.S.U. en Estudios Penitenciarios Mención Gerencia y Mención Seguridad. Máster en Seguridad Aplicada. Gerencia de Protección y Seguridad Integral.

CONTACTO

Contact Integrated Systems

Productos que ofrecemos

- Gestión Estratégica Y Revisión Gerencial
- Gestión de Clientes
- Gestión de Proveedores
- Continuidad de Negocio
- Gestión del Riesgo
- Gestión de Activos
- Gestión documental
- Talento Humano
- Requisitos Aplicables
- Solución de Problemas
- Auditoría
- Encuestas
- Calendario – Minutas
- Gestión de Controles

Beneficios

- Interfaces adaptables a múltiples dispositivos y de fácil utilización
- Optimización de procesos internos
- Módulos integrados que facilitan la carga de datos
- Visualización de la información a través de un site responsive que se adapta a cualquier dispositivo
- Gestión de riesgos para la toma de decisiones oportunas
- Gestión de aprobaciones automatizadas
- Reducción de errores generados por tareas repetitivas y manuales

Misión

Somos una empresa orientada al desarrollo y comercialización de soluciones para el soporte de sistemas de gestión empresarial, que agregan valor a nuestros aliados comerciales para lograr la excelencia y seguridad.

Promovemos el desarrollo personal y profesional de nuestro Talento humano para asegurar la sostenibilidad y el compromiso con la responsabilidad social empresarial.

Contacto

nilsa.sanabria@iscontacto.com
nsanabria_1@hotmail.com

+58 .824.84.17 / +58 414 420.23.78

Un modelo enfocado en prevenir riesgos, optimizar operaciones y proteger personas, activos e infraestructuras críticas.

PACTUM S.R.L.

SEGURIDAD INTEGRAL CON TECNOLOGÍA Y ESTRATEGIA

La integración de C4D SRL y Fortaleza y Tecnología permite ofrecer **servicios especializados de seguridad, tecnología avanzada y desarrollo de plataformas** y software para monitoreo y control.

Av. Perimetral 6to anillo
Edif. Las Torres de la Sierra
Of. 123 - piso 1

Tel.: +591 76755794

PACTUM S.R.L.

Estructura estratégica que articula experiencia operativa, innovación tecnológica y gestión avanzada del riesgo en el ámbito de la seguridad integral.

A través de C4D SRL y Fortaleza y Tecnología, se impulsan soluciones que comprenden:

- Administración de servicios de seguridad.
- Comercialización de equipamiento tecnológico especializado.
- Desarrollo, implementación y operación de plataformas y software para resguardo y gestión de seguridad.

Capacidades diseñadas para proteger activos críticos y fortalecer la resiliencia operativa.

Av. Perimetral 6to anillo - Edificio Las Torres de la Sierra Of. 123 piso 1 - Tel.: **+591 76755794**

LÍDERES DE PENSAMIENTO

Un puente de conocimiento para la seguridad en Hispanoamérica

Líderes de Pensamiento es el nuevo espacio de la revista Seguridad en Acción Venezuela diseñado para conectar las mentes más brillantes del sector en toda la región. En esta sección, profesionales de alto nivel de Iberoamérica comparten su visión, analizan las facetas más complejas de la seguridad y realizan un ejercicio necesario de comparación: ¿cómo se ejecutan las mejores prácticas en sus países de origen frente a la realidad de Venezuela? Nuestro objetivo es claro: profesionalizar el sector a través del intercambio de experiencias y la visión estratégica de quienes marcan el camino.

La Entrevista: Resiliencia, Tecnología y el Factor Humano

1. "Sensei, usted siempre dice que 'lo único permanente es el cambio'. En este 2026, donde la IA es una herramienta operativa, ¿cómo se mantienen vigentes los cimientos del POA (Protection of Assets) de ASIS? ¿La tecnología nos está haciendo olvidar las bases técnicas de los 80?"

R: Como dice la ley de Amara: tendemos a sobrestimar a corto plazo el impacto de las nuevas tecnologías y a subestimar a largo plazo sus consecuencias. La IA es un apoyo, pero creo que aún está lejos de ser lo suficientemente precisa para dejarla trabajar sola en seguridad. Por ahora, la Inteligencia Natural (IN) debe prevalecer. Debemos usar la IA para colección básica de información, pero complementarla con la revisión, conclusiones y recomendaciones humanas. Los fundamentos siguen siendo los mismos; de hecho, nuevas normas ISO ya señalan la necesidad de analizar los riesgos que el mismo uso de la IA nos está generando.

2. "¿Cuáles son las tres lecciones que la seguridad privada mexicana puede heredarle a la venezolana para mantener la continuidad de negocio en entornos de altísima incertidumbre?"

R: Primero, el compliance laboral y administrativo, ya que la regulación es cada vez más estricta y costosa. Segundo, la revalorización de los costos y precios de la seguridad privada para que se equilibren con los costos reales y no se propicien argucias legales para evadir el pago justo. Tercero: la formación y certificación del personal y sus procesos para cumplir cabalmente con los acuerdos de nivel de servicio pactados con el cliente.

3. "En una era de vigilancia autónoma, ¿cómo debe el Director de Seguridad gestionar el miedo de su personal y clientes sin caer en la paranoia, pero manteniendo el 'instinto de supervivencia'?"

R: Lo que dispara los mecanismos de supervivencia en una emergencia es la inyección de adrenalina que genera el miedo a un daño inminente. Esto es muy diferente a la falsa idea de que la seguridad se logra "vendiendo miedo". Un directivo debe desarrollar un programa de concientización (security awareness). Cuando desde la dirección hasta el trabajador operativo entienden el valor de los comportamientos seguros y visualizan las consecuencias graves de no hacerlo, su actitud hacia la seguridad cambia por completo.

4. "Para un profesional venezolano, ¿por qué obtener el CPP en 2026 sigue siendo un 'seguro de vida' para su carrera?"

R: He visto crecer la comunidad de profesionales certificados en Venezuela de uno solo (Carlos Flores) a más de 30, apoyando directamente a más de 8 a lograrlo. Aunque el clima político y económico no ha sido propicio y muchos terminan saliendo del país atraídos por mejores ofertas, quienes lo han logrado siempre señalan que la certificación les abrió puertas para nuevas oportunidades y mejoras profesionales.

La seguridad no se gestiona con miedo, sino con conciencia. El instinto de supervivencia se fortalece creando cultura, no paranoia.

5. "¿Hacia dónde debe mirar el líder de seguridad que ya tiene las certificaciones, pero siente que el mundo corre más rápido que sus manuales?"

R: El CPP es la base, la certificación "gold", pero obtenerlo no es suficiente. Al alcanzarlo, uno se da cuenta de que solo la actualización permanente y la diversificación te mantienen vigente y "deseable" para el mercado. Muchos CPP buscan certificaciones adicionales como el PSP (Physical Security Professional) o el PCI (Professional Certified Investigator) de ASIS, o miran hacia agrupaciones como ACFE, ICA o ISACA para particularizar tópicos. Y esto no es cuestión de edad: "el hombre no deja de aprender cuando se hace viejo, más bien se hace viejo cuando deja de aprender".

Adolfo M. Gelder

Lic. Rubén Fajardo
El "Sensei" de la Seguridad Latinoamericana

Director General de SIPROSI CORPORATIVO, Rubén Fajardo es una de las figuras más respetadas en el ámbito de la seguridad corporativa global. Con una trayectoria que lo ha llevado a trabajar con profesionales venezolanos desde 1997 y a conocer profundamente el suelo venezolano durante más de 15 años, Fajardo es reconocido por su labor incansable en la formación y mentoría de candidatos a certificaciones internacionales. Su sabiduría combina el rigor técnico de los fundamentos de ASIS International con una visión pragmática sobre el cambio y la supervivencia profesional.

ENTREVISTA

Ing. Juan Pirela

Director General de Fractal Solutions

En un entorno empresarial cada vez más expuesto a fallas de infraestructura y riesgos digitales, la ciberseguridad se ha convertido en un pilar de la continuidad operativa. En esta entrevista, el ingeniero Juan Pirela, director de Fractal Solutions, explica por qué las empresas venezolanas deben dejar de pensar solo en conectividad y comenzar a construir infraestructuras tecnológicas resilientes capaces de resistir crisis y garantizar la operación del negocio.

1. "Juan, tu empresa no lleva por nombre Fractal 'Internet', se denomina Fractal Solutions. En un mercado saturado de proveedores que solo venden 'megas', ¿cómo logras que el empresario venezolano entienda que lo que realmente necesita no es más ancho de banda, sino una arquitectura de red inteligente que soporte las crisis que hemos visto este primer trimestre de 2026?"

Ing. Juan Pirela: Fractal es una empresa de consultoría de Ciberseguridad y telecomunicaciones. Por lo que respondo modificando la pregunta a: "¿cómo logras que el empresario venezolano entienda que necesita robustecer su postura de ciberseguridad que soporte las crisis que hemos visto este primer trimestre de 2026?"
Lograr que el empresario venezolano entienda la necesidad de robustecer su postura de ciberseguridad no pasa primero por la tecnología, sino por traducir la ciberseguridad al lenguaje de la alta gerencia.

Históricamente, el empresario ha operado bajo múltiples riesgos simultáneos como la inestabilidad económica, fallas eléctricas, interrupciones de conectividad y presión operativa constante. A este contexto se suma el impacto que tiene la materialización de un evento de ciberseguridad, el cual puede tener consecuencias desastrosas para la organización.

Es por esto que la ciberseguridad debe presentarse no como un gasto tecnológico, sino como un mecanismo de continuidad del negocio. Para lograr transmitir este mensaje, es necesario hablar en términos de impacto financiero, no técnico; asociar la ciberseguridad con resiliencia operativa y como ventaja competitiva, y presentar los beneficios de aumentar progresivamente el nivel de madurez de ciberseguridad de la organización

En conclusión, el empresario comprende la necesidad de la ciberseguridad cuando deja de percibirla como un concepto tecnológico abstracto y empieza a verla como un seguro operativo que le permite sobrevivir, operar y crecer en un entorno permanentemente incierto.

2. "Como comunicador en 'Bit a Bit', analizas la tecnología global, pero como consultor en Venezuela te toca 'apagar fuegos'. Tras los eventos del pasado sábado 3 de enero, ¿cuál fue el error conceptual más común que encontraste en las empresas que quedaron fuera de juego y cómo Fractal Solutions está 'curando' esas infraestructuras para que no se repita la historia?"

Ing. Juan Pirela: Diversas fuentes reportaron fallas en la conexión de internet en distintas zonas de Caracas por motivos de fallas eléctricas durante la madrugada del 3 de enero.

En este sentido, la realidad es que las empresas se vieron afectadas debido al error conceptual común de creer que la ciberseguridad es proteger sistemas, cuando en realidad se trata de proteger la continuidad del negocio. Es decir, las organizaciones deben evitar confundir disponibilidad tecnológica con continuidad de negocios, y evitar los esquemas de seguridad reactiva en lugar de la resiliencia.

Para lograr esto, desde Fractal Solutions buscamos fomentar el desarrollo de infraestructuras tecnológicas resilientes para las organizaciones, y convertir la ciberseguridad en cultura operativa como eje principal de las estrategias de mitigación de riesgos de ciberseguridad en las empresas.

3. "A través de la radio educas al soberano y a través de Fractal proteges al corporativo. ¿Cómo ves el rol de los medios especializados para combatir la 'infodemia' y el miedo digital? ¿Es posible tener una Venezuela segura si no logramos llevar el mensaje técnico al lenguaje coloquial del dueño de negocio?"

Ing. Juan Pirela: El futuro exige que la ciberseguridad sea percibida como un problema que va mas allá de lo técnico; es un tema que tiene implicaciones en nuestro día a día y que puede afectarnos personalmente. Transmitir esto es vital, por lo que hemos abordado este problema desde una perspectiva comunicacional.

Desde Bit a Bit, buscamos crear un espacio de divulgación donde el ciudadano puede acceder a información sobre temas complejos de tecnología a través de conversaciones con expertos referentes del área.

A través del programa en vivo, y del canal de youtube, buscamos luchar contra la infodemia traduciendo la complejidad técnica de la ciberseguridad en información útil, tanto para el ciudadano como para el personal técnico de las organizaciones.

Por otra parte, honestamente, no podemos construir una Venezuela segura, a nivel digital, sin elevar los niveles de madurez de ciberseguridad en el país. Para lograrlo, debemos traducir la complejidad de esta área a un lenguaje sencillo que pueda entender el dueño de un negocio. Esta es la única forma de dar a conocer el riesgo que corre la organización y motivar al dueño a tomar acción.

En conclusión, no tendremos empresas seguras si primero no tenemos ciudadanos informados, y no tendremos ciudadanos informados si el conocimiento técnico sigue hablándose solo entre técnicos

La ciberseguridad debe presentarse no como un gasto tecnológico, sino como un mecanismo de continuidad del negocio.

4. "En 'Bit a Bit' siempre hablas de tendencias, pero vamos a lo disruptivo: ¿Estamos en Venezuela preparados para un ciberataque que no busque robar dinero, sino paralizar físicamente la producción de una zona industrial? ¿Cómo transforma Fractal Solutions una red vulnerable en una verdadera 'muralla digital' invisible?"

Ing. Juan Pirela: En Bit a Bit hablamos de tendencias y noticias de ciberseguridad a nivel mundial, por lo que sabemos que hoy los ataques no solo se enfocan en robar datos, también buscan la interrupción de los procesos del negocio.

El país aún está adaptándose a los desafíos que presenta la gestión de la ciberseguridad. Hoy observamos que las organizaciones abordan esta área con un enfoque erróneo al buscar unir las funciones de seguridad de la información con el departamento de tecnología, lo que diluye el enfoque de gestión de riesgos de ciberseguridad.

Desde Fractal, buscamos apoyar la resiliencia de los procesos de negocio a través de la categorización de activos que sostienen la operación de la empresa y modelar sus amenazas. Todo esto para crear mapas de ataque que permiten visualizar como una vulnerabilidad impacta la continuidad operativa. Con esta metodología de trabajo logramos identificar elementos de monitoreo y dimensionar las soluciones tecnológicas que necesitan nuestros aliados comerciales para la mitigación de sus riesgos de ciberseguridad y asegurar la resiliencia del negocio.

5. "Un fractal es una figura que se repite a diferentes escalas. Si el éxito de una empresa venezolana en 2026 depende de su seguridad y conectividad, ¿cuál es ese patrón o ese 'bit' de información que Juan Pirela le daría a los lectores de esta revista para que su crecimiento sea escalable y, sobre todo, invulnerable a los apagones tecnológicos que acechan la región?"

Ing. Juan Pirela: Un fractal es fascinante porque puedes ver el mismo patrón sin importar cuanto acerques la mirada. La ciberseguridad debe tener esa característica en nuestras empresas, debe aparecer como un patrón constante sin importar qué área de la organización se observe y a qué escala.

Es por esto que el "bit" de información que puedo aportar para los lectores es: "Diseñen los procesos del negocio preparándose para lo peor, mientras esperan lo mejor", es decir diseñen la empresa para que cuando falle, no se detenga.

Adolfo M. Gelder

Editor Revista Seguridad en Acción Venezuela En representación de Seguridad en Acción LATAM

ENTREVISTA

NILSA SANABRIA
CEO de IS Contacto

Consultora internacional con más de 35 años de experiencia en sistemas de gestión, creadora de IS Contacto, un aplicativo web que ha traspasado fronteras y hoy permite a empresas de Latinoamérica gestionar de forma integrada normas ISO, BASC, OEA y otros estándares internacionales, especialista en Riesgos y Continuidad de Negocio.

IS Contacto ofrece beneficios clave:

- **Integración real de múltiples normas en un solo sistema**
- **Automatización de procesos, evidencias y controles**
- **Trazabilidad completa y auditorías más rápidas**
- **Reducción de costos operativos y administrativos**
- **Gestión de riesgos centralizada**
- **Indicadores en tiempo real**
- **Eliminación del papel y de la duplicidad documental**
- **Acceso desde cualquier país, 24/7**
- **Arquitectura segura y escalable**
- **Actualizaciones alineadas a nuevas versiones ISO**

1. LA DECLARACIÓN DE LONDRES Y EL CAMBIO CLIMÁTICO

Pregunta:

"Nilsa Sanabria, CEO de IS Contacto, ¿cómo convence a un empresario venezolano de que la sostenibilidad no es una moda europea, sino un requisito global?"

Respuesta:

"La Declaración de Londres incorporó el cambio climático como requisito obligatorio en todas las normas ISO. Esto significa que la sostenibilidad dejó de ser un concepto aspiracional y se convirtió en un criterio de cumplimiento financiero, legal y comercial.

Desde IS Contacto lo vemos todos los días: las empresas que no gestionan riesgos climáticos quedan fuera de cadenas de suministro internacionales, pierden acceso a financiamiento y se vuelven menos competitivas.

Nuestro aplicativo es de fácil adaptación ya que su estructura permite seguir de manera fluida el proceso de carga e integra automáticamente los módulos por lo que asegura la trazabilidad completa. Permite abordar todos los requisitos de las normas que la empresa adopte sin costo adicional incluyendo los aspectos relacionados a los cambios climáticos, permitiendo que incluso empresas venezolanas —con recursos limitados— cumplan con estándares globales sin aumentar su carga operativa.

Adicionalmente apoyamos en la migración de la data, para el máximo aprovechamiento de los aplicativos.

La sostenibilidad no es una moda: es un requisito para seguir haciendo negocios en el mundo real."

2. VENEZUELA VS. EL MUNDO: LA RESILIENCIA

Pregunta:

"¿Las empresas venezolanas con ISO 22301 están mejor preparadas para crisis globales?"

Respuesta:

"Definitivamente sí. Venezuela ha sido un laboratorio natural de resiliencia.

Las empresas que hoy implementan ISO 22301 ya han vivido apagones, fallas logísticas, restricciones regulatorias y volatilidad económica. Eso les da una ventaja operativa real.

En IS Contacto hemos visto que las organizaciones venezolanas que digitalizan con un modelo estructurado su continuidad de negocio logran:

• Responder más rápido a interrupciones

• Mantener operaciones críticas activas

• Documentar incidentes con precisión

• Tomar decisiones basadas en datos

Mientras otros países simulan escenarios, en Venezuela se viven a diario.

Por eso, cuando una empresa venezolana se certifica, su nivel de madurez es superior al promedio regional."

3. DIGITALIZACIÓN: EL FIN DEL CONSULTOR DE CARPETAS

Pregunta:

"Con la ISO 9001:2026, ¿estamos viendo el fin del consultor tradicional?"

Respuesta:

"Definitivamente. La ISO 9001:2026 exige gobernanza de datos, digitalización e inteligencia artificial.

El consultor que llenaba carpetas ya no tiene espacio en este nuevo ecosistema.

IS Contacto nació precisamente para cerrar esa brecha.

Nuestro aplicativo automatiza:

- Flujos de aprobación
- Control documental
- Indicadores
- Auditorías
- Riesgos
- Acciones correctivas

Hoy el valor no está en producir documentos, sino en diseñar procesos digitales que generen evidencia en tiempo real.

Las empresas que siguen en papel no solo pierden eficiencia: pierden cumplimiento normativo."

4. SALUD MENTAL Y BIENESTAR EN ISO 45001

Pregunta:

"¿Cómo se integra la salud mental como indicador de productividad en Venezuela?"

Respuesta:

"La evolución de ISO 45001 exige gestionar riesgos psicosociales con la misma rigurosidad que cualquier otro riesgo operativo.

En un país como Venezuela, donde la presión económica y social afecta al trabajador, esto es crítico.

IS Contacto permite:

- Registrar factores psicosociales
- Medir indicadores de clima laboral
- Gestionar incidentes emocionales
- Automatizar encuestas de bienestar
- Integrar salud mental en la matriz de riesgos

La salud mental ya no es un beneficio: es un KPI de productividad, rotación y continuidad operativa."

5. LA ISO VENEZOLANA: GOBERNANZA BASADA EN RIESGO

Pregunta:

“Si diseñara una ISO a la venezolana, ¿cuál sería su pilar fundamental?"

Respuesta:

“Sería la gobernanza basada en riesgo.

Un modelo que integre calidad, ciberseguridad, seguridad física, BASC, OEA y continuidad de negocio en un solo sistema.

Eso es exactamente lo que hace IS Contacto:

centraliza riesgos, controles, indicadores y evidencias en una sola plataforma.

Una empresa que gobierna sus riesgos:

• Es más rentable

• Es más ética

• Es más sostenible

• Es más competitiva

Ese es el futuro de la gestión en Venezuela y en el mundo."

INTERNATIONAL SEGURITY ALLIANCE

INSEAL

"Te conviertes en lo que entrenas"

PROTECSOFT

Inteligencia que integra, software que impulsa

Sistema de gestión empresarial. Transforma la forma en que operas, te conectas con clientes y procesas pagos.

Ventajas Clave

- Sistemas tropicalizados
- Más de 50 Gb de aplicaciones integradas
- Código cerrado y seguro
- Disponible en la nube con seguridad robusta
- Desarrollamos todo lo que necesite tu empresa

100+
Empresas confían en PROTECSOFT

400+
Usuarios activos

Sobre Nosotros

Somos una empresa enfocada en el desarrollo de software a medida, aplicaciones web y móviles, y soluciones en la nube, con el objetivo de aumentar la productividad organizacional tanto pública como privada. Nos especializamos en crear herramientas seguras y escalables para automatizar procesos, gestión de ventas y pedidos, incluyendo funciones administrativas.

10+
Cantidad de desarrolladores

¿Listo para transformar tu negocio?

Agenda tu presentación gratuita

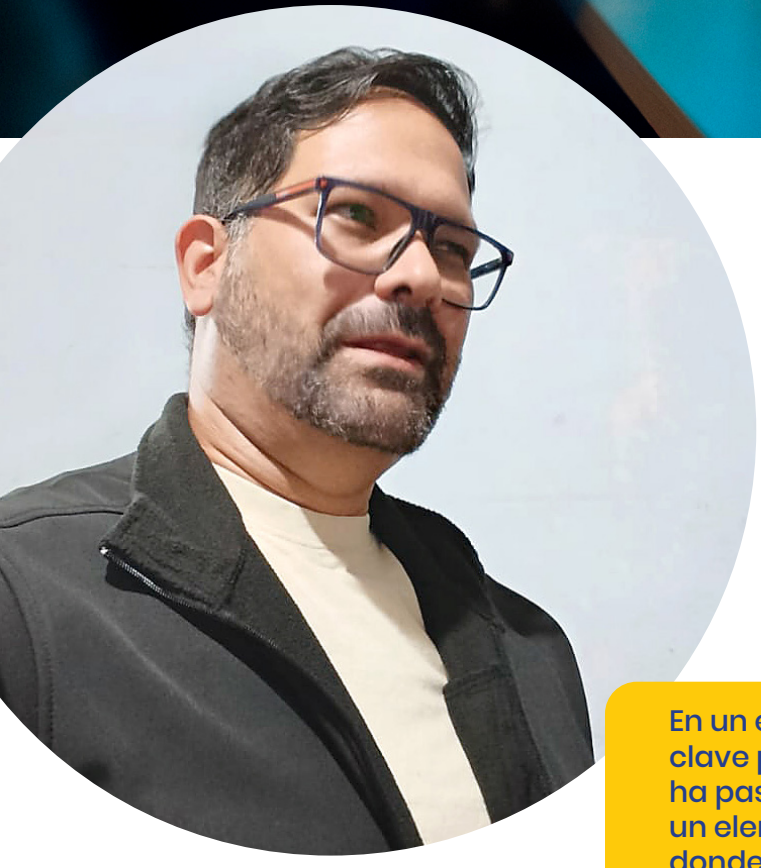
Visita protecsoft.pro

WhatsApp: +58 4149529039 | +58 426 5364624 | +58 412 2323903

info@protecsoft.pro

INFRAESTRUCTURA INTELIGENTE:

El Nuevo Escudo Digital de las Empresas en Venezuela



En esta entrevista, **Clarence Lemus, director general de Stellionet**, explica cómo la infraestructura inteligente, la ciberseguridad gestionada y la continuidad operativa se han convertido en pilares para proteger la información, garantizar conectividad y fortalecer la soberanía digital de las organizaciones.

En un entorno donde la estabilidad tecnológica es clave para la continuidad empresarial, la conectividad ha pasado de ser un simple servicio a convertirse en un elemento estratégico de seguridad. En Venezuela, donde las fallas de infraestructura pueden paralizar operaciones completas, las empresas necesitan redes resilientes capaces de anticipar riesgos y mantener la operación activa.

1. Sobre la infraestructura como escudo

"En Venezuela, la frase 'se cayó el sistema' es el mayor enemigo de la productividad. Para Stellionet, la conectividad no es solo un servicio de internet, es la columna vertebral de la seguridad de una empresa. En este 2026, ¿cómo han logrado diseñar una infraestructura que garantice que, incluso en los escenarios más críticos de conectividad nacional, sus clientes sigan operando mientras la competencia se queda a oscuras?"

En Stellionet entendimos hace años que en Venezuela la conectividad no es un lujo: es un mecanismo de defensa. Por eso diseñamos una infraestructura que no depende de un solo proveedor ni de un solo camino. Combinamos enlaces redundantes, rutas inteligentes, SD WAN, VPN de alta disponibilidad y monitoreo en tiempo real, todo sobre una arquitectura que anticipa fallas en lugar de reaccionar a ellas.

Mientras otros esperan a que "vuelva el internet", nuestros clientes ya están operando por rutas alternas, túneles seguros o enlaces de respaldo que se activan en segundos. La diferencia no está en tener más megas, sino en tener una red que piensa, decide y se adapta. Esa es la razón por la que, incluso en los peores escenarios de conectividad nacional, nuestros aliados siguen trabajando mientras la competencia se queda a oscuras.

2. Sobre la lección del 3 de enero

"Los eventos del pasado sábado 3 de enero pusieron a prueba la capacidad de respuesta de todo el sector tecnológico en el país. Desde la perspectiva de Stellionet, ¿cuál fue el gran aprendizaje de esa contingencia y cómo ha evolucionado su oferta de servicios gestionados (MSP) para asegurar que una falla en la infraestructura pública no se traduzca en una vulnerabilidad digital para sus aliados?"

El 3 de enero fue un recordatorio contundente: la infraestructura pública no es infalible, y depender de ella sin un plan B es una vulnerabilidad. Ese día validamos algo que veníamos impulsando: la resiliencia no se improvisa.

El gran aprendizaje fue que la continuidad operativa debe ser gestionada como un servicio, no como un conjunto de equipos. Por eso evolucionamos nuestra oferta MSP hacia un modelo donde Stellionet no solo monitorea, sino que predice, automatiza y ejecuta. Hoy nuestros clientes cuentan con:

- Failover inteligente entre proveedores.
- Políticas de seguridad centralizadas.
- Alertas proactivas basadas en comportamiento.
- Respuesta automatizada ante degradación de servicios.

La meta es simple: que una falla pública no se convierta en un incidente privado.

Un antivirus tradicional actúa cuando el daño ya está tocando la puerta. Una red inteligente actúa antes de que el atacante llegue al perímetro.

3. Sobre la Red Inteligente y la Ciberseguridad

"Hoy en día, el perímetro de seguridad de una empresa ya no termina en sus paredes, sino en su nube. Stellionet apuesta fuerte por soluciones como SD-WAN y seguridad gestionada; ¿podrían explicarnos de manera sencilla por qué una red 'inteligente' es hoy más efectiva para detener un ataque informático que un antivirus tradicional? ¿Es la red de Stellionet la primera línea de defensa de sus clientes?"

Un antivirus tradicional actúa cuando el daño ya está tocando la puerta. Una red inteligente actúa antes de que el atacante llegue al perímetro.

Con SD WAN, inspección profunda de paquetes, segmentación dinámica y políticas basadas en identidad, la red se convierte en un sistema nervioso capaz de detectar patrones anómalos, bloquear tráfico sospechoso y aislar amenazas en milisegundos. No espera firmas, no depende de actualizaciones: analiza comportamiento.

Por eso decimos que la red de Stellionet es la primera línea de defensa. No solo transporta datos: protege, filtra, decide y alerta. Es un escudo activo, no un simple canal.

4. Sobre la convergencia con la Seguridad Física

"Muchos de nuestros lectores invierten grandes sumas en cámaras de alta definición y control de acceso biométrico, pero olvidan que sin un 'tubo' de datos seguro y estable, esos equipos son inútiles. ¿Cómo colabora Stellionet con el ecosistema de seguridad física para garantizar que el monitoreo en tiempo real sea realmente 'en tiempo real' y no sea vulnerable a sabotajes digitales?"

La seguridad física dejó de ser analógica. Cámaras, biometría, control de acceso y monitoreo remoto dependen de un solo elemento: un tubo de datos confiable. Sin eso, la mejor cámara es solo un adorno costoso.

En Stellionet trabajamos para garantizar que cada dispositivo opere sobre una red blindada, segmentada y priorizada. Implementamos:

- VLAN dedicadas para CCTV y control de acceso.
- Protección Dos contra diversos vectores.
- Enlaces redundantes para evitar puntos únicos de falla.
- Túneles cifrados para monitoreo remoto sin riesgo de sabotaje digital.

El resultado es simple: si alguien intenta vulnerar la red, no solo no lo logra, sino que queda registrado. La seguridad física y la digital ya no son dos mundos; son un mismo ecosistema.

5. Sobre la soberanía de datos y el futuro de Venezuela

"Gestionar datos en Venezuela requiere un conocimiento profundo del entorno regulatorio y técnico local. Al mirar lo que resta del 2026, ¿cuál es el siguiente paso en la hoja de ruta de Stellionet para seguir siendo el socio estratégico de las empresas que no pueden permitirse un solo segundo de desconexión? ¿Hacia dónde llevan la soberanía digital de sus clientes?"

Operar datos en Venezuela exige entender la realidad técnica, regulatoria y geopolítica del país. Por eso nuestra hoja de ruta para 2026 se centra en soberanía digital, continuidad operativa y autonomía tecnológica.

La seguridad física dejó de ser analógica. Cámaras, biometría, control de acceso y monitoreo remoto dependen de un solo elemento: un tubo de datos confiable. Sin eso, la mejor cámara es solo un adorno costoso.

El siguiente paso es consolidar una plataforma donde las empresas puedan:

- Mantener sus datos seguros dentro del país o en nubes híbridas controladas.
- Operar incluso en escenarios de desconexión nacional.
- Integrar seguridad, conectividad y monitoreo en un solo ecosistema gestionado.
- Reducir dependencia de infraestructuras externas vulnerables.

Nuestro objetivo es claro: que cada cliente tenga el control total de su información y de su operación, sin importar lo que ocurra en el entorno. La soberanía digital no es un concepto político; es una necesidad empresarial. Y Stellionet está construyendo ese futuro desde hoy.

Adolfo M. Gelder | Revista Seguridad en Acción Venezuela En representación de Seguridad en Acción LATAM

INMUNIDAD OPERATIVA:
Recuperando el Control tras el Impacto Digital

Resiliencia industrial: blindaje de activos críticos ante el asedio cibernético.

La edición inaugural de esta publicación exploró con acierto la vulnerabilidad sistémica de la empresa venezolana frente a la "Selva Digital". Hoy, la narrativa técnica debe evolucionar hacia la necesidad de acción inmediata. Tras los eventos de ransomware que afectaron sectores críticos en el último trimestre de 2025, los directivos ya no solo preguntan si serán atacados, sino: **¿Cómo recupero mi operación si la red ya está comprometida y no puedo permitirme un solo día de inactividad?**

1. El Desafío Legacy

Venezuela posee una particularidad técnica marcada por la resistencia y la longevidad. En sectores estratégicos como el agroindustrial en Portuguesa, el manufacturero en Valencia o el logístico en el eje central, es habitual encontrar maquinaria controlada por sistemas operativos **Legacy** (Windows XP, Windows 7, Server 2003).

Aquí radica una distinción técnica crítica: la mayoría de los fabricantes globales ofrecen únicamente versiones "congeladas" para estos sistemas. Software antiguo que ya no recibe

actualizaciones de motor ni nuevas funcionalidades de defensa, limitándose a firmas de virus obsoletas.

Dr.Web rompe este paradigma al ofrecer **Soporte y Hardening Activo**. A diferencia de las versiones legacy de otras marcas que solo están ”presentes” de forma pasiva, el motor de Dr.Web en 2026 está diseñado para aplicar ingeniería de defensa moderna —como la protección contra inyección de procesos— directamente sobre kernels antiguos.

Figura 1: *Protección activa sobre sistemas heredados.*

2. Cirugía de Memoria RAM

El mito más destructivo en el soporte técnico nacional es que *”si una máquina se infectó, la única solución es formatear”*. Para un dueño de empresa, el formateo es sinónimo de catástrofe financiera y lucro cesante inaceptable.

Figura 2: *Intervención quirúrgica en procesos de memoria.*

La tecnología de **Dr.Web** introduce la **Desinfección en Caliente**. Gracias a su capacidad de **Autoprotección de Proceso**, el motor posee un controlador de nivel de núcleo [*Kernel-Mode Driver*] que impide que el malware lo detenga. Puede instalarse en máquinas ya infectadas para interceptar la memoria volátil [RAM], identificar los hilos de ejecución del malware y neutralizarlos quirúrgicamente sin necesidad de reiniciar el equipo.

3. Soberanía y MTTR

El eslabón más débil no es solo el error del usuario, sino la **lentitud en la recuperación**. Un ataque en una red de farmacias o supermercados puede paralizar los Puntos de Venta (POS) en todo el país.

Dr.Web reduce drásticamente el *MTTR [Mean Time To Recovery]* de días a minutos. Un factor vital en Venezuela es la autonomía: posee una base de virus interna y lógica de IA que no depende exclusivamente de una conexión a internet estable. En regiones con fallas de conectividad, la empresa mantiene su protección incluso ”offline”.

4. Comando CureNet!

Para los técnicos de seguridad que heredan redes ”envenenadas”, la utilidad **Dr.Web CureNet!** es la herramienta de respuesta definitiva:

- **Invisibilidad:** Escanea sin que el malware detecte el proceso.
- **Convivencia:** Opera sobre redes con otras soluciones instaladas.
- **Saneamiento:** Elimina virus y mineros de criptomonedas sin dejar rastros.

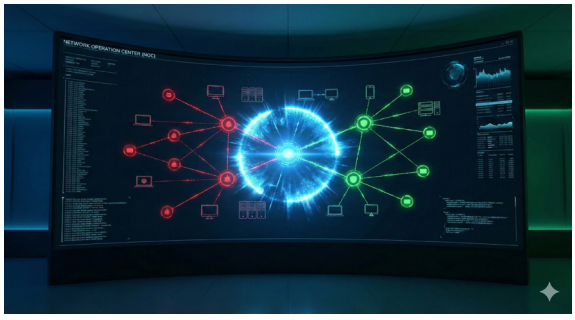


Figura 3: *Saneamiento centralizado de la red local.*

Conclusión

La ciberresiliencia no se construye con promesas comerciales, sino con ingeniería diseñada para la infraestructura real. En el mercado venezolano, proteger la inversión significa elegir soluciones que entiendan la escasez de recursos y la exigencia de producción ininterrumpida.

Dr.Web no es solo una barrera; es la garantía tecnológica de que los procesos vitales de la empresa seguirán funcionando.

BENEFICIO PARA LECTORES

En reconocimiento al compromiso de las empresas nacionales, los lectores podrán acceder a un **Incentivo de Actualización Tecnológica** al migrar a Dr.Web. Consulte con el consejo editorial para conocer los pasos de validación.

Colaboración Técnica Especial
Especialista Senior en Ciberresiliencia
Para Seguridad en Acción Venezuela

CONTACTO PREVENCIÓN INTEGRAL

Calidad, Seguridad y Desarrollo del Talento Humano para el éxito

Servicios que ofrecemos

- ISO 9001 Calidad
- ISO 14001 Gestión Ambiental
- ISO 18788 Seguridad Privada
- ISO 22301 Continuidad de Negocio
- ISO 27001 Seguridad de la Información
- ISO 28000 Seguridad en la cadena de Suministro
- ISO 31000 Gestión del Riesgo
- ISO 37001 Prevención de Soborno
- ISO 37301 Cumplimiento
- ISO 45001 Seguridad y Salud en el trabajo
- ISO 50001 Seguridad Energética
- Alianza para un Comercio Seguro: BASC y OEA

Beneficios de un Sistema de Gestión

- Satisfacción de los clientes
- Mejoramiento continuo del desempeño
- Aseguramiento de un servicio de excelente calidad y confiabilidad

¿Por qué contratar con nosotros?

Somos la empresa más innovadora del país por el desarrollo de sistemas automatizados para cada proceso que facilitan la gestión.

Servicio integral, tiempos de respuesta, adaptabilidad a las necesidades y circunstancias

Contacto

nilsa.sanabria@contactoprevencionintegral.com
nsanabria_1@hotmail.com

+58 .824.84.17 / +58 414 420.23.78

LA SEGURIDAD DE LA INFORMACIÓN COMO POLÍTICA PÚBLICA

ANÁLISIS ESTRATÉGICO, JURÍDICO Y CRIMINOLÓGICO ANTE LOS DESAFÍOS Y AMENAZAS PARA EL ESTADO VENEZOLANO

La Seguridad de la Información en el Ciberespacio como Política Criminal en Venezuela. Aportes desde la perspectiva de la Criminología Crítica.

La Seguridad de la Información en el Ciberespacio se constituye en un desafío para la Política Criminal en Venezuela debido a que en el mismo confluyen individuos y/o grupos de diferentes características y con intereses de diversas índoles, en ocasiones diametralmente opuestos. Desde la perspectiva de la Criminología Crítica y su posición con respecto a la lucha de clases y la dominación de los poderosos, las formas de control social sobre la misma pueden ser consideradas un medio de dominación. En función de estas premisas, las actividades ilícitas y las conductas desviadas relacionadas con la Seguridad de la Información en el Ciberespacio van a depender en buena medida del contexto político, social y económico en donde se desarrollan. Además, el análisis a la dinámica del conflicto en torno a éstas debe ser bien preciso ya que los crímenes o actos dañinos pueden constituirse en individuales, grupales, organizacionales o hasta estatales.

Sin lugar a dudas, todas y cada una de las personas que viven en el mundo actual, se relacionan y/o confluyen de una manera u otra en el Ciberespacio. Desde abrir una página web, llamadas telefónicas, correos electrónicos, una noticia, broma, vídeo o fotografía compartida en las redes sociales, un videojuego en donde participan varios usuarios en red, transacciones electrónicas bancarias, videoconferencias, firmas electrónicas, hasta el análisis de tráfico de las comunicaciones, espionajes y/o ataques tecnológicos, todos son actores de manera directa o indirecta en este medio virtual.

Venezuela no se escapa a esta realidad. Según los datos de la Comisión Nacional de Telecomunicaciones (CONATEL) publicados en su página web para el año 2014, la población venezolana que se estimaba en 30.206.307 habitantes (INE, 2014) poseía 30.325.373 líneas de teléfonos móviles activas. Es decir, más de una línea activa por cada persona. A nivel de telefonía fija, 93% de los hogares venezolanos contaban con este tipo de servicio y el uso de voz por telefonía móvil alcanzó para el segundo trimestre de 2014 los 11.991 millones de minutos con 28.662 millones de mensajes de texto SMS enviados (CONATEL, 2014).

Además, según los datos del uso de la internet para el segundo trimestre de 2014 el número de usuarios frecuentes y estables llegó a la cifra de 13.300.000 con una penetración del 44%, siendo los correos electrónicos utilizados con más frecuencia los de Microsoft (Hotmail o Outlook) y de Google (Gmail), las búsquedas a través de los motores de Google, Microsoft (Bing) y Yahoo, así como las redes sociales Facebook y Twitter, para mensajería el servicio Skype y en almacenamiento masivo en la nube a través de Drive y Dropbox. Por último, en la mayoría de los casos se está utilizando el sistema operativo Windows de Microsoft para las computadoras, el Android de Google para Smartphone, en "mensajería instantánea" el WhatsApp de Facebook y el PIN de Blackberry (CONATEL, 2014).

Estas nuevas realidades deben conllevar a redefinir la perspectiva criminológica sobre las oportunidades, métodos y medios de cometer conductas desviadas perjudiciales y delitos en este entorno, así como comprender que las variables de tiempo y espacio tal y como se conocen en el medio físico, son totalmente diferentes en este medio virtual. Por ende, lo que se sabe y ejerce a manera de control social en los espacios tradicionales, no se puede aplicar en el ciberespacio.

Por otro lado, además de estas interacciones tecnológicas de la vida cotidiana, existen otras que son mucho más importantes a nivel colectivo, como lo son las infraestructuras informáticas críticas y las instituciones estratégicas del Estado, que se encargan de velar por el bienestar de todos los ciudadanos, tales como las hidroeléctricas, Petróleos de Venezuela S. A. (PDVSA), el Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT), el

Venezuela fue pionero a nivel latinoamericano en cuanto al tema de la seguridad informática al promulgar la Ley Especial contra Delitos Informáticos en el año 2001, el marco legal en esta materia en la actualidad se encuentra desfasado, debido precisamente a la velocidad con que la tecnología avanza

Servicio Administrativo de Identificación, Migración y Extranjería (SAIME), el Consejo Nacional Electoral (CNE), entre otras. De esta manera, la perspectiva de algún tipo de actividad perjudicial o ilícita en este ámbito, se redimensiona hasta llegar al nivel de políticas públicas de seguridad de Estado.

Adicionalmente, cuando el consultor tecnológico estadounidense Edward Snowden, antiguo funcionario de la Central Intelligence Agency (CIA) y la National Security Agency (NSA), hizo público en junio de 2013 los programas de vigilancia masiva que a nivel mundial utilizan estas agencias de inteligencia norteamericanas para espiar a los gobiernos y en general a todos los países del planeta, entre los cuales surgió el nombre de Venezuela como uno de los principales, la perspectiva del problema del ciberespacio se sobredimensionó de manera indiscutible, convirtiéndose en tema de discusión fundamental como fenómeno social desde la perspectiva de la política criminal (The Guardian, 2013).

De hecho, Snowden hizo público un documento de inteligencia fechado en marzo de 2011, con la etiqueta "ultra secreto" (Telám S. E., 2015). En este se afirma que la NSA con la ayuda de la embajada de Estados Unidos (EEUU) en Venezuela espió las comunicaciones internas, correos electrónicos, perfiles de empleados y otros datos de la estatal PDVSA incluyendo a funcionarios de alto nivel miembros de la directiva de la misma (Telám S. E., 2015). El documento habría sido producido por un analista de la NSA y en el mismo se menciona que el propio individuo entró a la red interna de PDVSA aproximadamente a finales del año 2010.

Entre los datos a los que tuvo acceso dicho individuo estuvo el tráfico de correos electrónicos, más de 10 mil perfiles de empleados de PDVSA con direcciones de email, números de teléfono, nombres de usuario y contraseñas. Este acto de pesquisa coordinado entre la NSA y la embajada de EEUU en Venezuela -parafraseando el mencionado documento- les permitió aseverar que "entender PDVSA es entender el corazón económico de Venezuela" (Telám S. E., 2015).

En otro orden de ideas, si bien Venezuela fue pionero a nivel latinoamericano en cuanto al tema de la seguridad informática al promulgar la Ley Especial contra Delitos Informáticos en el año 2001, el marco legal en esta materia en la actualidad se encuentra desfasado, debido precisamente a la velocidad con que la tecnología avanza, la disponibilidad de ésta para el grueso de la población, la penetración de las redes sociales, el alcance de las telecomunicaciones y la gran cantidad de oportunidades para cometer actos delictivos o conductas desviadas perjudiciales que esto representa, lo cual ha introducido una gran cantidad de cambios culturales en el mundo y por tanto en la sociedad venezolana.

Es importante señalar, que en este trabajo es absolutamente necesario retomar la disyuntiva legendaria entre las tecnologías libres y las tecnologías privativas (haciendo referencia no solo al software sino también al hardware), para establecer los pro y los contra de cada una de ellas, en función del establecimiento de políticas de ciberseguridad y ciberdefensa efectivas, como problemas legales, técnicos y sociales en Venezuela.

Las teorías del conflicto en criminología han venido encasillando al control social de la conducta delictiva dentro del marco de la lucha de clases, de la confrontación entre sectores y grupos sociales diversos con intereses encontrados o confrontados.

Con base en estas teorías se puede aseverar que el ciberespacio constituye un lugar donde confluyen individuos y grupos de diferentes características y con intereses de las más diversas índoles, en muchas ocasiones diametralmente opuestos. Es importante resaltar que si se toma en cuenta la criminología crítica y su posición con respecto a la lucha de clases y la dominación de los poderosos, entonces el marco jurídico-legal que pretende controlar el ciberespacio puede ser visto como un medio de dominación. Esto es particularmente cierto si se toma en cuenta casos como el de los Estados Unidos, cuyas leyes permiten y promueven el espionaje tecnológico -interna y externamente- como instrumento de investigación para la famosa guerra contra el terrorismo, lo que ha producido el surgimiento de grupos de hackers que se hacen llamar "éticos", los cuales dicen luchar contra la hegemonía de los poderosos.

Las teorías del conflicto en criminología han venido encasillando al control social de la conducta delictiva dentro del marco de la lucha de clases, de la confrontación entre sectores y grupos sociales diversos con intereses encontrados o confrontados.

Debido a que la criminología crítica intenta romper con los paradigmas de la criminología tradicional, estructurándose en torno a una perspectiva macrosocial y política, se considera que ésta debe ser la teoría criminológica central para este trabajo de investigación, puesto que el ciberespacio se constituye en un problema legal y social desde la perspectiva de la política criminal, y por tanto, debe ser abordado con las herramientas de análisis propias de esta, de carácter político, económico y sociológico, que supera la visión restringida de la criminología tradicional.

En este sentido, se puede alegar que las principales premisas de la criminología crítica son: El contexto político, social y económico, la dinámica del conflicto, el ejercicio del poder y el control social preventivo.

Desde esta perspectiva, las actividades ilícitas o las conductas desviadas perjudiciales en el ciberespacio van a depender en buena medida del contexto político, social y económico en donde se desarrollan. Además, el mismo contiene una dinámica del conflicto muy particular, ya que los crímenes o actos dañinos pueden constituirse en individuales, grupales, organizacionales o hasta estatales. Por otro lado, dichas acciones se generan muy particularmente en torno al ejercicio del poder y la lucha de clases, entre los poderosos y los oprimidos. Y finalmente, tal y como lo plantea la criminología crítica, el control social formal e informal necesario para aplicar en el ciberespacio debe ser preventivo más que reactivo.

Situación problemática

En función de las principales premisas de la criminología crítica se tomaron en cuenta los aspectos legales, técnicos y sociales en Venezuela relacionados con el tema en estudio. Así, el contexto político y económico venezolano, la dinámica del conflicto y el ejercicio del poder en las últimas dos décadas han generado un marco legal con algunas fortalezas importantes relacionadas con la planificación, ejecución y control de lineamientos preventivos en la lucha contra los delitos y las conductas desviadas en el ciberespacio. No obstante, gran parte del mismo se haya desactualizado debido a la velocidad de los cambios tecnológicos y la penetración de las TIC en nuestra sociedad.

Por otro lado, este mismo ambiente político y económico ha producido grandes avances en torno a la creación de herramientas tecnológicas autóctonas y la adquisición de pericias científicas relacionadas con la seguridad informática. Sin embargo, aún existen inmensas necesidades de software, hardware y talento humano (profesionales en la materia) indispensables para alcanzar una verdadera independencia y soberanía tecnológica en nuestro país que garantice la Seguridad de la Información en el ciberespacio.

Y por último, las más profundas debilidades a ser atacadas desde el control social preventivo, se hallan en el medio social. Existe un desconocimiento generalizado de la población acerca de la importancia del uso de las tecnologías libres, además de los riesgos y peligros implícitos en el uso de las TIC, así como de las nociones básicas fundamentales relacionados con la independencia y la soberanía científico-tecnológica, menos aún lo que representa una Política Criminal responsable sobre el uso de las TIC y el papel de todos los ciudadanos en estas.

Solución propuesta y justificación

Desde Enrico Ferri en 1884 pasando por Karl Marx por esa misma época, el primero llegó a la conclusión que no era la pobreza en sí, sino la distribución desigual de la riqueza la que determina el nivel de la delincuencia; y el segundo expuso lo siguiente:

En la producción social de su vida los hombres se adentran en unas relaciones determinadas. Necesarias, independientes de su voluntad [...] El conjunto de esas relaciones de producción constituye la estructura económica de la sociedad, la base real sobre la que se alza un edificio jurídico y político y a las que responden unas determinadas formas de conciencia social. El tipo productivo de la vida material condiciona en definitiva el proceso vital social, político y espiritual. No es la conciencia del hombre la que determina su ser, sino que, a la inversa, es su ser social el que condiciona su conciencia (Molina, 2003: 177).

Los argumentos de Marx se han proyectado con contundencia a lo largo de los siglos XX y XXI, y aunque no propone un programa de política criminal, autores norteamericanos como Chambliss en 1975 y Quinney en 1972, también Taylor, Walton y Young en 1973 (The New Criminology), estructuraron un pensamiento criminológico marxista, impulsando estos últimos como premisa:

El poder utiliza todos los recursos y mecanismos a su alcance, incluida la propia ley y la justicia, para afianzar y mantener su posición dominante en la sociedad. Ello implicaría que los grupos no dominantes vendrían a convertirse en objetivos preferentes del control legal. […] La ley es mera fachada ideológica de la justicia universal armada para proteger al poderoso en la búsqueda de su propio interés particular (Taylor, Walton y Young, 1973: 87).

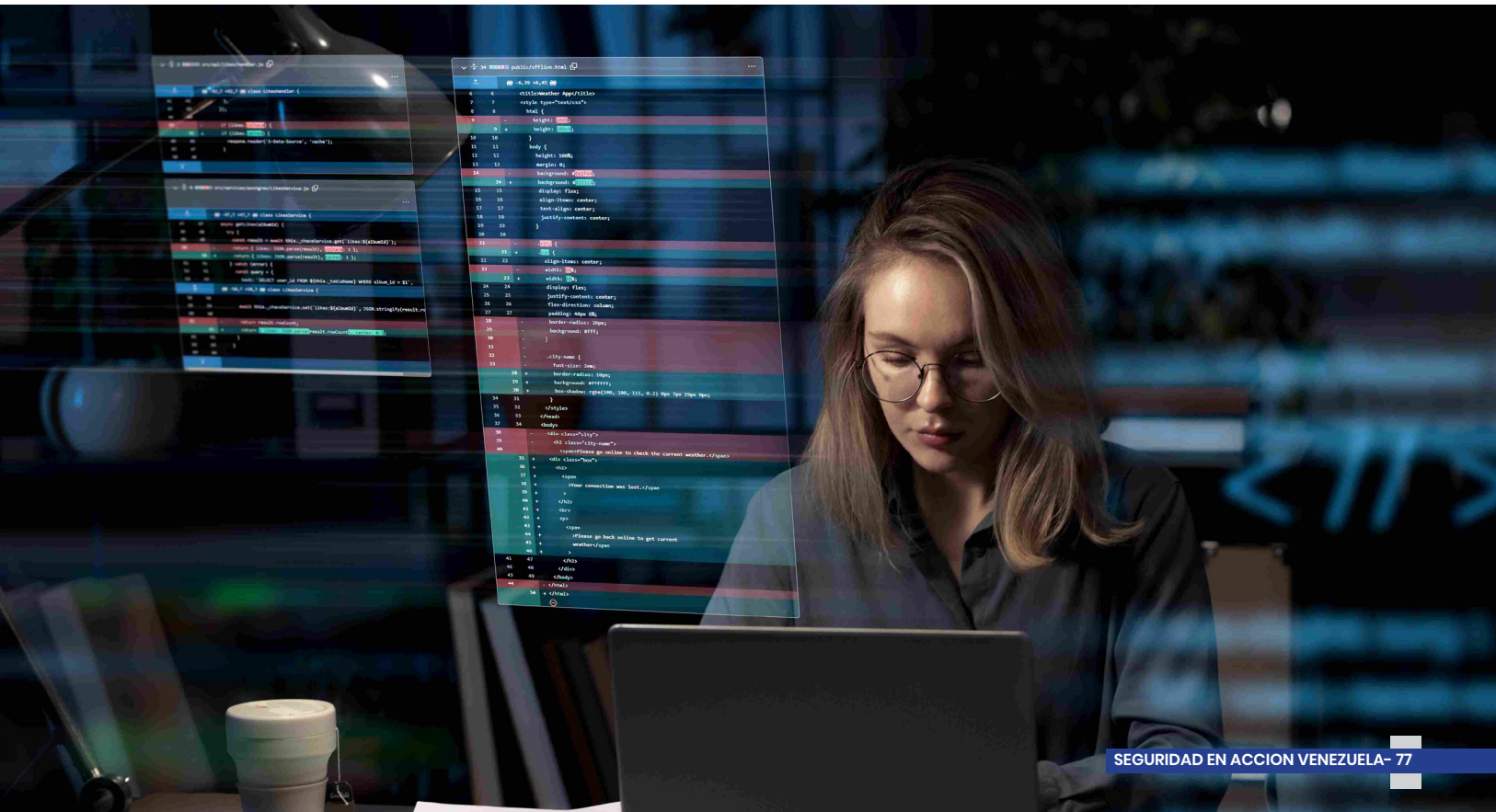
En esos años setenta del siglo XX, surge en el marco de las teorías del conflicto, nuevas críticas a la criminología tradicional, como ciencia causal explicativa -parafraseando a Jiménez de Asua (1950)- y se abocan un buen número de criminólogos al análisis del control social y los mecanismos de justicia como paradigma de la criminología crítica, nueva tendencia epistemológica de la criminología, sin que ello implique una nueva ciencia; pues es simplemente una visión del problema del conflicto social que se adhiere a la defensa de las clases dominadas como víctimas criminalizadas y reprimidas por el derecho penal, instrumento del Estado y de los grupos dominantes de la sociedad.

Algunos postulados de las teorías del conflicto consideran que el crimen es una función de los conflictos existentes en toda sociedad, sin que por ello tales conflictos deban reputarse necesariamente nocivos o disfuncionales. Pudiéramos establecer algunos postulados básicos de estas teorías según García Pablos de Molina:

- El orden social de una sociedad plural no descansa en un supuesto consenso, sino en el disenso. Puesto que el conflicto es inherente a la misma sociedad, ésta en la era actual es antagónica y conflictiva; parte de la evolución dinámica de los pueblos.

- El conflicto es funcional, puesto que generalmente contribuye a un cambio social positivo; no expresa el conflicto una realidad patológica, sino la propia estructura y la dinámica del proceso social.

- El Derecho representa los valores e intereses de las clases dominantes, no los intereses generales de la sociedad.



- La justicia penal integra el mecanismo del control social y gestionan la aplicación de las leyes de acuerdo con los intereses de las clases dominantes.

- El comportamiento desviado es una reacción al desigual e injusto reparto de poder y riqueza en la sociedad (Molina, 2003: 182).

De esta manera, puede admitirse que una de los aportes más importantes de las teorías del conflicto reside en la crítica desmitificación del paradigma "consensual". Con notorio realismo han puesto de relieve, que la sociedad moderna es una sociedad plural y, por tanto, necesariamente "conflictiva". Y que el conflicto puede contribuir de modo decisivo a la integración y al cambio social, tanto como el propio consenso.

Un determinado conflicto puede explicar ciertas manifestaciones de la criminalidad, eso parece indiscutible. Ahora todo hecho criminal no debe reconducirse a un conflicto existente en el sistema social; ello sería una generalización sin fundamento (Molina, 2003: 185).

En este sentido, se puede alegar que las principales premisas de la criminología crítica son:

- El contexto político, social y económico.
- La dinámica del conflicto.
- El ejercicio del poder.
- El control social preventivo.

8) Asuntos claves y recomendaciones de política pública

Propuestas en el marco jurídico

Para hacer más seguro el uso de las TIC para el Estado venezolano y todos sus ciudadanos, la proposición surgida desde la intervención criminológica es minimizar las carencias de nuestras leyes en la materia, para lo cual se proponen la ejecución de las siguientes acciones:

1.- Actualizar el glosario de términos informáticos contenidos en el marco legal vigente, incluyendo nuevos vocablos o expresiones utilizados en la materia en el presente, así como renovar los conceptos ya existentes.

2.- Incorporar nuevas tipificaciones delictivas que incluyan específicamente actividades contra infraestructuras críticas, acciones que pudiesen ser cometidas por un Estado foráneo en contra de Venezuela, la inferencia de información desde el análisis de tráfico de las comunicaciones a partir de las TIC y que además garanticen el anonimato, la privacidad y la identidad digital de todos los ciudadanos.

3.- Sancionar con todo el peso de la ley a los funcionarios públicos que no garanticen el uso de tecnologías libres en todas las instituciones, empresas y organismos del poder público e incluir en estas el uso obligatorio de formatos libres para el manejo e intercambio de datos e información.

4.- Impulsar desde el marco legal la integración y el intercambio de recursos tecnológicos y científicos con países vecinos y/o aliados a través de los organismos de integración existentes.

5.- Generar una Política Criminal eficiente y eficaz sobre el uso de las TIC cuya construcción se origine no solo desde el ámbito militar, sino con la participación de diversos actores profesionales, científicos y sociales que garanticen una verdadera Seguridad de la Información en el ciberespacio.

Propuestas en el marco técnico

Para hacer más seguro el uso de las TIC para el Estado venezolano y todos sus ciudadanos, la proposición surgida desde la intervención criminológica es reforzar los aspectos técnicos y las pericias científicas requeridas con el propósito de proyectar las necesidades de software, hardware y talento humano (profesionales en la materia) indispensables para alcanzar una verdadera independencia y soberanía tecnológica en Venezuela, para lo cual se proponen la ejecución de las siguientes acciones:

1.- Realizar un censo de software y hardware privativo, libre y abierto usado en el país en infraestructuras críticas e instituciones estratégicas, con el fin de contextualizar las fortalezas y amenazas para establecer una planificación en corto, mediano y largo plazo para la migración completa a las tecnologías libres.

2.- Crear y fortalecer centros de investigación y educativos en la materia, con el objeto de mejorar las capacidades nacionales en ciencia, tecnología e innovación, referidas a la formación de talento (especialmente en estándares criptográficos), la creación y fortalecimiento de infraestructura científica y el conjunto de plataformas tecnológicas requeridas en el país, así como la formación de todos los ciudadanos en esta temática.

3.- Desarrollar y reforzar el andamiaje de herramientas tecnológicas autóctonas, tanto de equipos como de servicios que tengan sus servidores en el país, –todas elaboradas en tecnologías libres- las cuales deben ser estables, seguras y confiables para entes públicos, privados y personas naturales, entre las que se pueden destacar: computador, smartphone, tablet, correo electrónico, mensajería instantánea, redes sociales y almacenamiento tipo nube, entre otros.

4.- Mejorar los niveles de seguridad y respuesta del poder público mediante la implementación obligatoria en todos los entes del Estado venezolano, así como en los representantes de los mismos y de la ciudadanía en general, el uso de la certificación electrónica, con el fin de proporcionar altos valores de confiabilidad y resultados eficaces y eficientes.

5.- Estructurar ejes de desarrollo de tecnologías libres (hardware y software) en conjunto con nuestros países vecinos y/o aliados a través de los organismos de integración existentes.

Propuestas en el marco social

Para hacer más seguro el uso de las TIC para el Estado venezolano y todos sus ciudadanos, la proposición surgida desde la intervención crimi-

nológica es ejecutar a manera de control social preventivo un conjunto de pautas protocolares al alcance de cualquier persona, las cuales deben ser socializadas por el Estado mediante la difusión, publicidad y educación de la ciudadanía, que permitan acciones a nivel personal para proteger la privacidad, el anonimato y la identidad digital individual y colectiva de todos los venezolanos, para lo cual se proponen la ejecución de las siguientes acciones:

1.- Concientizar a la ciudadanía en general sobre la importancia del uso de las tecnologías libres (hardware y software) para protegerse en contra de los ciberataques y el espionaje de las telecomunicaciones al utilizar las TIC.

2.- Apropiar a cada habitante del país del conocimiento de los riesgos y peligros implícitos en el uso de las TIC según el dispositivo (computador, smartphone, tablet, ente otros) y las aplicaciones (correo electrónico, mensajería instantánea, redes sociales, almacenamiento tipo nube, entre otros) que se utilicen, así como la conveniencia de producir y utilizar herramientas tecnológicas autóctonas.

3.- Internalizar en todos los venezolanos las nociones básicas fundamentales de la independencia y la soberanía científico-tecnológica según la realidad regional, tales como el anonimato, la privacidad, la identidad digital, la encriptación y la certificación de datos, entre otras, para que cada ciudadano cumpla su rol en función de una Política Criminal eficiente y eficaz.

4.- Promover las diversas herramientas basadas en tecnologías libres que permitan navegar de manera anónima por internet, no dejar ningún tipo de rastro sobre el usuario que está utilizando un computador, afianzar las comunicaciones seguras, asegurar el intercambio privado de correo electrónico a través del sistema de cifrado de llave pública, posibilitar el intercambio de mensajería instantánea de manera segura utilizando canales cifrados de la información, facilitar el almacenamiento de información de manera confiable en los computadores personales y utilizar sistemas operativos basados en software libre para evitar la inserción de software malicioso en los computadores personales.

5.- Promocionar la participación de toda la colectividad en la construcción de una Política Criminal eficiente y eficaz aportando su contribución los más diversos actores sociales que integran la nación en el resguardo de una verdadera independencia y soberanía científico-tecnológica.

Referencias

1) BID (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. Washington: Observatorio de la Ciberseguridad en América Latina y el Caribe.

2) Cohen, L y Felson, M. (1979).Social Change and Crime Rate, Trends. A Routine Activity Approach. American Sociológica Review, 44, 5 88, 608.

3) Felson, M., & Clarke, R. V. G. (1998). Opportunity makes the thief: Practical theory for crime prevention(Vol. 98). Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

4) Felson, Marcus en Miro, Fernando, (2012). Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons. Madrid-España.

5) García, Natalia (2016) Actividades cotidianas de los jóvenes en Internet y victimización por malware, IDP N.º 22 (Junio, 2016) Revista de los Estudios de Derecho y Ciencia Políticahttp://journals.uoc.edu/index.php/idp/article/viewFile/n22-garcia/n22-garcia-es 21/12/2016

6) Kaspersky (2016). Internautas en América Latina sufren 12 ataques de malware por segundo. Comunicado de prensa. Disponible en: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2016/internautas-en-america-latina-sufren-doce-ataques-de-malware-por-segunda-revela-kaspersky-lab.

7) Miro, Fernando, (2012). Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons. Madrid-España.

8) Miro, Fernando (2013)La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio;Revista Española de Investigación Criminológica Artículo 5, Número 11 (2013) www.criminologia.net. 01/12/2016.

9) OEA (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf.

10) Agustina, J. (2009) La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual. Universitat Internacional de Catalunya. Barcelona – España.

11) Birkbeck, C. y Lafree, G. (1989). Una revisión crítica de las teorías de las oportunidades para el delito. Revista Cenipec, 12. Universidad de Los Andes. Mérida -Venezuela.

12) Clarke, R. y Knake, R. (2011). Ensayos. En Clarke, R. & Knake, R. Guerra en la red: Los nuevos campos de batalla. Editorial Planeta. Barcelona – España.

13) Correa, C., Batto, H., Czar, S. & Nazar, F. (1987). Derecho informático. Cap. El derecho ante el desafío de la informática. Depalma. Buenos Aires – Argentina.

14) Cuervo, J. (2008). Delitos informáticos: Protección penal de la intimidad. Revista Informática Jurídica. Monterrey – México. Publicado en http://www.INFORMÁTICA-jurídica.com/trabajos/delitos.asp

15) Felson, M. (1997). Technology, Business and Crime. Felson, M., Clarke, R.V. (ed.), Business and Crime Prevention. Nueva York – EEUU.

16) García-Pablos de Molina, A. (2003) Tratado de Criminología. 3era Edición Editorial TiranLoBlanch. Valencia – España.

17) Garrido V., Stangelan P., y Redondo S. (2006). Principios de Criminología. 3era Edición. Editorial TiranLoBlanch. Valencia – España.

18) Miró, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons. Madrid – España.

19) Tellez, J. (2004). Derecho Informático. 3era. Edición. McGraw-Hill. Ciudad de México – México.

20) Danezis, G., y Clayton, R., (2007). Introducing traffic analysis (pp. 95-117). Auerbach Publications, Boca Raton, FL. Estados Unidos. p.1.

21) Leer, A., (Ed.). (2001). La visión de los líderes en la era digital. Pearson Educación. p.206.

22) Lévy, P., y Levis, D., (1999). ¿Qué es lo virtual?. Paidós. Barcelona. p.p. 10, 12.

23) Martínez, F., (2003). Premios nacionales de investigación e innovación educativa, Nº. 1 (Ejemplar dedicado a: Innovación educativa), 101-124. España. p.113.

24) Ordóñez, D., (2014). La protección judicial de los derechos en internet en la jurisprudencia europea. Editorial Reus. España. p.21.

25) Raymond, J., (2001). Traffic analysis: Protocols, attacks, design issues, and open problems. In Designing Privacy Enhancing Technologies (pp. 10-29). Springer Berlin Heidelberg. (January). p.2.

26) Tejerina, O., (2014). Seguridad del Estado y privacidad. Editorial Reus. p.10.

27) Wright, C., Coull, S., y Monrose, F., (2009). Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis. In NDSS. (February). p.1.W

MSc. Oscar González Díaz

CEO de PROTECSOFT C. A.

Magíster en Ciencias para el Desarrollo Estratégico, Especialista en Seguridad Informática, Criminólogo

FORTEX

PROTECCIÓN CORPORATIVA

"INTEGRIDAD QUE PROTEGE,
TECNOLOGÍA QUE RESPALDA"

Telf. (591-4) 4429949
Telf. (591-4) 4429950
61783554
61780817
comercial@fortex.com.bo

Visita nuestra pagina web

www.fortex.com.bo

EN SEGURIDAD,
LA CONFIANZA LO ES TODO.

Por eso **su marca** también debe estar protegida.

Marketing Digital Especializado para empresas del sector Seguridad.

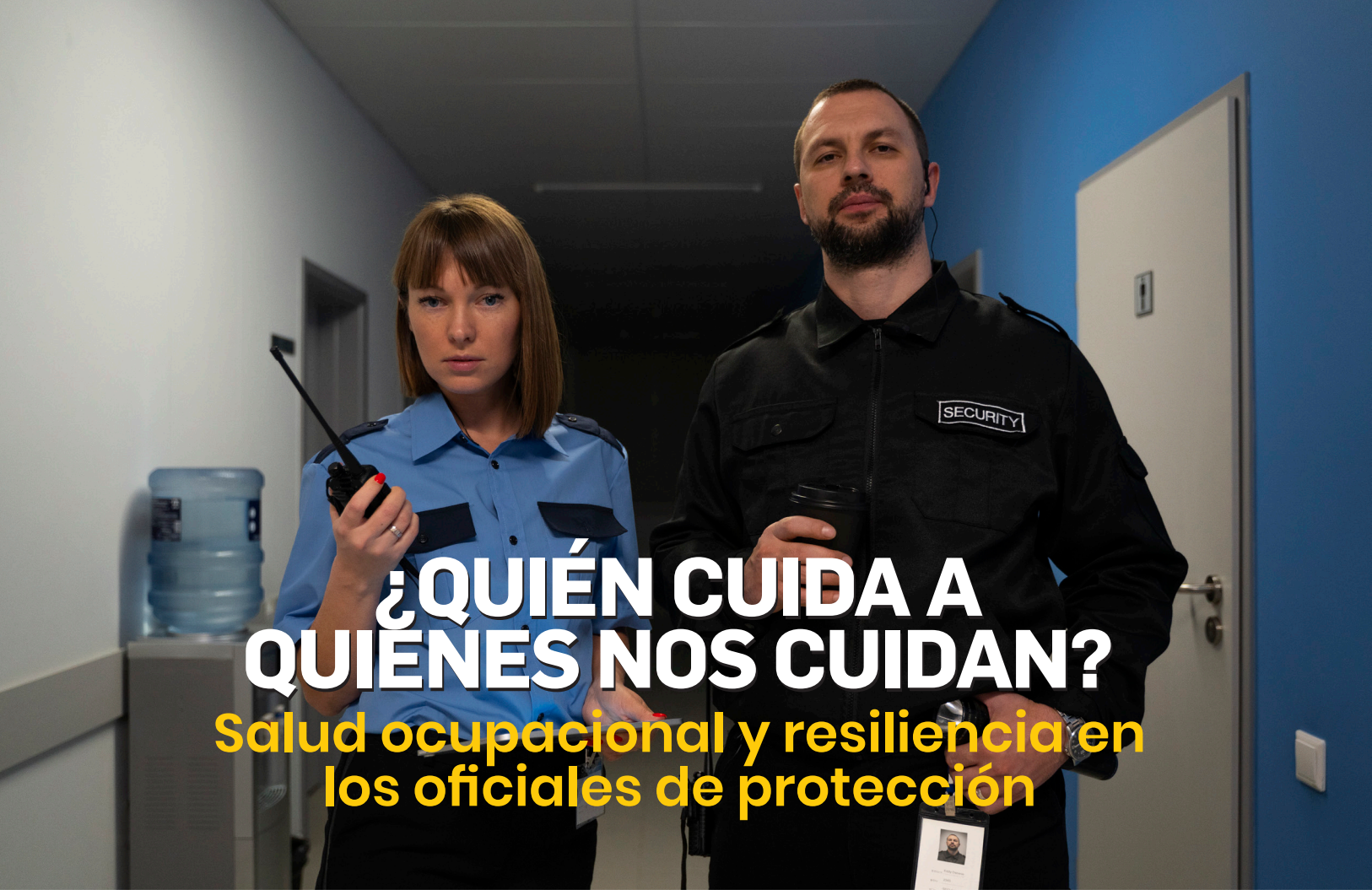
ideativa
MARKETING DIGITAL ESTRATÉGICO

¡CONTÁCTANOS!

info@ideativa.net

www.ideativa.net

+591 77070045



¿QUIÉN CUIDA A QUIÉNES NOS CUIDAN?

Salud ocupacional y resiliencia en los oficiales de protección

Cada noche, miles de oficiales de protección en Venezuela se enfrentan a largas jornadas de trabajo, a la incertidumbre de la violencia y al desgaste de un trabajo que exige estar siempre alerta. Son quienes protegen nuestras infraestructuras, empresas, industrias, escuelas, hospitales y comunidades. Sin embargo, pocas veces nos preguntamos: ¿quién cuida la salud de quienes nos cuidan?

En un contexto global donde la Organización Internacional del Trabajo (OIT) estima que cada año mueren 2,3 millones de personas por accidentes y enfermedades relacionadas con el trabajo, y ocurren más de 340 millones de accidentes laborales, la reflexión se vuelve urgente. El tema de la OIT para 2026 —***"Entornos de trabajo psicosociales saludables: un camino hacia trabajadores realizados y organizaciones fuertes"***— nos invita a mirar de frente la realidad de los oficiales de protección y a pensar en cómo proteger su salud ocupacional.

¿Qué está pasando?

Los oficiales de protección diariamente enfrentan una doble vulnerabilidad:

- **Riesgos físicos:** violencia, enfrentamientos, ergonomía deficiente, turnos prolongados y exposición a condiciones ambientales adversas.

- **Riesgos psicosociales:** estrés crónico, ansiedad, aislamiento, falta de reconocimiento y presión constante por mantener la protección y vigilancia de las áreas a cargo.

En Venezuela, la ausencia de estadísticas oficiales sistemáticas sobre accidentes laborales y salud ocupacional dificulta la prevención. Sin embargo, la evidencia internacional y los testimonios locales muestran que este sector es uno de los más expuestos a riesgos integrales.

Por lo general, los oficiales de protección que resguardan nuestras empresas y comercios provienen de compañías contratadas de seguridad privada. En muchos casos, las grandes organizaciones se preocupan por certificarse en sistemas de gestión ISO, como la ISO 45001, ISO 14001 o la ISO 9001, pero limitan su alcance al personal que tienen directamente dentro de su nómina. Esto genera una brecha: los oficiales de protección, que realizan un trabajo fundamental para la continuidad operativa y la protección de activos, quedan fuera de las políticas de salud ocupacional y bienestar, a pesar de que enfrentan riesgos tan relevantes como cualquier trabajador del área productiva. Reconocerlos como parte integral del sistema de gestión es un paso clave hacia la resiliencia organizacional.

Normas internacionales como guía

La gestión de la seguridad no puede limitarse a blindar infraestructuras. Debe incluir la salud integral de quienes garantizan esa protección. Por lo que aquí entran en juego dos normas clave:

- **ISO 45001:** que establece un marco para la gestión de la seguridad y salud en el trabajo, integrando prevención de accidentes, ergonomía y condiciones seguras en los turnos de trabajo.
- **ISO 45003:** que complementa este enfoque al abordar específicamente los riesgos psicosociales, como el estrés, la fatiga, la carga de trabajo excesiva y la falta de apoyo organizacional.

La gestión de la seguridad no puede limitarse a blindar infraestructuras. Debe incluir la salud integral de quienes garantizan esa protección.

Aplicadas en conjunto, estas normas permiten que la gestión de seguridad física no solo proteja activos e infraestructuras, sino también la salud ocupacional y el bienestar emocional de los oficiales de protección.

¿Qué significa esto para la sociedad venezolana?

Para la sociedad venezolana, este tema revela una verdad fundamental: la seguridad física no puede seguir viéndose como un ámbito aislado de la salud ocupacional. Ambos aspectos están íntimamente relacionados y deben abordarse de manera conjunta si queremos construir entornos laborales y comunitarios más seguros y humanos.

Para la sociedad venezolana, este tema revela una verdad fundamental: la seguridad física no puede seguir viéndose como un ámbito aislado de la salud ocupacional. Ambos aspectos están íntimamente relacionados y deben abordarse de manera conjunta si queremos construir entornos laborales y comunitarios más seguros y humanos.

En este sentido, los oficiales de protección representan un grupo particularmente vulnerable. Su labor es esencial para la continuidad de las empresas y la tranquilidad de las comunidades, pero muchas veces no cuentan con políticas públicas ni normas técnicas que reconozcan los riesgos específicos que enfrentan. Es necesario visibilizar que detrás de cada uniforme hay una persona que merece entornos laborales seguros, saludables y psicosocialmente sostenibles.

El impacto de aplicar marcos normativos como la ISO 45001 y la ISO 45003 en este sector sería profundo. Por un lado, contribuiría a reducir el miedo y la ansiedad que experimentan los trabajadores al desempeñar sus funciones en contextos de alta presión. Al mismo tiempo, permitiría fortalecer el tejido comunitario, ya que reconocer y valorar el rol de quienes protegen genera cohesión social y confianza.

Además, la implementación de estas normas se traduciría en un mayor bienestar laboral, lo que impacta directamente en la productividad y en la reducción de la rotación de personal. Finalmente, las organizaciones ganarían en resiliencia, al contar con equipos de seguridad más preparados, motivados y saludables, capaces de responder de manera efectiva a los desafíos del entorno.

¿Qué podemos hacer para proteger la salud ocupacional de los oficiales de protección?

Para avanzar hacia entornos laborales más seguros y saludables, es necesario que todos los actores asuman un compromiso compartido. Los ciudadanos deben reconocer y respetar el rol de los oficiales de protección, promoviendo la colaboración y la empatía hacia quienes garantizan la seguridad cotidiana. Las empresas, por su parte, tienen la responsabilidad de implementar medidas concretas como rotación de turnos con tiempos adecuados de descanso y pausas, ergonomía en los puestos de vigilancia y programas de vigilancia a la salud y atención preventiva, que atiendan tanto los riesgos físicos como los psicosociales. Las autoridades deben incluir a los oficiales de protección en campañas de prevención y en programas de salud ocupacional, alineando sus acciones con los marcos regulatorios de la OIT, las regulaciones nacionales que nacen de la LOPCYMAT, así como los marcos normativos internacionales de la ISO 45001 y la ISO 45003. Finalmente, la academia y los gremios profesionales tienen un papel clave en la investigación y divulgación de los riesgos psicosociales que enfrenta este sector, generando evidencia que sirva de base para políticas públicas más inclusivas y efectivas.

La seguridad no es completa si quienes la garantizan trabajan enfermos, agotados o invisibles. Protegerlos es también protegernos a todos. En el Día Mundial de la Seguridad y Salud en el Trabajo 2026, recordemos que un entorno psicosocial saludable no es un lujo, es un derecho. Y que cuidar la salud ocupacional de los oficiales de protección es el primer paso hacia comunidades más seguras y resilientes.

Saimerej Rondón Mendoza

La seguridad no es completa si quienes la garantizan trabajan enfermos, agotados o invisibles. Protegerlos es también protegernos a todos.

Seguridad estratégica en entornos de alta incertidumbre:

El modelo BOSS que convierte la vigilancia en continuidad operativa

En esta entrevista, BOSS Seguridad Integral explica cómo la seguridad privada puede pasar de ser un simple servicio de vigilancia a un socio estratégico que combina talento humano, tecnología y análisis del entorno para garantizar la continuidad operativa de las empresas en Venezuela.

Seguridad en Acción Venezuela (SV): "En un mercado como el venezolano, donde han proliferado tantas opciones de seguridad, muchos clientes caen en el error de contratar por 'precio' y no por 'valor'. En BOSS Seguridad Integral, ¿cómo han logrado redefinir el concepto de vigilancia privada para pasar de ser un simple gasto operativo a convertirse en un socio estratégico que garantiza la continuidad de negocio de sus clientes?"

BOSS: Nuestra empresa, a lo largo de estos 6 años que tenemos operando desde su fundación, nos hemos enfocado en dar valor al recurso humano, desde la preparación y entrenamiento del oficial, hasta la respuesta oportuna al cliente por cualquier circunstancia que se le presente, no tenemos intermediarios, la junta directiva y sus socios comerciales, mantienen constante comunicación con sus clientes a diario, este trato preferencial es lo que nos diferencia del resto de las empresas.

2. (SV): "Estamos en marzo de 2026 y ya no podemos separar lo físico de lo digital. Tras los eventos que vimos al inicio de año, donde la conectividad fue crítica, ¿cómo integra BOSS Seguridad la vigilancia física tradicional con herramientas tecnológicas de última generación? ¿Qué hace que un oficial de BOSS sea diferente a un guardia convencional frente a las amenazas híbridas actuales?"

BOSS: Aunque la tecnología es el musculo, la resiliencia que aprendimos a inicios de año, nos dice que el factor humano sigue siendo el cerebro, la tecnología no reemplaza al guardia, le da "superpoderes" de percepción, En Venezuela, donde la realidad social y económica a menudo supera la ficción, la seguridad no es un commodity, es una garantía de continuidad operativa, es por eso que nuestros departamento de operaciones en conjunto con los supervisores y oficiales de seguridad, conocen el compromiso que se tiene para con nuestros clientes. El servicio es primero.

3. (SV): "La seguridad es, ante todo, un negocio de confianza. En un entorno laboral tan retador como el de Venezuela, ¿cuáles son los pilares de BOSS Seguridad para la selección y formación de su personal? ¿Cómo garantizan que ese oficial que custodia una industria o a un ejecutivo tenga no solo la capacidad técnica, sino el compromiso ético que la marca promete?"

BOSS: En Venezuela, la seguridad de la empresa comienza por la seguridad del empleado, un Oficial con hambre o desmotivado es un riesgo de seguridad, la lealtad se cultiva con salarios competitivos y beneficios que alivien la carga logística (transporte, alimentación, Bonos de asistencias) la confianza se construye con la consistencia de un personal que se siente valorado y motivado y que este entienda que su rol es proteger la tranquilidad de otros para que el país siga moviéndose, por esta razón, nuestros pilares fundamentales para hacer de que nuestra empresa sea pionera en seguridad, es la confianza, valor y motivación.

4. (SV): "Venezuela presenta dinámicas de riesgo muy particulares que cambian de una semana a otra. BOSS Seguridad integral es referente en protección ejecutiva y seguridad industrial; desde su sala de control, ¿cómo analizan el entorno venezolano actual para anticiparse a los riesgos antes de que ocurran? ¿Cuál es ese 'plus' preventivo que el cliente solo encuentra con ustedes?"

BOSS: En nuestro pais, la seguridad no se puede gestionar con manuales estáticos; aquí la realidad tiene una "tasa de refresco" extremadamente rápida, para anticiparnos, no solo monitoreamos las cámaras, analizamos contexto, señales débiles y flujo de información. No esperamos a que ocurra un evento; monitoreamos la atmosfera social y digital que lo precede, lo que el cliente encuentra con nosotros es el protocolo de autonomía de continuidad, mientras otros esperan instrucciones durante una crisis, nosotros ya hemos ejecutado la Pre-decisión.

5. (SV): "Si un empresario venezolano está leyendo esto y se pregunta si su inversión está realmente protegida para lo que resta de 2026, ¿cuál es la promesa de valor que BOSS Seguridad Integral le hace hoy? ¿Hacia dónde se dirige la empresa para seguir siendo el estándar de oro en seguridad privada en los próximos años?"

BOSS: Para un empresario en la Venezuela actual, la seguridad ha dejado de ser un "gasto de vigilancia" para convertirse en un seguro de continuidad operativa, el clima actual, la seguridad es una ventaja competitiva, un negocio seguro es un negocio que puede seguir funcionando y operando, a pesar de los entornos sociales y económicos que puedan atravesarse, nuestro estándar de oro hoy, es una empresa sólida que se comporta más como una firma de consultoría tecnológica y de riesgos que como una agencia de vigilancia tradicional.

Adolfo M. Gelder
Editor Revista Seguridad en Acción
Venezuela en representación de Seguridad
en Acción LATAM

LA NUEVA ERA DE LA SEGURIDAD CORPORATIVA:

DE LA VIGILANCIA REACTIVA A LA RESILIENCIA EMPRESARIAL

En el complejo entorno actual, caracterizado por la volatilidad y la incertidumbre, las grandes corporaciones y los ejecutivos de alto perfil se enfrentan a amenazas cada vez más sofisticadas. En este escenario, el modelo tradicional de seguridad basado únicamente en la presencia física ha quedado obsoleto.

Hoy, la seguridad no debe verse como un gasto operativo o una función reactiva, sino como una inversión estratégica fundamental para garantizar la continuidad del negocio y salvaguardar la reputación. Es aquí donde entra en juego el concepto de resiliencia corporativa: la capacidad de una organización para absorber, adaptarse y prosperar frente a eventos disruptivos en un entorno cambiante.

Para lograr esta resiliencia, la seguridad corporativa debe elevarse al nivel de la alta gerencia, integrándose plenamente en la toma de decisiones estratégicas. Esto se logra a través de la filosofía ESRM (Enterprise Security Risk Management). El ESRM es un enfoque holístico que vincula las prácticas de seguridad directamente con la misión y los objetivos globales de la empresa, impulsando a todas las áreas del negocio a reconocer y tratar proactivamente los riesgos. Bajo el paraguas del ESRM, los líderes empresariales y los profesionales de la seguridad se

convierten en socios estratégicos, asegurando que la protección de activos tangibles e intangibles esté alineada con el gobierno corporativo.

Para que la alta dirección tome decisiones informadas, estas deben estar sustentadas en metodologías científicas y estandarizadas. En primer lugar, la norma ISO 31000 proporciona los principios y directrices universales para la gestión del riesgo, estableciendo un marco que permite identificar, analizar y tratar la incertidumbre de manera estructurada y auditable.

Complementando este marco normativo de alto nivel, utilizamos herramientas de cálculo preciso como el Método Mosler. Este método secuencial nos permite realizar un análisis y evaluación de riesgos exhaustivo (identificando criterios de función, sustitución, profundidad, extensión, agresión y vulnerabilidad) para cuantificar la clase y dimensión del riesgo real al que se expone una instalación o un alto ejecutivo. Lo que no se puede medir, no se puede gestionar; y mediante el método Mosler, transformamos percepciones subjetivas de inseguridad en datos matemáticos precisos que justifican el costo-beneficio de cada contramedida.

El Compromiso de FORTEX

En FORTEX, comprendemos profundamente esta evolución. Nuestra filosofía institucional es clara: no vendemos guardias; ofrecemos inteligencia de seguridad y resiliencia corporativa. Nos alejamos radicalmente del modelo tradicional para convertirnos en su socio estratégico en la gestión integral de riesgos.

A través de nuestra división de consultoría, diseñamos soluciones a la medida para clientes corporativos, industrias críticas y ejecutivos de alta talla (VIPs). Integramos el profesionalismo de un personal de élite rigurosamente seleccionado con el poder del análisis de datos y tecnología de vanguardia, creando anillos de protección 360°.

Nuestro objetivo es dotar a la alta gerencia de la información crítica necesaria para operar con tranquilidad en entornos desafiantes. Con FORTEX, su organización podrá dar el paso definitivo: pasar de la incertidumbre de la seguridad reactiva a la certeza absoluta de la resiliencia gestionada.

Protegemos su patrimonio.
Aseguramos su continuidad.
Fortalecemos su liderazgo.

Lic. Gabriel Burgoa,
Director Ejecutivo de FORTEX
(a BBGROUP Company)

FRACTAL

PROTEGE TU NEGOCIO ANTES DEL PRÓXIMO ATAQUE

Soluciones integrales de Ciberseguridad, Telecomunicaciones e Infraestructura para garantizar la continuidad operativa de tu empresa.

En Fractal Solutions

Protegemos los activos digitales críticos de tu organización mediante servicios especializados en:

- **Prevención**
- **Detección**
- **Respuesta a incidentes**
- **Cumplimiento normativo**

Somos tu socio estratégico

En *ciberseguridad empresarial*.

- **Soluciones 360°**
- **Monitoreo continuo 24/7**
- **Protección de la continuidad del negocio**

Seguridad & SOC

Monitoreo y respuestas a incidentes 24/7

Auditoría ISO y Cumplimiento

ISO 27001-ISO 22301
Evaluación de Madurez

Pentesting

Simulación de ataques reales en redes y aplicaciones

Infraestructura & Telecom

Redes seguras y alta disponibilidad

Protege tus datos. Protege tu futuro

Diseñamos estrategias de seguridad adaptadas a tu organización

info@securityfractal.com
www.securityfractal.com
@securityfractal

Aprendizaje SIN LÍMITE

*Con **Aprendo Ya** encuentra la forma más fácil de vender profesionalizar tus cursos.*

APRENDOYA

APRENDIZAJE SIN LÍMITES Y FRONTERAS

Recibe pagos locales en bolivianos y ofrece tus cursos en un aula profesional

¡Es hora de crecer!

*Ahora puedes destacar y vender más porque tus cursos pueden estar en el centro de atención con **Aprendo Ya***

El momento de actuar es

AHORA

Haz que tu conocimiento brille y tus ventas despeguen.

Correo: info@aprendoyaa.com
Página web: www.aprendoyaa.com

CORPROJO

SERVICIOS INTEGRALES

PREPARACIÓN INTEGRAL EN SEGURIDAD PARA UN FUTURO MÁS PROTEGIDO

CON FORMACIÓN PRÁCTICA Y ESTRATEGIAS EFECTIVAS

www.corporacionrojo.com