VENEZUELA, JUNIO DE 2026 - AÑO 1 - NÚMERO 3

SEGURIDAD en acción VENEZUELA

LA CACERÍA INVISIBLE EN LAS PANTALLAS ELECTRÓNICAS

EDITORIAL

Llegamos a nuestra tercera edición en un mes que, para el venezolano, respira historia, compromiso y futuro. Junio no es solo una página más en el calendario de Seguridad en Acción; es el mes donde la estrategia, el valor y la protección convergen para recordarnos de dónde venimos y hacia dónde debemos dirigir nuestra mirada profesional.

Hace 205 años, en las sabanas de Carabobo, se libró una batalla que no solo se ganó con fuerza, sino con una planificación táctica impecable y una visión de unidad. Hoy, en pleno 2026, los profesionales de la seguridad en Venezuela libramos nuestra propia "Batalla de Carabobo" en frentes mucho más complejos y diversificados.

La soberanía de nuestras organizaciones ya no depende solo de un perímetro físico. Se construye en la Seguridad Industrial y Laboral, garantizando que el motor humano de nuestras empresas opere bajo estándares de máxima protección; se defiende en las trincheras de la Seguridad Informática y de la Información, donde la "Inmunidad Digital" es nuestra mejor artillería contra las amenazas invisibles del ciberespacio; y se consolida en la Seguridad Física, que ha evolucionado de la vigilancia tradicional hacia una gestión de riesgos inteligente y certificada.

En este mes también celebramos el Día del Padre, una figura que representa la esencia misma de nuestra profesión: el resguardo y la guía. Así como un padre anticipa los peligros para proteger su hogar, el líder de seguridad moderno debe ser el custodio de la continuidad de su organización, combinando la firmeza de la autoridad con la sabiduría de la prevención.

Pero nuestra visión no se detiene en nuestras fronteras. Con un profundo orgullo, inauguramos en esta edición nuestra sección de gala: "Frontera Cero: Nuestra huella en el resguardo internacional". En este espacio, rendimos tributo a los profesionales venezolanos que, repartidos por el mundo, llevan nuestra bandera en alto en las latitudes más exigentes. Su éxito en el exterior es el testimonio de que la resiliencia y el talento venezolano son hoy un estándar de exportación en la seguridad global.

Juntos, trazamos el mapa de una seguridad que ya no solo reacciona, sino que diseña el futuro. Bienvenidos a la tercera edición de Seguridad en Acción. Porque la seguridad, como la patria, se construye cada día con inteligencia, integridad y visión de futuro.

Adolfo M. Gelder

Escanea el QR y únete a nuestra comunidad de más de 3 mil miembros en LATAM.

Staff

HUMBERTO COPA G.
DIRECTOR GENERAL

LUCIEL RÍOS 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

NUESTRA HUELLA EN EL RESGUARDO INTERNACIONAL

ALBERTO RAY
EXPERTO EN GESTIÓN DE RIESGOS Y ESTRATEGIA

En un entorno global saturado de incertidumbre, las viejas murallas de la protección física ya no son suficientes para garantizar la continuidad operativa. Para inaugurar nuestra nueva sección Frontera Cero, conversamos en exclusiva con Alberto Ray, renombrado consultor internacional y estratega de seguridad. Con la agudeza analítica que lo caracteriza, Alberto Ray desmantela los mitos de la protección absoluta y nos introduce en el nuevo y crucial campo de batalla: la seguridad cognitiva. Una cátedra imperdible sobre cómo transformar al individuo de un eslabón frágil a la barrera defensiva más sólida de la organización a través del modelo MAPS.

La seguridad y el talento venezolano no conocen límites geográficos. En esta sección cruzamos fronteras para seguir el rastro de profesionales que, formados en nuestra tierra, lideran hoy estrategias de protección, investigación y resiliencia global. Frontera Cero es un reconocimiento a la excelencia y un testimonio imborrable en el resguardo internacional.

Nuestro primer invitado es Alberto Ray, un peso pesado en el mundo de la gestión de riesgos y la estrategia. Es uno de esos profesionales venezolanos que ha logrado elevar el debate de la seguridad desde lo meramente operativo hacia lo estratégico y sistémico. Sus libros y sus constantes artículos lo posicionan no solo como un consultor, sino como un filósofo de la seguridad. Tiene esa capacidad de explicar problemas complejos de forma sencilla, pero con una profundidad técnica impecable.

P: Alberto, el sistema MAPS estructura el análisis en entornos complejos. Desde tu perspectiva en EE. UU., donde imperan la predictibilidad y el Compliance, ¿cómo se adapta tu metodología al entorno caótico venezolano de 2026? ¿Es posible medir el riesgo cuando las variables cambian más rápido que la respuesta del sistema?

R: El sistema MAPS, como todo modelo de medición de riesgos, es una fotografía del momento. Sin embargo, la alta incertidumbre actual nos obliga a que los modelos sean dinámicos. No basta con una imagen estática; necesitamos una secuencia de "instantáneas" para observar patrones y desarrollar capacidad predictiva en entornos donde la impredecibilidad es la constante.
A mayor incertidumbre, mayor debe ser la frecuencia de análisis. Si rigidizamos los modelos, perdemos tiempo vital en la ejecución; prefiero un análisis riguroso pero ágil. Lo que realmente importa hoy no es el análisis puntual y aislado, sino la sucesión de mediciones a lo largo del tiempo.
Anteriormente, las organizaciones actualizaban su análisis de riesgo cada seis meses; hoy eso es un siglo. Considero imperativo realizar una medición al menos cada dos meses.
Al tener tres análisis en un semestre, dejas de ver datos aislados y observas la curva de evolución: cómo cambian las amenazas y cómo se desplaza nuestra capacidad de respuesta. El modelo MAPS facilita esta agilidad por su naturaleza cualitativa, evitando que quedemos ciegos ante un mundo que cambia a velocidad vertiginosa.

P: Recientemente vivimos en Venezuela eventos que demostraron que la seguridad física es ciega sin la ciberseguridad. Si la seguridad es un sistema interconectado, tras los incidentes de enero, ¿crees que los directivos en Latinoamérica subestiman la fragilidad sistémica, protegiendo la puerta física mientras dejan abierta la ventana digital de la infraestructura crítica?

R: Persiste una brecha significativa entre la seguridad física y la digital, fenómeno global que se manifiesta con mayor crudeza en Latinoamérica. El núcleo del problema radica en la falta de comprensión profunda por parte de la alta gerencia. Muchas organizaciones operan bajo estructuras divididas, donde la seguridad física y la ciberseguridad corren por carriles separados.
Sin embargo, la evolución profesional se encamina hacia la gestión integral del riesgo, no hacia la "seguridad" aislada. Quien entiende el riesgo comprende que la seguridad es un dominio técnico interconectado donde lo físico y lo digital son ya indivisibles.
Respecto a Venezuela, prefiero verlo como una ventana de oportunidad excepcional. Tras años encapsulado y separado de la evolución global, los incidentes de principios de este año deben actuar como un catalizador para ponernos al día. No se trata solo de recuperar el tiempo perdido, sino de ejecutar un "salto de rana" tecnológico y mental: pasar del rezago directamente a la vanguardia, tal como ocurre cuando una sociedad salta de redes 3G a 5G. El reto es triple: actualización tecnológica profunda, renovación de la capacidad gerencial y, sobre todo, un cambio de paradigma. Lo ocurrido en enero fue el punto de partida que nos obligó a abrir la puerta de la actualización para transformar nuestra visión en una disciplina moderna, integrada y resiliente.

P: Planteas que la seguridad está en crisis. Con la llegada de la IA generativa y los deepfakes afectando decisiones ejecutivas, ¿debería el Director de Seguridad dejar de obsesionarse con los perímetros físicos y ocuparse de la Seguridad Cognitiva? ¿Cómo protege el sistema MAPS la integridad de la verdad organizacional?

R: Históricamente, hemos cometido el error de ver al individuo únicamente como el eslabón más débil, alguien a quien rodear de muros pasivamente. Propongo un cambio de paradigma: el ser humano debe dejar de ser un sujeto pasivo para convertirse en el generador y productor de su propia seguridad. Si insertamos cognitivamente en la conducta del individuo los elementos de gestión de riesgo, transformamos esa fragilidad en la fortaleza más sólida de la organización.

Hoy, la IA es un arma de doble filo. Más allá de modificar narrativas, se utiliza para afectar directamente la mente y la conducta de la gente. Es en la mente donde se ganan o pierden las batallas; allí reside la capacidad para afrontar el peligro. Por eso, las grandes amenazas actuales son cognitivas: buscan minar tu sentido de valor o hacerte sentir que la amenaza es tan grande que es inútil combatirla. Es el arma de quinta generación diseñada para que pierdas la batalla antes de empezar a pelearla.

La Seguridad Cognitiva es nuestra última barrera.

En cuanto al sistema MAPS, su metodología es lo suficientemente flexible para integrarla. Es un área que planeo desarrollar a futuro: definir qué indagaciones hacer para detectar si el capital humano está siendo atacado en su dimensión psicológica. La resiliencia organizacional depende hoy de que recuperemos el control sobre lo que pensamos y cómo reaccionamos ante la desinformación y el miedo.

P: Eres un referente de la diáspora intelectual en seguridad. En un mercado tan competitivo como el estadounidense, ¿cuál ha sido esa ventaja competitiva que traías de Venezuela para posicionarte como consultor de alto nivel? ¿Es la gestión de la incertidumbre nuestro mayor activo de exportación?

R: Suelo decir que los profesionales venezolanos venimos del futuro. Hemos aprendido a gestionar la complejidad de una manera que pocos especialistas globales han experimentado. Los retos enfrentados en Venezuela no se enseñan en universidades; son una escuela de fuego que desarrolla una capacidad de análisis y de prospectiva excepcional.

En mi práctica como consultor internacional, mi mayor activo es predecir lo que viene. Venezuela se convirtió en la vanguardia de los problemas; nos enfrentamos a entornos tan saturados de incertidumbre que nos vimos obligados a ser extremadamente resilientes. Hace una década, cuando nadie hablaba de esto, en los congresos de ASIS en Venezuela ya poníamos la resiliencia en el centro del debate. Esa capacidad de resistir y adaptarse es nuestra ventaja competitiva exterior.

Sin embargo, la resiliencia no debe ser una excusa para abandonar la planificación. Las organizaciones crecen donde hay certezas. Si bien el mundo es incierto, el rol de la seguridad en la reconstrucción de Venezuela debe ser convertir lo impredecible en predecible. Necesitamos que las instituciones vuelvan a ser transparentes, que hablemos con la verdad y reconozcamos nuestras vulnerabilidades para abordarlas con seriedad. Tenemos una ventaja extraordinaria, pero el reto es usar esa experiencia para construir entornos de estabilidad y confianza.

P: Muchos clientes todavía compran seguridad buscando "riesgo cero". Como autor y estratega, ¿cuál es la verdad incómoda que nadie se atreve a decirles a los dueños de negocios en 2026? Si la protección absoluta es un mito, ¿la inversión debe ir a murallas más altas o a una ingeniería de resiliencia para fallar de forma segura?

R: El mito de la muralla siempre será necesario, pero hoy es totalmente insuficiente. La posición más honesta y profesional frente a un cliente es hacerle entender que el riesgo es una constante con la que debemos convivir. No podemos eliminarlo; el riesgo cero no existe mientras exista la incertidumbre. El objetivo primordial de la seguridad moderna es generar una conciencia profunda de los riesgos para abordarlos con naturalidad e integridad.

Incluso en las organizaciones que más invierten en prevención, la posibilidad de que un riesgo se materialice siempre está latente. El mejor ejemplo es la industria aeronáutica civil: es el sistema más seguro del mundo, pero ante una tragedia la respuesta es radical. Lo vimos con los incidentes del Boeing 737 MAX; tras dos accidentes, la industria detuvo toda la flota para analizar la causa raíz. No se permitieron seguir corriendo el riesgo sin entender la falla. Fue costoso, pero la confianza en el sistema vale mucho más.

La clave de la resiliencia no es solo evitar el impacto, sino estar preparados para responder eficientemente y extraer lecciones. Si un riesgo se materializa y no aprendes de él, la pérdida es doble. Al final del día, la lección más barata es la que aprendemos de lo que les sucede a otros. Capitalizar las experiencias ajenas para fortalecer nuestras propias defensas es la forma más inteligente de gestionar la seguridad en un mundo que nunca deja de ponernos a prueba.

Adolfo M. Gelder - Editor

LA SEGURIDAD FÍSICA DEL PERSONAL DE RECURSOS HUMANOS

QUÉ TAN A MENUDO SE PASA POR ALTO

La labor que se realiza en el departamento de Recursos Humanos es a menudo percibida como segura y libre de riesgos, lo cual no podría estar más equivocado, ya que tratamos con la parte más compleja de una organización: el ser humano. El personal de RRHH se encuentra en primera línea en situaciones de alta tensión emocional y confrontación.

El nivel de compromiso de su seguridad física varía dependiendo del cargo que ocupe, y dependerá de las responsabilidades asignadas, pero mucho más alto de lo que las empresas quieren reconocer.

Dentro de este maravilloso departamento existen cargos que son los que requieren mayor atención como son el reclutador que pertenece a la Unidad de ingreso y selección, su riesgo es mayormente externo, el peligro está en que se expone a personas externas a la empresa, para poder encontrar a la persona indicada para un puesto se puede llegar a entrevistar o contactar a más de 20 personas y eso representa diferentes tipos de situaciones con las cuales nos podemos encontrar indistintamente del cargo que se esté ofertando, en este caso se sugieren las siguientes recomendaciones: no citar a los candidatos fuera de horas de oficina o en sitios fuera de las instalaciones de la empresa, no utilizar tu teléfono personal para realizarles llamadas o citarlos con tu dirección de email ya que estarías revelando tus datos personales a una consi-

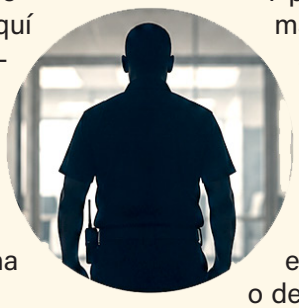
derable cantidad de personas desconocidas, lo cual a largo plazo traería serias consecuencias, en el momento de explicar las especificaciones del cargo es decir remuneración, beneficios, horarios ser lo más sincero y claro posible para evitar conflictos al momento de la contratación, porque esas personas formarán parte de la organización es decir tus futuros compañeros del día a día.

En Venezuela existen diversas formas de publicar vacantes laborales. Los portales web de empleo son una de las formas más segurasde publicar ya que nos permite un contacto netamente corporativo con los candidatos, pero algunas empresas no poseen los recursos monetarios para cancelar dichos servicios o simplemente no quieren asumir el gasto, en ese caso nos toca al grupo de reclutamiento buscar otras alternativas, si poseemos teléfono corporativo sería lo mejor, pero en el caso de que tengas que usar tu teléfono personal es recomendable integrarse en los grupos o canales de búsqueda de empleo en donde se puede publicar las vacantes y existe una opción en tu perfil de ocultar tu número telefónico y tu foto de perfil a personas que no sean tus contactos para evitar fuga de tu información personal.

RIESGO "efecto olla de presión"

¿Cuál es el cliente de recursos humanos?

Nuestro cliente es el interno, es decir, todo el personal que labora en la empresa, debemos atenderlo de una manera cordial, amable y oportuna y sobre todo con empatía, para eso siempre nos encontramos con un asistente o secretaria que recogerá los reclamos o dudas que puedan surgir, estará expuesto a explosiones emocionales en caliente. El riesgo aquí es el "efecto olla de presión", un trabajador que se encuentra frustrado puede estallar en una discusión administrativa o un altercado físico, si no siente que está bien atendido, que sus derechos no están siendo respetados o no le están dando una respuesta efectiva.



¿Qué se recomienda?

Atender al personal en las instalaciones administrativas de Recursos Humanos, brindándole una buena atención y tomando sus datos como número de teléfono o email para darle una respuesta oportuna y en caso de que se pueda resolver de manera inmediata pasarlo al analista encargado.

Y por último, dejé para el final uno de los cargos más importantes y a la vez más peligrosos en el área, la persona que se encarga de notificar los despidos, gestionar la liquidación, en muchas ocasiones no son la misma persona pueden ser personas diferentes, pero de igual manera se enfrenta a un detonante muy fuerte la pérdida de empleo y la disputa por dinero, son eventos que pueden disparar reacciones de ira o de tristeza en la mayoría de las personas y ade-

más de saber manejarlas es necesario tomar medidas para nuestra seguridad se recomienda estar acompañado por personal de seguridad de la empresa o el supervisor directo, que sea en un ambiente administrativo, no ser ofensivo ni agresivo, mostrarse totalmente comprensivo y empático a la situación del trabajador, tener a la mano la documentación necesaria para minimizar el tiempo de la reunión, todo lo que he mencionado es el deber ser pero la realidad es muy diferente, las empresas toman decisiones sobre su personal ignorando las recomendaciones dadas por el equipo de recursos humanos o muchas veces toman la decisión pero dejándonos a nosotros la tarea de ejecutarlas y allí es cuando debemos hacer lo mejor posible aunque existen circunstancias que no podamos controlar, en Venezuela la ley del trabajo permite la contratación por tiempo determinado, y muchas empresas utilizan este recurso para en caso de que no funcione la relación laboral terminar el contrato en la fecha de su finalización o para que su personal no genere mayor antigüedad en la empresa, esa rotación de personal hace que el departamento de recursos humanos se enfrente a esa situación más veces de las que quisiéramos, en ese caso debemos hacer la diferencia e implementar los cambios requeridos para que ese proceso no sea traumático y no genere faltas de respeto lo cual no puede ser permitido hacia el personal de recursos humanos, recordemos que no podemos cambiar las decisiones directivas, pero sí cómo aplicarlas.

EL RIESGO FÍSICO EN RR.HH. ES REAL Y DEBE SER TRATADO COMO UN ASPECTO CRÍTICO DE LA SEGURIDAD CORPORATIVA, NO SOLO COMO UNA MOLESTIA ADMINISTRATIVA

DESIREE DA SILVA

TSU EN ADMINISTRACIÓN TÉCNICO CONTABLE

Venezolana, emprendedora y madre de familia. Especialista en legislación laboral, cuenta con más de dos décadas de experiencia laboral en el área de recursos humanos privada y pública. Actualmente se encuentra estudiando en la UNEXCA

LA CIENCIA DE LA PROTECCIÓN APLICADA POR EL LÍDER DE LA INDUSTRIA EN VENEZUELA

Carlos Luis Blanco Donaire

Presidente OESVICA

Hablar de protección patrimonial e industrial en Venezuela es hablar de experiencia y evolución. Carlos Blanco nos muestra cómo Oesvica ha integrado disciplina táctica, tecnología y gestión moderna para convertirse en un aliado estratégico de las empresas que demandan altos estándares de seguridad, control y resguardo de sus activos.

1. Carlos, en un mercado saturado de nuevas ofertas de seguridad que a veces priorizan el bajo costo sobre la estructura, Oesvica cumple más de 20 años en la cúspide. Para un CEO o un Director de Operaciones que hoy debe decidir su presupuesto de resguardo: ¿Por qué apostar por la robustez institucional de Oesvica es, en realidad, una inversión de ahorro a largo plazo frente a las opciones de 'seguridad low-cost' que abundan en el país?

Respuesta: En OESVICA, entendemos que la seguridad no es un gasto que se recorta, sino un activo que se protege. Con 20 años en el mercado venezolano, nuestra robustez no es solo estructural, es operativa. Apostar por nosotros es una inversión en ahorro porque minimizamos la siniestralidad mediante la gestión de riesgos basada en normas internacionales. Mientras las opciones low-cost ofrecen una presencia reactiva, nosotros ofrecemos una estructura certificada bajo ISO 9001 y BASC,

garantizando que cada proceso, desde el reclutamiento hasta la supervisión, cumpla con estándares de calidad que evitan pérdidas patrimoniales y legales catastróficas para nuestros clientes.

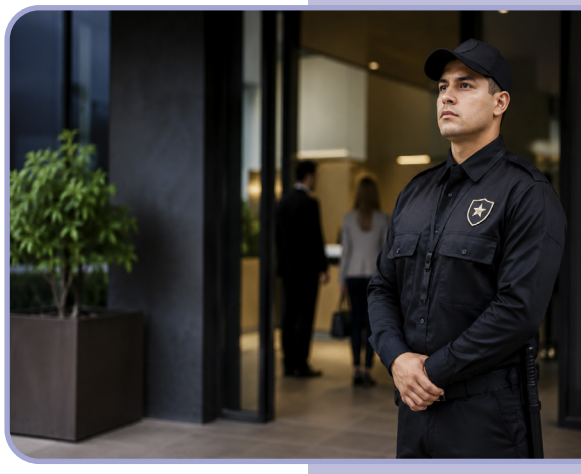
2. En el flyer de esta edición vemos que Oesvica no se queda solo en el oficial de seguridad. Ustedes hablan de una integración inteligente. ¿Cómo están utilizando la analítica de datos y la tecnología para potenciar el factor humano? ¿Cómo ha logrado Oesvica que sus oficiales dejen de ser 'vigilantes' para convertirse en analistas de riesgos en tiempo real en los puestos de servicio?

Respuesta: Hemos evolucionado la figura del oficial de seguridad. En OESVICA, no solo contamos con personal; contamos con una red de analistas de riesgos en terreno potenciados por tecnología de vanguardia. Utilizamos herramientas de Business Intelligence y analítica de datos para identificar patrones de vulnerabilidad antes de que se conviertan en incidentes. Esta integración inteligente nos permite optimizar el recurso humano: el oficial ya no es un observador pasivo, sino un nodo de información que alimenta un sistema de protección 360°, permitiendo decisiones gerenciales basadas en datos reales y en tiempo real.

3. Hoy en día, las empresas internacionales y las grandes industrias en Venezuela exigen estándares de cumplimiento rigurosos. ¿Qué garantías de tranquilidad legal y operativa ofrece Oesvica que otras empresas más pequeñas no pueden respaldar? ¿Cómo se traduce su estructura organizativa en continuidad de negocio para sus clientes ante situaciones de crisis extrema?

Respuesta: Nuestra experiencia multisectorial en hotelería, banca e industria tradicional nos ha permitido desarrollar protocolos de resiliencia únicos. Actualmente, estamos adaptando este know-how a las exigencias críticas de la industria petrolera y sus empresas de servicios, donde la continuidad operativa es vital. Ofrecemos la tranquilidad de una empresa que está en proceso de certificación ISO 18788 (Sistema de Gestión para Operaciones de Seguridad Privada), lo que asegura que nuestras operaciones respetan los derechos humanos y la legalidad internacional, blindando a nuestros clientes ante cualquier contingencia operativa o reputacional en momentos de crisis extrema.

4. Sabemos que el recurso más crítico en la seguridad es la confianza. En una era de alta rotación, ¿cuál es el secreto de Oesvica para el reclutamiento y la formación de sus filas? ¿Qué pasa 'detrás de escena' en sus procesos de selección para asegurar que el personal que llega a la puerta de un cliente es el más apto, confiable y capacitado del mercado?



Respuesta: El secreto de nuestra baja rotación y alta confiabilidad reside en la rigurosidad. Detrás de cada oficial en la puerta de un cliente, hay un proceso de selección que incluye estudios socioeconómicos profundos, pruebas psicométricas y validación de antecedentes, alineados con los estándares de la certificación BASC. No buscamos llenar vacantes; buscamos vocación de servicio. La formación continua en nuestra propia academia asegura que el personal no solo sea el más apto técnica y físicamente, sino que comparta los valores éticos que han sostenido a OESVICA durante dos décadas.

5. Oesvica ha sobrevivido a todos los cambios de paradigma en Venezuela. Si pudieras hablarle directamente a los más de 3.000 líderes de seguridad que leen esta revista: ¿Hacia dónde se dirige Oesvica en este segundo semestre de 2026 y por qué deberían verlos no solo como un proveedor de servicios, sino como el socio estratégico para su resiliencia operativa?

Respuesta: Para este segundo semestre de 2026, OESVICA se proyecta como el socio estratégico indispensable para la resiliencia operativa en Venezuela. Estamos enfocados en la expansión hacia sectores de alta complejidad técnica y en la culminación de estándares internacionales que nos pongan a la par de las mejores firmas globales. A los líderes de seguridad les digo: no busquen un proveedor que solo vigile sus activos; busquen un aliado que entienda su negocio, mitigue sus riesgos y asegure su rentabilidad. OESVICA es la ciencia de la protección aplicada a su favor.

Adolfo M. Gelder - Editor


TECNO SISTEMAS BFG, C.A.
BFG
Soluciones Integrales en Ciberseguridad, Continuidad de Negocio y Energía Segura
Continuidad de Negocio
Energía Segura
Ciberseguridad
PONTE EN CONTACTO CON NOSOTROS
J-41147373-1
+58 414 113.95.48
412 313.95.48
agonzalez@bfgtecno.com
ventas@bfgtecno.com
www.bfgtecno.com


PROTEX
SEGURIDAD 2013, C.A.
J-402916345
En Protex Seguridad, creamos el espacio para tu tranquilidad.
Cobertura Nacional
+ 500 Profesionales Capacitados
Escanea y Conócenos
SOMOS EL ESCUDO QUE TE PROTEGE
www.corporacionprotex.com.ve

ALBERTO ÁLVAREZ
CORPORATE RELATIONS MANAGER
ALAS ASOCIACIÓN LATINOAMERICANA
DE SEGURIDAD

EL MAPA DE LA **Seguridad Latinoamericana** PARA EL SEGUNDO SEMESTRE DEL AÑO

Alberto Álvarez, con más de 40 años de trayectoria en los sectores de seguridad electrónica, automatización de edificios y protección contra incendios, ha tenido el privilegio de evolucionar desde roles técnico-comerciales, hasta la dirección ejecutiva y el desarrollo de nuevos negocios a escala internacional. Lleva más de 25 años trabajando en asociaciones profesionales promoviendo la profesionalización, normativas y buenas prácticas.

1. “Alberto, ALAS ha logrado crear un lenguaje común para la seguridad en una región con realidades políticas y económicas totalmente dispares. En este año 2026, ¿cuál es el mayor desafío para unificar criterios técnicos en Latinoamérica cuando algunos países están en la frontera de la IA avanzada y otros luchan por mantener la estabilidad básica de su infraestructura? ¿Cómo se logra una ‘Seguridad sin Fronteras’ real?”

R. Lograr una “Seguridad sin Fronteras” en una región con realidades tan asimétricas no se consigue imponiendo la misma tecnología a todos, sino unificando el conocimiento. Mientras unos mercados debaten sobre IA, otros robustecen su infraestructura básica; el puente entre ambos mundos son las buenas prácticas compartidas. En ALAS resolvemos este desafío convirtiendo las soluciones locales en estándares regionales.

Un ejemplo concreto de esto es el primer Estándar Técnico ALAS para la Seguridad en Urbanizaciones Cerradas —solo en la provincia de Buenos Aires, Argentina existen unas 900 comunidades de este tipo—. Desarrollado tras cinco años de análisis e investigación por el Consejo Asesor del Comité Nacional ALAS en Argentina, este estándar mide, evalúa y permite certificar la seguridad de los conjuntos residenciales. Hoy, este modelo ya está siendo adoptado y adaptado por comités de otros países, demostrando que un criterio técnico local puede volverse global.

Esta transferencia de conocimiento se sostiene gracias a una red viva: cerca de 800 socios en 28 países y comités nacionales en 10 naciones (con la proyección muy cercana de abrir nuestro comité número 11 en Venezuela, para lo cual invitamos a todos los profesionales venezolanos a sumarse a ALAS Venezuela). A través de consejos asesores sectoriales, más de 12 Encuentros Tecnológicos anuales en distintas ciudades, la Cumbre ALAS y webinars accesibles para una comunidad de más de 50.000 miembros, logramos que los usuarios finales y los proveedores de tecnología interactúen. La seguridad sin fronteras ocurre cuando uno de nuestros comités nacionales replica con éxito la iniciativa de otro, nivelando la propuesta técnica en toda Latinoamérica. Además, los Premios ALAS a los mejores proyectos de seguridad de la región permiten visibilizar y compartir los mejores casos de éxito de Latinoamérica.

2. “Como líder con base en Colombia, un mercado que ha madurado profundamente en legislación y tecnología de seguridad privada, ¿qué diagnóstico haces de la resiliencia del profesional venezolano? ¿Consideras que la capacidad de adaptación forzada que tenemos en Venezuela nos está dando una ventaja competitiva en términos de ‘Ingeniería de Resiliencia’ que otros países de la región aún no han tenido que desarrollar?”

R. Sin duda alguna. A través de mis actividades de relacionamiento en ALAS, tengo el privilegio de interactuar constantemente con el talento venezolano, y puedo afirmar que su nivel profesional es excepcional. Lo que en Venezuela ha sido una necesidad de adaptación forzada, en el resto de la región lo valoramos como una verdadera “Ingeniería de Resiliencia”. Esta capacidad superior para gestionar la incertidumbre, optimizar recursos limitados y mantener la

continuidad operativa en escenarios críticos les otorga, indiscutiblemente, una ventaja competitiva única. Hoy vemos a líderes de seguridad venezolanos migrar o liderar operaciones corporativas regionales con un éxito rotundo. Su gran fortaleza no es solo técnica; es la agilidad cultural para integrarse a diferentes organizaciones y transformar entornos de alta presión en sistemas estables y eficientes.

3. "Muchos directivos de seguridad siguen atrapados en la 'operatividad del día a día' y descuidan la gestión estratégica. Desde la perspectiva de ALAS, ¿cómo debe mutar el perfil del CEO de seguridad para el cierre de esta década? ¿Debería dejar de ser un experto en armas y cámaras para convertirse en un experto en análisis de datos y continuidad de negocio?"

R. Coincido plenamente con tu planteamiento. El rol tradicional del responsable de seguridad ha mutado de forma exponencial, impulsado por la optimización de costos y las nuevas exigencias del mercado. Para el cierre de esta década, el líder de seguridad debe migrar definitivamente de un enfoque reactivo basado en activos físicos, hacia un rol de gestor estratégico del negocio.

La seguridad ya no puede ser percibida como un gasto operativo, sino como una inversión estratégica que genera retornos tangibles. Nuestro enfoque en ALAS promueve la integración de servicios tecnológicos que protegen a la organización y, al mismo tiempo, generan valor para su operación. El verdadero desafío actual es dominar la convergencia entre la ciberseguridad, la Inteligencia Artificial y las nuevas tecnologías, alineándolas de forma milimétrica con los objetivos comerciales y la continuidad del negocio.

4. “Estamos en un punto donde la tecnología nos permite saberlo prácticamente todo de cualquier persona en nombre de la seguridad. Siendo ALAS un referente ético, ¿dónde trazamos la línea en 2026? ¿Estamos sacrificando el derecho a la privacidad en el altar de la protección, o existe una fórmula tecnológica para garantizar ambas?”

R. En ALAS sostenemos que la fórmula correcta no es elegir una sobre la otra, sino garantizar la “Privacidad con Seguridad”. En mis años moderando paneles de expertos en la región, una especialista en ciberseguridad me dio esa frase que hoy es nuestra bandera. La tecnología actual nos da un poder sin precedentes, pero el límite ético lo marcan la gobernanza de los datos, la legislación local y el respeto a la cadena de custodia de la evidencia para que sea útil a la justicia.

Existen formas viables de equilibrar ambos mundos. Un ejemplo positivo es la integración regulada de cámaras privadas a los centros de monitoreo públicos (C4 o C5). Esto expande la cobertura urbana sin costos de hardware para el Estado, respetando perímetros y colaborando directamente en la resolución de incidentes bajo marcos legales claros.

Por otro lado, la innovación nos desafía constantemente. Hoy ya vemos tecnologías como los escáneres Bluetooth de largo alcance, capaces de asociar los dispositivos dentro de un vehículo con su matrícula para luego rastrear a los ocupantes. Es aquí donde la línea ética debe ser firme: herramientas tan invasivas no pueden operar en el vacío legal. La tecnología siempre va más rápido que las leyes, y nuestro rol en ALAS es orientar a la industria para que la protección de los ciudadanos no vulnere sus derechos fundamentales.

5. “Venezuela cambió después del 3 de enero y la percepción del riesgo es otra. Si pudieras hablarle al oído a todos los socios de ALAS que leerán esta edición de junio de ‘Seguridad en Acción’, ¿cuál es esa amenaza silenciosa que todos estamos ignorando hoy por estar distraídos con la IA y los drones? ¿Hacia dónde debe mirar el líder de pensamiento que no quiere ser sorprendido por el próximo ‘Cisne Negro’?”

R. El próximo “Cisne Negro” no nacerá de un fallo en la Inteligencia Artificial ni del ataque de un dron; nacerá de nuestra propia desconexión con la realidad social. Mientras la industria se deslumbra con la revolución tecnológica, la amenaza silenciosa que estamos ignorando son las profundas fracturas estructurales de nuestra región.

Las cifras de nuestro entorno son un llamado urgente a la acción. De acuerdo con el ranking anual del Consejo Ciudadano para la Seguridad Pública y la Justicia Penal de México, de las 50 ciudades más violentas del mundo, más de 40 se encuentran en Latinoamérica. Concentramos apenas el 8% de la población global, pero generamos más del 25% de los homicidios del planeta.[1]

A este panorama violento se suma el último informe de la CEPAL, que advierte que unos 162 millones de latinoamericanos (un 25% de la población) viven bajo la línea de la pobreza.[2] Somos una de las regiones más desiguales del planeta: el 10% más rico capta el 34,2% del ingreso total, mientras el 10% más pobre subsiste con el 1,7%. Con casi la mitad de la población ocupada en la informalidad y un alarmante rezago en la educación secundaria, el tejido social está bajo una presión extrema.

Mi mensaje para todos los socios de ALAS es claro: la tecnología es una herramienta extraordinaria, pero no es la solución definitiva. El verdadero líder de pensamiento debe entender que la seguridad privada ya no puede gestionarse de forma aislada a la realidad socioeconómica. Si queremos anticipar las crisis del futuro, debemos mirar hacia la raíz del problema, integrando la tecnología corporativa con estrategias sólidas de prevención y desarrollo social.

1. Ranking Consejo Ciudadano para la Seguridad Pública y la Justicia Penal de México (1)
2. https://www.cepal.org/es/comunicados/la-concentracion-ingreso-sigue-siendo-extrema-america-latina-10-mas-rico-capta-342

Adolfo M. Gelder - Editor

Clima preventivo y convivencia comunitaria

COMO ESTRATEGIA DE SEGURIDAD EN VENEZUELA

En un sector residencial, los conflictos entre vecinos iniciaron como desacuerdos menores y evolucionaron hacia conductas hostiles, afectando la convivencia.

La repetición de estos episodios evidenció una disminución del control social informal y un debilitamiento de los vínculos comunitarios. Desde una perspectiva criminológica, estos escenarios permiten observar cómo la pérdida de cohesión social y la ausencia de mecanismos de regulación social pueden favorecer la aparición de factores criminógenos.

La seguridad no se limita a la intervención formal, sino que también se construye desde dinámicas regulares que influyen en la conducta colectiva.

Reforzar la cultura preventiva resulta necesario. Promover el diálogo, reconstruir normas compartidas y fomentar la participación comunitaria son herramientas clave para reducir la violencia y consolidar entornos sociales más seguros.

La prevención no inicia en la norma, sino en la conciencia colectiva que decide NO normalizar la violencia.

Leila Castillo

Abogada con formación en perfilación criminal y análisis conductual, con conocimientos en seguridad privada y evaluación estratégica de riesgo.
Desarrolla análisis técnico de patrones de conducta y dinámicas de poder en contextos jurídicos e institucionales, con enfoque estructural preventivo y estratégico.

AMADEO GONZÁLEZ
CEO TECNO SISTEMAS BFG, C.A.

Tecnología de Infraestructura, Ciberseguridad y Continuidad de Negocio

Las amenazas modernas no conocen fronteras físicas. En una era hiperconectada, la infraestructura técnica y los activos digitales son blancos constantes de ataque. Amadeo González, líder de Tecno Sistemas BFG, C.A., nos explica en exclusiva cómo su organización diseña "trajes a la medida" para blindar a las empresas venezolanas. Desde auditorías de Ciberseguridad avanzadas (Pen Testing) hasta sistemas robustos de Energía Segura y Disaster Recovery, BFG nos demuestra por qué la resiliencia tecnológica es el pilar indispensable para que un negocio nunca se detenga.

1. **Amadeo, Tecno Sistemas BFG se define a través de tres pilares críticos: Tecnología de Infraestructura, Ciberseguridad y Continuidad de Negocio. ¿Cómo logran que estas tres áreas converjan para que un cliente no vea la seguridad como compartimentos aislados, sino como un ecosistema blindado que protege desde el cableado físico hasta sus activos digitales más sensibles?**

   R: La idea siempre ha sido mostrar a los directores de las empresas una visión gerencial sobre el riesgo, es decir, no quedarnos solo con un planteamiento técnico, ya que en la mayoría de los casos las personas que toman decisiones en las organizaciones no siempre comprenden el lenguaje técnico. Por eso, a veces es mejor mostrar una visión holística sobre cómo el riesgo afecta transversalmente todas las áreas dentro de su empresa para que entonces puedan darle un valor real a nuestra propuesta a través de nuestras tres áreas de competencia.

2. **En su oferta destacan servicios especializados como Pen Testing y Disaster Recovery. En un entorno donde las amenazas son cada vez más sofisticadas, ¿cómo diseña BFG un plan de recuperación que garantice que, tras un incidente crítico, una empresa pueda retomar su operación en tiempo récord sin perder su reputación ni sus datos?**

   R: La continuidad de negocios (BCP/BCM) es la capacidad de una organización para mantener funciones críticas y reanudar operaciones rápidamente tras interrupciones (ciberataques, desastres, fallos técnicos), minimizando pérdidas económicas y operativas. Se basa en identificar riesgos, proteger activos clave y definir estrategias de respuesta, generalmente bajo la norma ISO 22301.

   Componentes Clave de un Plan de Continuidad (BCP): Análisis de Impacto al Negocio (BIA): Identifica procesos críticos y sus tiempos de recuperación objetivos (RTO/RPO).

   Evaluación de Riesgos: Analiza amenazas potenciales, desde desastres naturales hasta fallas de TI.

   Estrategias de Recuperación: Medidas preventivas, de respaldo y planes de contingencia (teletrabajo, sitios alternos).

   Gestión de Crisis: Estructura ordenada para tomar decisiones ágiles y gestionar la comunicación.

   Beneficios de Implementar BCM: Reducción de Tiempo de Inactividad: Minimiza el impacto financiero y la pérdida de datos.

   Protección de la Reputación: Asegura a clientes y partes interesadas que la empresa puede manejar crisis.

   Cumplimiento Normativo: Alinea a la organización con estándares internacionales como la ISO 22301.

   Diferencia Clave: Mientras el BCP se enfoca en la continuidad operativa, el Plan de Recuperación ante Desastres (DRP) se centra en restaurar la infraestructura tecnológica y datos.

3. Ustedes consideran la Energía Segura como una pieza clave de la Continuidad de Negocio, manejando desde UPS hasta Grupos Electrógenos de clase mundial. ¿Por qué para Tecno Sistemas BFG la gestión eléctrica es un asunto de seguridad estratégica y no simplemente un tema de mantenimiento preventivo?

R: Lo primero que debemos aterrizar en este sentido es el entorno donde operan las organizaciones, sus procesos y entender la sensibilidad que puedan tener para cada caso a una mala calidad en la energía eléctrica dentro de su operación. Desde hace mucho tiempo la energía eléctrica ya no es solo una materia prima, es un bien preciado que forma parte de todo proceso productivo, garantizar su calidad y su continuidad puede ser parte de una estrategia en la cadena de producción, incluso desde el punto de vista financiero, ya que al minimizar lo más que se pueda una parada no programada dentro de cualquier proceso de producción puede afectar incluso las primas de seguro y de reaseguro de cualquier corporación. Es por todo lo anterior que nosotros vemos a la Energía Segura como un concepto fundamental en la visión que todo gerente o director debe tener dentro de su organización.

4. Su filosofía establece que la videovigilancia y el control de acceso no deben ser solo herramientas forenses, sino activos estratégicos que previenen riesgos y aportan valor al mercadeo. ¿Cómo transforman ustedes estos sistemas tradicionales en herramientas de inteligencia de negocios que generan un retorno real sobre la inversión para sus clientes?

R: Uno de los factores diferenciadores que tiene Tecno Sistemas BFG con respecto a su competencia en el mercado es el alto nivel de su personal profesional y, en la convicción absoluta sobre los resultados que se obtienen con la formación continua en todas las marcas y/o sistemas que actualmente manejamos y representamos. Esto ha permitido conocer todas las bondades que el avance de la tecnología nos brinda, así como, la reciente intervención de la IA en el procesamiento de las imágenes y metadatos que hoy en día manejan los procesadores de imágenes en las marcas que manejamos, de tal manera que el valor agregado que ponemos en las manos de nuestros clientes es entender cómo estos sistemas de video vigilancia pueden aportar información importante para sacar provecho en entornos industriales y comerciales.

5. Desde la asesoría e ingeniería hasta la procura y construcción, ustedes acompañan al cliente en todo el ciclo de vida del proyecto. ¿Qué significa para BFG entregar un "traje a la medida" en un mercado tan exigente como el venezolano y cómo aseguran que esa solución siga siendo escalable frente a los retos tecnológicos del 2026?

R: Nuestra filosofía comercial está fundada en un profundo respeto a las ideas y a las necesidades de nuestros clientes, por lo cual, nuestras soluciones deben ser prácticamente un alter ego de cómo ellos ven su negocio. Esto se traduce en una visión clínica sobre cómo nosotros podemos traducir aquella necesidad o problema en algo que no solo sea una solución, sino que pueda ser un proyecto viable desde el punto de vista técnico y financiero. Pensando siempre en el futuro para que las soluciones no sean rígidas, sino que también puedan ser escalables, actualizables y siempre están al día tecnológicamente hablando para sacar su mejor provecho sobre la inversión. Sumado a lo anterior, transferimos a nuestros clientes la mayor cantidad de información posible. Esto crea confianza y saca el mejor provecho a la tecnología que sea implementada.

Adolfo M. Gelder - Editor

De las Salas de Monitoreo
A LA INTELIGENCIA DE SEGURIDAD

La seguridad electrónica demanda capacidad de procesamiento, capacidad predictiva y capacidad de detectar y neutralizar amenazas antes de que estas se conviertan en un incidente.

En la actual Gestión de Riesgos, las Salas de Control y Monitoreo (SCM) han dejado de ser simples centros de visualización de cámaras y recepción de alarmas, para convertirse en la unidad central y el cerebro de la seguridad corporativa, lo que quiere decir que, hoy en día, mantener a un operador solamente observando imágenes de cámaras es mantenerse en el pasado; la actualidad de la seguridad electrónica demanda capacidad de procesamiento, capacidad predictiva y capacidad de detectar y neutralizar amenazas antes de que estas se conviertan en un incidente.

Es evidente notar, desde nuestra perspectiva como profesionales de seguridad, cómo la tecnología avanza a pasos agigantados, incluso superando la velocidad y la capacidad con la que las organizaciones pueden actualizar sus sistemas. Es por ello que, en estos nuevos tiempos, para lograr obtener un mínimo de excelencia operativa en el campo de la seguridad electrónica, necesariamente se debe migrar hacia modelos tecnológicos de control y seguimiento, basados en herramientas de vanguardia, tales como: IA y Autonomía Real, Analítica Prescriptiva, Protocolos de Ciberseguridad, Interfaces Inmersivas y Nube Híbrida, entre otros. A continuación, detallo la ventaja posicional que ofrece cada una de estas herramientas:

- **La IA y la Autonomía Real,** dentro de una SCM, pueden validar señales de alarmas sin intervención humana de primera línea, detectando comportamientos anómalos mediante análisis biomecánicos en tiempo real.

- **La Analítica Prescriptiva** (a diferencia de la Big Data que nos decía "qué pasó") nos dice "qué hacer", mediante el uso de un Gemelo Digital que simula escenarios de crisis en entornos virtuales, antes de activar cualquier respuesta en la realidad física.
- **Los Protocolos de Ciberseguridad**, mediante una verificación constante, nos permiten blindar la integridad de los datos contra ataques que intenten vulnerar la IA.
- **Las interfaces Inmersivas utilizan tableros de Realidad Aumentada,** permitiendo el "ingreso virtual" al sitio del incidente con capas de datos superpuestas, para lograr una toma de decisiones mucho más efectiva y precisa.
- **Por último, la nube híbrida** se trata de una solución que permite una gestión de evidencias fluida y un acceso remoto seguro, facilitando la colaboración inmediata con los organismos de seguridad del Estado.

A pesar de todas estas herramientas de automatización, el criterio humano continúa representando el eslabón fundamental, por lo que el perfil del antiguo "Ceconista" ha venido evolucionando al de un "Analista de Inteligencia de Seguridad", en virtud de que se trata de un profesional que debe estar debidamente capacitado con las tecnologías que opera, así como en el manejo de situaciones de crisis y gestión de entornos con alto flujo informativo. Es aquí donde la International Security Alliance (INSEAL), en una alianza estratégica de alto nivel con empresas líderes como SECURTEC 360, de Costa Rica y ZAHLEN, de México, marca la pauta con programas de formación de élite. En abril 2026 hemos presentado el robusto Programa Integral de Formación de Operadores de Salas de Control y Monitoreo, el cual comprende un total de 15 módulos diseñados y estructurados para actualizar al personal de esta área en temas tecnológicos y críticos inherentes al área, entre ellos: Inteligencia Artificial aplicada a la Videovigilancia, Gestión Avanzada de GPS y Rastreo Satelital y Operaciones de Seguridad con Drones.

Lo que nos convierte en punta de lanza es que no solo capacitamos y formamos líderes en tecnología de seguridad. Gracias a nuestro convenio, estos estudios cuentan con el aval universitario del Instituto de la Seguridad "San Juan de Estudios Superiores" de Zacatecas, México, garantizando que el egresado cuente con una certificación con validez a nivel internacional.

Los invitamos a visitar nuestro portal web www.inseal.us y explorar nuestras ofertas académicas en la plataforma "INSEAL – Crea Facilito", que es un espacio de formación asincrónica, accesible y de un elevado e indiscutible nivel profesional, pensado para aquellos líderes que entienden que la seguridad y la actualización constante son el único estándar de cumplimiento válido.

Ramón Mejías
Senior Security Advisor
INSEAL-USA
T.S.U. Ramon Mejias. Consultor de Seguridad Corporativa & Senior Security Advisor INSEAL-USA. Instructor Internacional acreditado en Autoprotección y Sistema de Combate Militar y Policial (SISCOMP).

SEGURIDAD CON
Calidad y Lealtad

PEDRO VALLEJO
CEO CORPORACIÓN PROTEX

La protección en el siglo XXI exige un compromiso que va mucho más allá de la fuerza perimetral. Pedro Vallejo, Director de Corporación Protex, nos presenta un enfoque empresarial profundamente disruptivo, donde la responsabilidad social, el bienestar del capital humano y el apoyo corporativo integral (jurídico y administrativo) se configuran como una ventaja competitiva. Descubra cómo Protex está transformando la gestión de riesgos en Venezuela mediante un modelo de negocio sostenible que pone a las personas en el centro de la estrategia defensiva.

1. Muchos ven la seguridad como un servicio de fuerza, pero Protex Seguridad pone un énfasis especial en la formación con sentido humano y la responsabilidad social. ¿Cómo influye este compromiso con el bienestar de sus oficiales en la calidad del servicio que recibe el cliente final y por qué la sostenibilidad es hoy un factor clave para la seguridad privada en Venezuela?

Para nosotros, la seguridad no es una cuestión de fuerza, sino de confianza. Entendemos que un oficial que se siente valorado, empoderado y respetado, proyecta esa misma dignidad en su puesto de servicio. Ese bienestar se traduce directamente en calidad y lealtad hacia el cliente. En cuanto a la sostenibilidad, no es un accesorio; en la Venezuela actual, ser sostenibles significa ser responsables con el entorno que nos permite operar. Un servicio de seguridad que no impacta positivamente en su comunidad está incompleto.

2. Ustedes no solo ofrecen vigilancia; forman parte de una corporación con servicios jurídicos y contables. En el diseño de una estrategia de resguardo para una gran empresa: ¿Cuál es la ventaja de que un mismo aliado comprenda tanto el riesgo físico en la puerta como el riesgo legal y administrativo en las oficinas?

La seguridad moderna debe ser integral. Al entender los riesgos legales y administrativos, no solo protegemos activos físicos, sino la continuidad del negocio. La ventaja para el empresario es la coherencia estratégica: esto nos permite diseñar soluciones que mitigan vulnerabilidades antes de que se conviertan en un problema jurídico o financiero, ofreciendo una tranquilidad de 360 grados.

Hoy, la analítica de video avanzada y el monitoreo inteligente en tiempo real están marcando la diferencia,

3. La trayectoria de PROTEX SEGURIDAD demuestra una gran capacidad de mantenerse y evolucionar en el mercado nacional. Para esta edición dedicada a la Estrategia de Carabobo: ¿Cuáles han sido esas tácticas de adaptación que le han permitido a Protex Seguridad seguir siendo una opción confiable frente a los desafíos económicos y operativos de este 2026?

Ante los desafíos económicos de este 2026, nuestra táctica ha sido no retroceder en la inversión en nuestro talento. Mientras otros recortan en capacitación, nosotros la reforzamos. La adaptabilidad no es solo sobrevivir al cambio; es liderar la evolución de la industria siendo más eficientes y manteniendo la honestidad como nuestra brújula, incluso en entornos inciertos.

4. En sus redes sociales mencionan la incorporación de tecnología avanzada. ¿Cómo seleccionan las herramientas tecnológicas para que realmente potencien al talento humano y no sean solo un adorno? ¿Qué innovación específica está marcando la diferencia hoy en sus puestos de servicio?

En Protex Seguridad, la tecnología nunca reemplaza al hombre; lo eleva. Seleccionamos herramientas que actúen como multiplicadores de fuerza para nuestros oficiales, asegurándonos de que cada innovación sea una solución real y no un adorno. Hoy, la analítica de video avanzada y el monitoreo inteligente en tiempo real están marcando la diferencia, permitiendo que nuestro equipo pase de ser reactivo a ser preventivo, optimizando cada segundo de respuesta.

5. Si tuvieran que definir el estándar Protex Seguridad para la próxima década: ¿Hacia dónde debe mirar el empresario venezolano hoy para que su seguridad sea proactiva y no solo una respuesta ante el incidente ya ocurrido?

El estándar de Protex Seguridad para los próximos diez años es la prevención inteligente. El empresario venezolano debe dejar de mirar la seguridad como un gasto reactivo y empezar a verla como una inversión estratégica. El futuro está en la sinergia entre el talento excepcional y la vanguardia tecnológica. Para que la seguridad sea proactiva, hay que mirar hacia la gestión de datos, la ética profesional y, sobre todo, hacia la formación de equipos que tengan el criterio para anticiparse al riesgo.

Adolfo M. Gelder - Editor

Una cosa es Eficacia y otra es Función

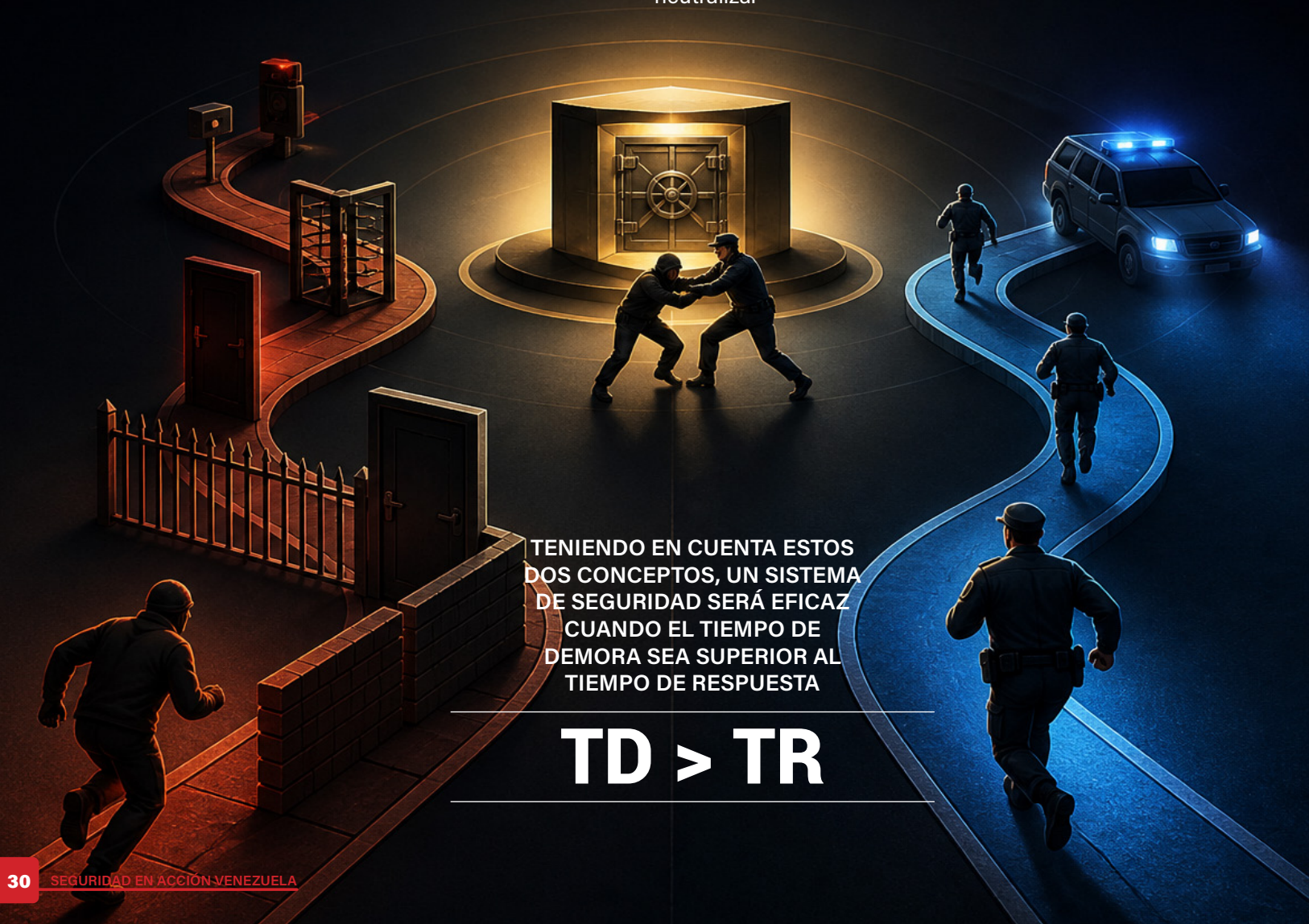
EN UN SISTEMA DE SEGURIDAD FÍSICA

En una Venezuela cada vez más volcada hacia la ciberseguridad, existe el riesgo de subestimar el pilar fundamental de cualquier estrategia de protección: la seguridad física enfocada como sistema. La eficacia de un sistema de este tipo no se mide simplemente por la robustez de una puerta, la resolución de una cámara o la sensibilidad de una alarma, sino por su capacidad de reducir o neutralizar los riesgos.

Para comprender mejor, vamos a definir dos conceptos:

(Td) Tiempo de demora o retardo es el que transcurre desde que se produce el intento de intrusión o la alarma, hasta que el agente dañino alcanza su objetivo en el interior del área protegida.

(Tr) El tiempo de respuesta es el tiempo disponible para la fuerza de respuesta, que transcurre desde que se activa la alarma, hasta que la fuerza de respuesta logra interceptar al agente dañino y lo neutraliza.



TENIENDO EN CUENTA ESTOS DOS CONCEPTOS, UN SISTEMA DE SEGURIDAD SERÁ EFICAZ CUANDO EL TIEMPO DE DEMORA SEA SUPERIOR AL TIEMPO DE RESPUESTA

TD > TR

Para que un sistema de seguridad física sea realmente efectivo, debe cumplir con cinco funciones básicas:

Disuasión	Retardo o demora	Detección o alarma	Identificación	Reacción o respuesta
Medidas Pasivas y Medidas Activas	Medios técnicos pasivos	Medios Técnicos Activos y Humanos	Sistemas Activos, Medios Humanos y Alarmas	Medios Humanos y Sistemas Activos

1. Disuasión: Esta función es prioritaria, se consigue mediante la prevención y consiste en establecer distintos medios de defensa, a través de elementos físicos. Sistemas pasivos de seguridad, como vallas, puertas, concertinas, etc., y sistemas activos de seguridad, elementos como iluminación perimetral, señalética de advertencia y presencia de guardias buscan influir en la psicología del intruso. Un sistema eficaz convence al atacante de que el costo o el riesgo de intentar el ingreso es demasiado alto. Si esto no funciona, entonces se activa la siguiente función del sistema.

2. Demora o retardo: función que tiene por objeto obstaculizar, dificultar o retardar el acceso a una instalación por puntos no autorizados, al tiempo que obliga a utilizar la fuerza y la violencia para acceder al recinto protegido.

3. Detección: Aquí entran los sensores de movimiento, cercas electrificadas y sistemas de video con analítica. La detección busca identificar oportunamente una intrusión o evento anómalo mediante sensores, cámaras o alarmas.

4. Identificación: consiste en reconocer de manera rápida y fiable cualquier acción no autorizada o accidente imprevisto. La identificación de una alarma es determinante para poner en marcha la respuesta adecuada al tipo de alarma que se produzca. Está constituida por cuatro fases: alarma, comprobación, análisis y decisión.

5. Reacción: tiene por objetivo poner en marcha las acciones de respuesta adecuadas a cada tipo de incidente, por lo general es el componente humano o procedimental. De nada sirve una alerta inmediata si no existe un protocolo de reacción claro, con el fin de restablecer la normalidad.

Conclusión

Evaluar la eficacia de la seguridad física no es una tarea de **"instalar y olvidar".** Requiere auditorías constantes, pruebas de penetración y mantenimiento preventivo. En última instancia, un sistema eficaz no es el que promete ser impenetrable, sino aquel que reduce el riesgo a un nivel gestionable, protegiendo lo más valioso: los activos y las vidas humanas.

Luis Silva Ascanio

LIC. EN EDUCACIÓN

Profesor universitario, andragogo, 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.

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

JESÚS GOYO
DIRECTOR COMERCIAL - RBJG

SEGURIDAD LABORAL E HIGIENE

La productividad de una industria es directamente proporcional a la seguridad de su entorno laboral. Jesús Goyo, líder de Multiservicios RBJG 2000 C.A., nos adentra en el vital mundo de la Seguridad, Higiene y Ambiente (SIAHO). En esta nota, Jesús Goyo rompe con el enfoque tradicional de la prevención de accidentes para demostrarnos cómo una cultura laboral preventiva y un asesoramiento técnico riguroso se traducen en rentabilidad, bienestar y soberanía operativa para el sector corporativo nacional.

1. Jesús, desde tu rol como Director Comercial, ¿cómo logras que un empresario vea la inversión en Seguridad Laboral e Higiene, no como una "salida de dinero" impuesta por la ley, sino como una herramienta de rentabilidad que reduce costos ocultos y aumenta la eficiencia de su nómina?

JG. Me parece genial que comencemos con esta pregunta, nuestro modelo de inspecciones le hace comprender al patrono que no es un tema meramente administrativo o de cumplir con la norma, sino que por el contrario, es más costoso a la larga cubrir los gastos por un incidente, accidente o enfermedad ocupacional de uno de sus colaboradores. La idea es minimizar un resultado no deseado como los que acabamos de mencionar. Al mantener a tu equipo cumpliendo con las normas básicas de seguridad y salud laboral, ejecutar un cronograma de capacitaciones y cumplir con actividades del buen uso del tiempo libre, cuentas con un personal motivado. Eso impacta directamente en la productividad y la eficiencia y a su vez cumples con la ley.

2. Con más de 10 años en el mercado venezolano, han visto nacer y desaparecer a muchos competidores. ¿Cuál es ese pilar fundamental en la propuesta comercial de RBJG 2000 que ha permitido que las empresas sigan confiando en su asesoría para navegar las inspecciones de INPSASEL y el cumplimiento de la LOPCYMAT?

JG. Esto lo tenemos muy claro: la clave es la personalización del servicio, en muchos casos las empresas y trabajadores del área se rigen por manuales y formatos genéricos que no te llevan a un resultado efectivo, nosotros nos basamos en trabajar de la mano con el cliente para entender su dinámica y así adaptamos nuestros servicios a sus operaciones reales, nuestros especialistas en el área están en constante desarrollo y aprendizaje para poder ofrecer tecnología y calidad a nuestros aliados. Por ejemplo, al entregar un Programa de Seguridad y Salud en el Trabajo o un análisis de riesgo, el inspector no encuentra vacíos ya que manejamos con precisión la norma y a su vez las operaciones del cliente. Las empresas no nos contratan para que les hagamos el papeleo, nos contratan porque saben que sus operaciones están seguras.

3. En la "Batalla de Carabobo" corporativa que planteamos en esta edición, la retaguardia es la salud del trabajador. ¿Cómo ayuda la consultoría técnica de su equipo a que una empresa pueda enfocarse en crecer y vender, con la tranquilidad de que su frente legal y ambiental está blindado ante cualquier contingencia?

JG. Desarrollamos auditorías técnicas internas que permiten validar el cumplimiento de la normativa en tiempo real, comunicando y trabajando en conjunto con el patrono para lograr los objetivos del Programa de Seguridad y Salud Laboral y de la organización. Cuando una empresa intenta gestionar su seguridad de forma improvisada, el dueño vive apagando incendios. Al contar con nosotros, asumimos la carga técnica, vigilamos los vencimientos, las normativas actualizadas y los estándares técnicos. Si surge una duda legal o ambiental, la respuesta no la busca el dueño, la damos nosotros.

4. La seguridad industrial ha evolucionado hacia la gestión integral del ambiente y el bienestar. ¿Qué nuevos servicios o enfoques están incorporando RBJG 2000 en su oferta comercial para este segundo semestre de 2026 que respondan a las exigencias de un mercado cada vez más consciente y fiscalizado?

JG. Para este semestre, hemos entendido que la seguridad ya no se trata solo de evitar accidentes, sino de potenciar el bienestar como un activo estratégico. Nuestra oferta ha evolucionado para convertirnos en un Servicio de Seguridad y Salud en el Trabajo Integral. Dicho

esto, estamos trabajando en una Gestión Predictiva y Transformación Cultural, más allá del modelo reactivo, enfocados no solo en buscar el cumplimiento legal (INPSASEL, LOPCYMAT), sino integrar la salud y seguridad en el ADN del negocio para mejorar la reputación y productividad de nuestros clientes. Realizamos auditorías bajo una premisa proactiva que nos permite evaluar no solo el equipo, sino también el liderazgo y la participación activa de los trabajadores.

5. Jesús, como líder comercial de una empresa referente en el área: ¿Qué le dices al dueño de negocio que hoy cree que puede "ahorrar" descuidando su gestión de Higiene y Ambiente? ¿Cuál es el costo real de no contar con un aliado experto en el momento en que ocurre un evento adverso?

JG. En Multiservicios RBJG 2000 entendemos perfectamente la presión por los números, sin embargo, mi respuesta para ese dueño de negocio es directa: "No estás ahorrando; estás apostando el patrimonio de tu empresa" cuando ocurre un accidente grave o un desastre ambiental y no tienes un respaldo sólido, el costo no se mide solo en dinero, tienes una responsabilidad penal, una parálisis en las operaciones incluso la destrucción de tu marca. Nunca va a ser mayor el ahorro por no cumplir la norma que por cumplirla. Las sanciones por el incumplimiento de la LOPCYMAT son bastante altas y van desde lo pecuniario hasta la privativa de libertad para los responsables.

Adolfo M. Gelder - Editor

"Las empresas no nos contratan para que les hagamos el papeleo, nos contratan porque saben que sus operaciones están seguras"

Protección ejecutiva en el siglo XXI

Hacia un modelo ontológico, interoperable y teóricamente fundamentado, en el entorno de riesgo de Venezuela

Vivimos en un mundo globalizado, denso en contradicciones, atravesado por conexiones inesperadas y transformaciones aceleradas. Los cambios geopolíticos, las disrupciones tecnológicas y la crisis ambiental han reconfigurado por completo el mapa de riesgos que enfrentan líderes, directivos y figuras públicas. En este contexto, la protección ejecutiva ha dejado de ser una función meramente reactiva o un conjunto de medidas físicas aisladas.

1. BASES ONTOLÓGICAS DE LA GESTIÓN INTEGRAL DE RIESGOS EN PROTECCIÓN EJECUTIVA

Cuando hablo de ontología en este campo, me refiero a una pregunta fundamental: ¿qué entendemos por "riesgo", "vulnerabilidad", "amenaza" y "capacidad de respuesta" en el contexto concreto de proteger a una persona? Sin respuestas claras a estas preguntas, cualquier sistema de protección ejecutiva operará sobre supuestos implícitos, muchas veces contradictorios, lo que genera inconsistencias graves en la identificación y priorización de amenazas.

1.1 Peligro objetivo y riesgo subjetivo

Una ontología sólida debe partir de una distinción central: entre peligro objetivo y riesgo subjetivo. El primero alude a condiciones materiales o acciones hostiles verificables: un explosivo, un atacante armado, un ciberataque al vehículo blindado. El segundo, en cambio, remite a la percepción, la construcción social y emocional del peligro, influida por factores como la exposición mediática, la psicología del protegido o la cultura organizacional.

1.2 El protegido como sujeto situado

La visión tradicional concibe al ejecutivo como un "objetivo a proteger". Esta mirada, además de deshumanizante, es ontológicamente pobre. El ejecutivo moderno es un nodo inmerso en múltiples redes superpuestas: geográficas (movilidad constante), digitales (huella en redes sociales, dispositivos del Internet de las Cosas personal), organizacionales (decisiones estratégicas que generan enemigos) y familiares (personas cercanas que pueden ser vectores de ataque).

2. Tendencias de interoperabilidad en protección ejecutiva

La interoperabilidad es, en esencia, la capacidad de distintos sistemas, organizaciones y tecnologías para trabajar juntos, compartir información y coordinar acciones sin fricciones. En protección ejecutiva, constituye el puente que permite pasar de acciones dispersas (escoltas, blindajes, alarmas, inteligencia) a un verdadero sistema integral de gestión de riesgos.

2.1 Interoperabilidad técnica

Implica conectar sensores, plataformas de videovigilancia, sistemas de geolocalización, aplicaciones de gestión de rutas y centros de comando.

3. Fundamentos teóricos para la protección ejecutiva en la gestión integral de riesgos

La protección ejecutiva no puede reducirse a una lista de procedimientos. Necesita fundamentos teóricos que expliquen por qué ciertos modelos funcionan y otros fallan. Propongo tres marcos esenciales.

3.1 Teoría de la resiliencia en sistemas sociotécnicos

Aplicada a la protección ejecutiva, la resiliencia no es solo "resistir un ataque", sino la capacidad de anticipar, absorber, adaptarse y recuperarse de eventos adversos.

Sus componentes son:

- Anticipación: uso de inteligencia de amenazas futuras.
- Absorción: blindajes, rutas alternas, protocolos de reacción inmediata.
- Adaptación: ajuste de conductas y rutinas basado en lecciones aprendidas.
- Recuperación: restablecimiento de la normalidad funcional y reputacional del ejecutivo.

4. Tecnología y prospectiva en protección ejecutiva

Las nuevas tecnologías están transformando las oportunidades operativas y estratégicas en la gestión de riesgos.

4.1 Tecnologías actuales

- Inteligencia artificial predictiva: modelos de machine learning entrenados con datos históricos de amenazas (acoso, secuestros, atentados) para prever rutas o eventos críticos.
- Biometría conductual: sistemas que detectan anomalías en la forma de caminar del ejecutivo o en sus patrones de uso de dispositivos para identificar coacción.
- Drones de escolta: vehículos aéreos no tripulados para vigilancia perimetral móvil.
- Blindajes ciberfísicos: automóviles que aíslan redes externas y crean cortafuegos móviles.

5. El entorno de riesgo en Venezuela: particularidades que exigen un nuevo modelo

Venezuela representa un caso de estudio particularmente complejo para la protección ejecutiva contemporánea.

La investigación académica ha documentado cómo, durante el período conocido como Puntofijismo (1958-1998), la representación discursiva del riesgo delictivo evolucionó desde la identificación del comunismo como amenaza principal hacia la criminalización de la pobreza, hasta llegar a un clima de anomia donde la propia estructura social se convirtió en potenciadora del riesgo por su incapacidad de proteger a la sociedad.

El riesgo político en Venezuela es particularmente elevado. Estudios internacionales señalan que Venezuela se encuentra entre los países que actualmente se evitan con mayor frecuencia debido al riesgo político percibido, junto con Irán, Libia, Argentina, Rusia y Egipto.

6. Referencias internacionales: lecciones comparadas

La experiencia internacional ofrece valiosas lecciones aplicables al entorno venezolano, siempre con las debidas adaptaciones contextuales.

6.1 Casos globales de alto impacto

El asesinato del ex primer ministro japonés Shinzo Abe en julio de 2022 reveló la vulnerabilidad de las estructuras tradicionales de seguridad incluso en países con bajos índices de violencia. El atacante utilizó un arma casera y disparó a plena luz del día en un acto público; la reacción del equipo de protección fue tardía y desorganizada, evidenciando una desconexión entre protocolo y realidad.

Conclusión

El análisis presentado muestra que la protección ejecutiva, en el marco de la gestión integral de riesgos, trasciende con creces las técnicas tradicionales de seguridad física. Requiere, en primer lugar, una base ontológica que entienda el riesgo como relacional, emergente y multidimensional, situando al ejecutivo como un nodo en ecosistemas complejos. En segundo lugar, necesita tendencias de interoperabilidad semántica, técnica y organizacional que permitan coordinar en tiempo real a actores y sistemas diversos, sin generar nuevas vulnerabilidades. En tercer lugar, exige fundamentos teóricos sólidos –resiliencia, sistemas complejos adaptativos y gestión estratégica del riesgo– que orienten la toma de decisiones en situaciones inciertas y desmantelen el mito de la seguridad absoluta.

Dr. John R. Tovar C., CPO.
CONSULTOR EN SEGURIDAD INTEGRAL
Contacto: 0414-1000724
Correo: jrtovarc@gmail.com
Instagram: @tovar-john

ANTICIPAR PARA PROTEGER

Daniel Jiménez
CEO SECURITY WORLD

En los sectores financiero, retail de alta gama y banca, el margen de error no existe. Daniel Jiménez, Presidente de Security World, nos detalla en esta entrevista los rigurosos protocolos de excelencia, pulcritud y análisis preventivo que han convertido a su marca en el sinónimo de confianza para los clientes más exigentes en el país. Una mirada exclusiva a cómo se gestiona el control de pérdidas en entornos comerciales complejos mediante oficiales de élite e inteligencia logística de vanguardia.

1. **Daniel, Security World es reconocida en el mercado por manejar clientes con estándares de exigencia muy elevados. ¿Cuál es el ADN que diferencia a un oficial de Security World del resto del mercado y cómo logran mantener ese nivel de disciplina y pulcritud en entornos tan complejos como los actuales?**
R. Adoptar estándares internacionales como los que establece ASIS International ha sido un hito transformador para Security World. Nuestro proceso comienza con la selección rigurosa del personal bajo criterios de integridad, aptitud y vocación de servicio. Pero más allá del reclutamiento, hemos construido una cultura de seguridad sostenida: cada oficial recibe inducción estructurada, seguimiento diario de desempeño y evaluaciones periódicas alineadas con las mejores prácticas globales. Creemos que la disciplina no se impone, se cultiva. Y esa cultura la extendemos también hacia nuestros clientes, porque la seguridad efectiva es siempre una responsabilidad compartida.

2. **Ustedes tienen una presencia fuerte en sectores donde el margen de error es cero, como la banca y el retail de alto impacto. ¿Cómo diseñan un plan de seguridad que sea lo suficientemente robusto para disuadir el delito, pero lo suficientemente fluido para no entorpecer la experiencia del cliente o la operación del negocio?**
   R. Como consultores alineados con los estándares de ASIS International, nuestro punto de partida es siempre el negocio del cliente: entender su modelo operativo, sus flujos de personas, sus activos críticos y su tolerancia al riesgo. Sobre esa base diseñamos un Plan de Seguridad Integral que no es un obstáculo, sino un habilitador del negocio. En negocios de alto impacto, esto significa capas de protección escalonadas, disuasión visible, controles de acceso inteligentes y protocolos de respuesta calibrados—todo ello pensado para que el cliente final viva una experiencia fluida y el negocio opere sin fricciones

3. **En esta edición hablamos de Inmunidad Digital y resiliencia. ¿De qué manera Security World está integrando la inteligencia de datos y el análisis de riesgos previo en sus servicios de vigilancia física para anticiparse a las amenazas antes de que lleguen a la puerta del cliente?**
   R. En Security World no esperamos que la amenaza llegue a la puerta: la anticipamos. Nuestro enfoque parte de un análisis de riesgos de base cero, en el que evaluamos el entorno desde dos perspectivas simultáneas: la del atacante externo que busca vulnerabilidades, y la del consultor interno que conoce los puntos ciegos del sistema. Las condiciones del entorno cambian constantemente —y nuestros análisis también. Incorporamos inteligencia operativa, indicadores de alerta temprana y revisión continua de escenarios para mantener los planes de seguridad actualizados y vigentes. La resiliencia no es un estado, es un proceso vivo

4. **Sabemos que la rotación de personal es un reto en este sector. ¿Cómo invierte Security World en la carrera de su personal para asegurar que el oficial que custodia a un cliente hoy, sea un profesional motivado y fiel a los valores de la organización a largo plazo?**
   R. Partimos de una convicción fundamental: no puedes exigir lo que primero no has enseñado. Por eso nuestra inversión en el oficial de seguridad no termina en la contratación. Tenemos programas de capacitación continua en técnicas operativas, manejo de situaciones críticas y atención al cliente, acompañados de un esquema de comunicación abierta y reconocimiento al desempeño. Tratamos a nuestro personal con respeto genuino y presencia real. Un oficial motivado, que siente que pertenece a algo más grande que una guardia, es el mejor activo que cualquier organización de seguridad puede tener

5. **¿Cuál es el compromiso de Security World con el futuro de la seguridad en Venezuela y qué innovaciones podemos esperar de la marca para el cierre de este año 2026?**
   R. Security World está en un momento de crecimiento estratégico. Estamos consolidando procesos bajo estándares de calidad reconocidos internacionalmente, lo que nos permite competir con rigor y transparencia. Y tenemos algo en desarrollo que va a redefinir la forma en que respondemos a nuestros clientes, una solución que, sin adelantar detalles, responde exactamente a las nuevas exigencias del entorno venezolano actual. Nuestro compromiso con el país es claro: profesionalizar el sector, elevar el estándar y demostrar que en Venezuela se puede hacer seguridad de clase mundial.

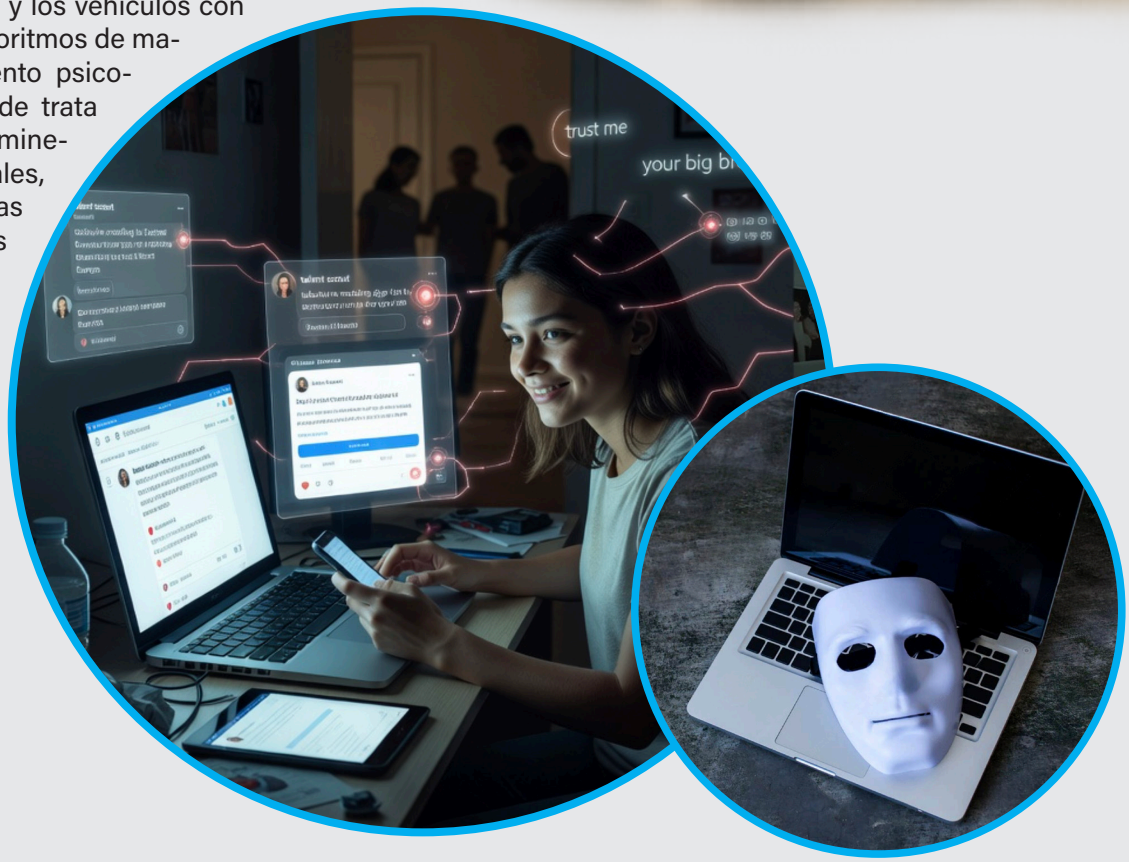
Adolfo M. Gelder - Editor

LA CACERÍA INVISIBLE EN LAS

Pantallas Electrónicas

El asfalto de esa calle venezolana, que aún exhala el calor acumulado de la tarde, es el testigo mudo de una transformación tan silenciosa como dolorosa. En este 2026, la vulnerabilidad ya no siempre viste de harapos ni se evidencia únicamente en la desnutrición física; a veces se esconde tras la luz azul de un teléfono inteligente en manos de un adolescente que, entre risas superficiales, busca una salida a un entorno que parece asfixiarlo.

Como observadores analíticos de esta realidad, entendemos que esa pantalla no es solo un juguete o un mero canal de entretenimiento. Se ha convertido en el umbral de una cacería sofisticada donde el depredador ha cambiado el camuflaje físico, el acecho en las esquinas y los vehículos con vidrios oscuros, por algoritmos de manipulación y perfilamiento psicológico. Hoy, las redes de trata operan mediante una minería de datos emocionales, identificando carencias a través de lo que los jóvenes publican, comentan o incluso de lo que callan en el entorno digital.



La Danza de los Espejismos

La captación comienza con una danza de espejismos milimétricamente calculada.

Tomemos el caso de Victoria, una joven de dieciséis años en un barrio popular de Caracas. Su captador no fue un extraño en un vehículo, sino un perfil impecable en redes sociales que se hacía pasar por un "scout" de modelos internacionales. Este es el rostro moderno del cibergrooming, donde la violencia física es reemplazada por la coerción psicológica.

Durante semanas, la relación se construyó sobre el terreno fértil de la empatía simulada, utilizando técnicas de ingeniería social, La validación emocional: él escuchaba sus frustraciones sobre la falta de futuro en el país y el estancamiento académico, validaba sus nobles deseos de ayudar a su madre con los agobiantes gastos del hogar, mientras que él le enviaba notas de voz que sonaban a una calidez paternal y profesional, llenando vacíos afectivos evidentes.

Cuando él le prometió un contrato en el extranjero, no le pidió dinero; le pidió "confianza". Este es el punto de inflexión táctico. Lo convenció de que, para empezar su portafolio, debía enviarle fotos de prueba que, poco a poco y bajo una falsa premisa de exigencia profesional, fueron subiendo de tono. Una vez obtenido el material, la máscara cayó y el mensaje cambió radicalmente: ya no era una invitación, era una amenaza de publicar su intimidad (sextorsión) si no seguía sus instrucciones de traslado hacia una red de explotación sexual.

O pensemos en el caso de Samuel, un adolescente en una zona rural cerca de la frontera. Para él, el gancho no fue el glamour, sino la necesidad disfrazada de "oportunidad de trabajo". Un conocido de un conocido le escribió por WhatsApp hablándole de un empleo de logística en el sector fronterizo, con un sueldo en divisas que parecía resolver, de un solo golpe, las deudas y las necesidades crónicas de medicinas de su abuela.

El captador, operando como un maestro en el arte de la manipulación emocional, ejecutó un protocolo de aislamiento sistemático. Lo fue aislando gradualmente de su familia, convenciéndolo de que sus padres, con sus miedos y advertencias, eran un "obstáculo para su éxito", le insistió en que, si quería ser un "hombre responsable" y el pilar de su casa, debía tomar la decisión de partir en secreto, evitando las despedidas que "debilitan el carácter". Cuando Samuel llegó al estado Bolívar, el "empleador" ya no existía. En su lugar, se encontró con una estructura de crimen organizado que le confiscó su teléfono (anulando su huella digital y capacidad de auxilio) y le impuso una deuda impagable por el supuesto costo de su traslado. Lo obligaron a trabajar bajo coerción extrema en las minas para pagar un precio inflado y rotatorio que nunca dejará de subir, un fenómeno técnico conocido como peonaje por deudas o esclavitud moderna.

En esta narrativa de captación, el depredador se convierte en un "mentor de crisis". Si el adolescente co-

menta en una publicación lo difícil que es costear los medicamentos de su madre o la inmensa frustración de no poder estudiar, el captador responde con una empatía diseñada quirúrgicamente.

"Yo estuve ahí, sé lo que duele ver a la familia pasando trabajo", dice el victimario, creando una falsa simetría de experiencias.

Este vínculo de confianza sustituye la figura del padre, del Estado o del guía ausente. El simple "me gusta" se transforma rápidamente en conversaciones diarias por aplicaciones de mensajería encriptada, evadiendo la supervisión parental. Allí, la promesa empieza a tomar forma de contrato informal: un empleo en un "comercio" en el estado Táchira, o una oportunidad como "asistente de logística" en las minas de Bolívar, con la promesa anestésica de que el transporte y la comida "ya están pagados por la empresa".

Estos relatos no son incidentes aislados ni anomalías estadísticas; son el reflejo de una explotación estructural que ha mutado hacia un fenómeno de "captación por empatía". El criminal moderno es un gestor de esperanzas rotas. Utiliza la necesidad de ayudar a la familia –ese motor tan noble y arraigado en nuestra idiosincrasia venezolana– para tejer una red de dependencia emocional y económica que, en la práctica, es el robo sistemático de la inocencia y el futuro.

La Fractura del Radar Social y el Agujero Negro Fronterizo

Esta dramática realidad se ve agravada por lo que sociológicamente podríamos definir como la "fractura del radar social". En la Venezuela de hoy, la prolongada crisis ha empujado a las comunidades hacia un hiperindividualismo de subsistencia.

Ese tejido social que antes funcionaba como una red de pesca comunitaria, atrapando los problemas antes de que cayeran al fondo, hoy está deshilachado. La mirada del vecino se ha vuelto hacia adentro, no por maldad intrínseca, sino por un instinto de autopreservación, una fatiga crónica que nos susurra que "no debemos meternos en problemas ajenos". Este silencio cómplice es el oxígeno del tratante. Sin una comunidad alerta que cuestione por qué una joven dejó de ir al colegio repentinamente, o por qué un adulto extraño frecuenta una vivienda a deshoras, el criminal goza de una inmunidad territorial absoluta.

Cuando un adolescente inicia su tránsito hacia estados fronterizos, su rastro se desvanece en un limbo de información. Al llegar a la frontera, el sueño de libertad y prosperidad se estrella violentamente contra la realidad de las deudas impagables por "traslado y logística". En este punto de no retorno, la explotación deja de ser una amenaza lejana para convertirse en una cruda moneda de cambio transnacional. La falta de opciones reales y el aislamiento comunicacional total, donde el tratante confisca el dispositivo móvil y corta todo puente con el pasado, anulan cualquier capacidad de resistencia, dejando al joven a merced de estructuras criminales que ven en el cuerpo humano un recurso puramente renovable, monetizable y desechable.

Hacia la Recuperación de la Humanidad como Escudo

Para revertir esta realidad, la noción de seguridad ciudadana debe trascender las patrullas, los operativos reactivos y los uniformes. Enfrentar la trata y la explotación en 2026 requiere que miremos más allá de las frías estadísticas y los partes policiales.

Debemos ver las historias de libertad que aún pueden ser escritas si decidimos volver a mirar al vecino con responsabilidad colectiva; si nos atrevemos a intervenir de forma segura en esa esquina donde la sombra se proyecta; y si logramos, a través de la educación y el apoyo, que la esperanza de un futuro próspero no sea el cebo de las mafias, sino la justa recompensa de una sociedad que aprendió, desde el dolor, a proteger de nuevo a los suyos.

La sombra del vehículo de vidrios oscuros, ahora metamorfoseada en perfiles falsos, solo desaparecerá cuando la luz de la comunidad sea más fuerte que la del celular que promete falsos paraísos. Al final del día, el análisis técnico, sociológico y criminológico nos da las herramientas teóricas para entender el fenómeno de la trata, pero es la humanidad recuperada, la empatía en acción, la que nos dará la verdadera fuerza para detenerlo. La seguridad es, en su esencia más pura, el derecho inalienable de esos adolescentes a reír en una esquina de su barrio, sin que el sol de la tarde sea lo último que vean en libertad.

Esta trágica transición de la risa en la esquina al silencio sepulcral de la frontera es lo que debemos entender e interiorizar como sociedad. La captación es un proceso de seducción perversa que se nutre directamente de nuestras carencias sistémicas. Para detenerlo, necesitamos urgentemente que la mirada del vecino vuelva a ser un escudo preventivo. Un radar humano capaz de notar las “banderas rojas”: cuando un joven de la cuadra empieza a hablar de “amigos extranjeros” que nunca ha visto en persona, o cuando menciona viajes repentinos y misteriosos hacia las zonas críticas, debemos actuar. Hay que encender las alarmas antes de que su rastro se pierda definitivamente en el mapa, y su voz se convierta en un eco silencioso más en la frontera.

Elías Cabeza

Militar retirado de la Fuerza Aérea Venezolana

Lic. en Criminalística, Convenio FFAANN – CICPC (IUPOLC) Máster en Seguridad Física e Instalaciones Militares, graduado en el Centro de Estudios Militares Avanzados (CEMA), Caracas – Venezuela. Consultor de Seguridad y Coach Ontológico.

www.linkedin.com/eliascabezaconsultor/

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

EL SUPERVISOR

como analista y gestor del riesgo ante la supervisión ineficiente en Venezuela y Latinoamérica

Un análisis crítico sobre la transición necesaria desde el control de formularios estáticos hacia la detección de fallas latentes. Explica por qué el "Teatro de la Seguridad" está dejando vulnerables a las organizaciones en LATAM y cómo implementar una verdadera vigilancia estratégica basada en la resiliencia operativa.

El sector de la seguridad en América Latina se enfrenta hoy a un desafío silencioso pero crítico: la implementación del Teatro de la Seguridad y la institucionalización de la supervisión ineficiente. Venezuela no está exenta de este desafío. En muchas organizaciones, se invierte en tecnología de punta sin contar con la infraestructura de un centro de control o personal capacitado, creando protocolos sin estudios previos de vulnerabilidad.

Cuando la supervisión se reduce a una revisión mecánica de listas de verificación, donde el éxito se mide por el cumplimiento de tareas y no por la detección de anomalías, estamos ante lo que Bruce Schneier define como el "Teatro de la Seguridad": acciones que crean una sensación de seguridad sin mejorarla realmente.

La trampa de los estándares tradicionales

Históricamente, la supervisión se ha basado en indicadores superficiales (uniforme impecable, libros firmados). Sin embargo, este enfoque presenta fallas estructurales:

- **Chequeo superficial:** Importancia de la estética sobre la operatividad real.
- **Procedimientos burocratizados:** Pasos administrativos para satisfacer auditorías, no para proteger activos.
- **Indicadores de cumplimiento vacíos:** Se rinde cuentas al compliance pero se ignora el análisis del riesgo dinámico.
- **Ceguera de taller:** Pérdida de la capacidad de "ver" anomalías reales debido a la repetición mecánica.

Las señales de alerta y el modelo del queso suizo

Para los directores C-Level, es vital identificar una supervisión que no detecte amenazas. Una gestión ineficiente ignora los Indicadores Clave de Riesgo (KRI) y se limita a los Indicadores Clave de Desempeño (KPI).

Aplicando el "Modelo del Queso Suizo" de James Reason, entendemos que los accidentes ocurren cuando las fallas latentes (agujeros en las capas de seguridad) se alinean. Supervisar no es chequear lo hecho; es detectar la falla latente de manera proactiva antes de que el incidente atraviese todas las defensas.

De la "Seguridad I" a la resiliencia operativa

La transición exige un cambio hacia la "Seguridad II" (Erik Hollnagel), centrada en asegurar que las cosas salgan bien potenciando la capacidad de anticipar anomalías. El protocolo requiere:

- **Indagación profunda:** Cuestionar el sistema visualmente ordenado.
- **Enfoque dinámico en el riesgo:** Auditoría de eficacia según vulnerabilidades específicas.
- **Enfoque estratégico:** El supervisor como líder que transmite el "porqué" de las tareas.
- **Cultura de proactividad:** Reporte de "casi-accidentes" sin temor a represalias.

El valor de la autoridad técnica

La seguridad en LATAM debe consolidarse como un referente de análisis crítico. La verdadera calidad de la supervisión no reside en la lista de tareas más larga, sino en el método técnico para detectar fallas antes de que se conviertan en pérdidas irreparables.

El supervisor debe ser un analista de riesgos en tiempo real.

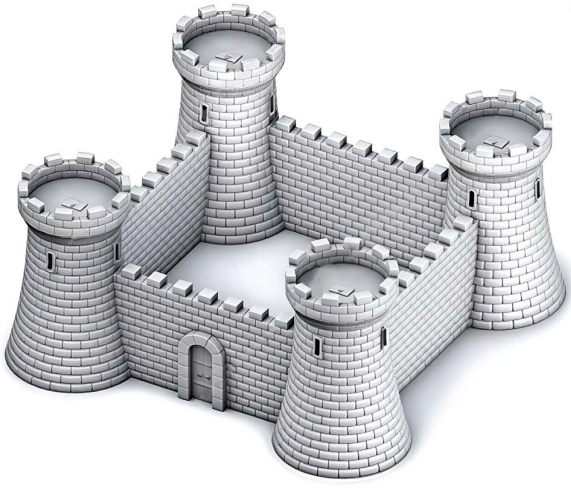
My(r). Marcos Antonio Carrillo Castillo

Consultor y capacitador estratégico de seguridad, con más de 30 años de experiencia. Especialista en análisis de riesgos y protección ejecutiva. Lidera la firma Carrillo & Consultores en Venezuela y miembro activo de la International Foundation for Protection Officers (IFPO).

El Pentágono de la Seguridad
Y LA PROTECCIÓN INTEGRAL

Tiene como finalidad constituirse en una guía práctica y conceptual orientada al fortalecimiento de la calidad en los servicios de seguridad integral. Se propone un ciclo estructurado en cinco pasos esenciales, acompañado de sus círculos derivados, cuyo eje central es la protección de las personas, sus activos y el entorno. Este material se enmarca dentro de los trabajos de investigación de la cátedra Metodología de la Investigación del Doctorado en Seguridad Ciudadana de la Universidad Nacional Experimental de Venezuela.

COMPONENTES DEL PENTÁGONO DE LA SEGURIDAD



1. Introducción histórica y conceptual

Desde los albores de la civilización, el ser humano ha buscado mecanismos para resguardar su integridad frente a las amenazas de la naturaleza, los animales y, posteriormente, de otros individuos. Ejemplos como la ciudad de Jericó (8.530 a.C.), con sus murallas y sistemas defensivos, o los castillos medievales con fosos y barreras naturales, evidencian cómo la necesidad de seguridad ha impulsado la creatividad y el ingenio.

Con el paso del tiempo, la seguridad evolucionó hacia modelos conceptuales más sofisticados, entre ellos los triángulos de análisis que consideran la víctima (objetivo), el victimario, la oportunidad (dónde), el deseo y la motivación (por qué). A estos enfoques se suman principios modernos como la confidencialidad, integridad y disponibilidad, que consolidan una visión de seguridad integral más efectiva, eficiente y adaptada a los desafíos contemporáneos.

2. CONCEPTOS CLAVE

- **Seguridad:** Estado dinámico caracterizado por la ausencia de peligros, daños o temores.
- **Protección:** Conjunto de medidas tangibles aplicadas para preservar la seguridad (paredes, cercas, iluminación, alarmas, cámaras, personal de vigilancia).
- **Seguridad física:** Mecanismos de prevención y detección destinados a salvaguardar instalaciones, bienes y procesos.
- **Protección física:** Acciones de prevención, detección y neutralización de amenazas, apoyadas en controles, registros e inspecciones.

3. SEGURIDAD FÍSICA

La seguridad física se centra en la prevención, detección y neutralización de amenazas que puedan afectar instalaciones, bienes y procesos.

Elementos fundamentales:

- Plan de seguridad.
- Contramedidas tangibles.
- Personal entrenado y motivado (95% de efectividad cuando se combina con sistemas electrónicos y normas).
- Estrategias operativas: controles, registros e inspecciones. Principios de administración aplicados: Planificación, Organización, Dirección, Coordinación y Control.

4. Securitización

Concepto acuñado por Ole Waever (1995), describe el proceso mediante el cual actores políticos (prensa, gobernantes, militares) presentan ante la opinión pública la existencia de amenazas, reales o supuestas, ampliando la noción de seguridad más allá del ámbito militar hacia dimensiones sociales, económicas y ambientales.

5. Premisas Básicas de la Seguridad

1. ¿Qué quiero proteger?
2. ¿Contra qué lo quiero proteger?

Amenaza, riesgo, vulnerabilidad, probabilidad y posibilidad.

6. Indicadores de Gestión

La efectividad del sistema de seguridad se mide con indicadores como:

- Cumplimiento de tareas clave.
- Tiempo promedio de respuesta.
- Asistencia e inspecciones.
- Registro de siniestros y accidentes.
- Optimización de operaciones.
- Reportes de ubicación.

Control de costos y recursos:

- Capacitación estratégica.
- Identificación de riesgos y vulnerabilidades.
- Valoración de usuarios y clientes.

7. Principio de Proporcionalidad

- **Prevención:** 80%
- **Disuasión:** 15%
- **Reacción:** 5%

"LA PREVENCIÓN SIEMPRE GANA."

CONCLUSIÓN

El Pentágono de la Seguridad y la Protección Integral constituye un modelo práctico y conceptual que integra análisis de riesgo, infraestructura, tecnología, políticas y recursos humanos. Su aplicación fortalece la capacidad de prevención y respuesta, optimiza recursos y garantiza la protección de personas, bienes y procesos en cualquier organización.

8. Componentes del Pentágono de la Seguridad

1. Análisis de Riesgo

- Detección y prevención.
- Estudio del entorno, probabilidad de ocurrencia y vulnerabilidades.
- Clasificación: bajo, medio y crítico.
- Conceptos clave: previsibilidad, cadena de seguridad.
- Estrategias: sociedad, comunas, fuerzas de seguridad, organización vecinal.
- Normas de referencia: COVENIN, NFPA, ASIS, ANSI, ASTM, UL, ISO, SDI.

2. Infraestructura

- Protección física de personas y bienes.
- Infraestructura crítica: subestación, planta eléctrica, ascensores, azotea.
- Capas de protección: vigilancia, sistemas electrónicos, contra incendios.
- Círculos de seguridad: perímetro, proximidad, área interna, núcleo protegido.
- Principios: detener, detectar, demorar, denegar.

3. Tecnología (Seguridad Electrónica)

- **Activos:** biometría, videovigilancia con aplicaciones de IA, alarmas, control de rondas, comunicaciones.
- **Pasivos:** cerramientos, concertinas, rejas, cajas fuertes.
- **Tendencias:** automatización, inteligencia artificial aplicada a seguridad.

4. Políticas, Normas y Procedimientos

Políticas: metas de protección.

Normas: reglas y principios de convivencia.

Procedimientos: instrucciones detalladas para actividades específicas.

5. Recursos Humanos y Educación

Supervisión: planificar, organizar, dirigir, coordinar y controlar.

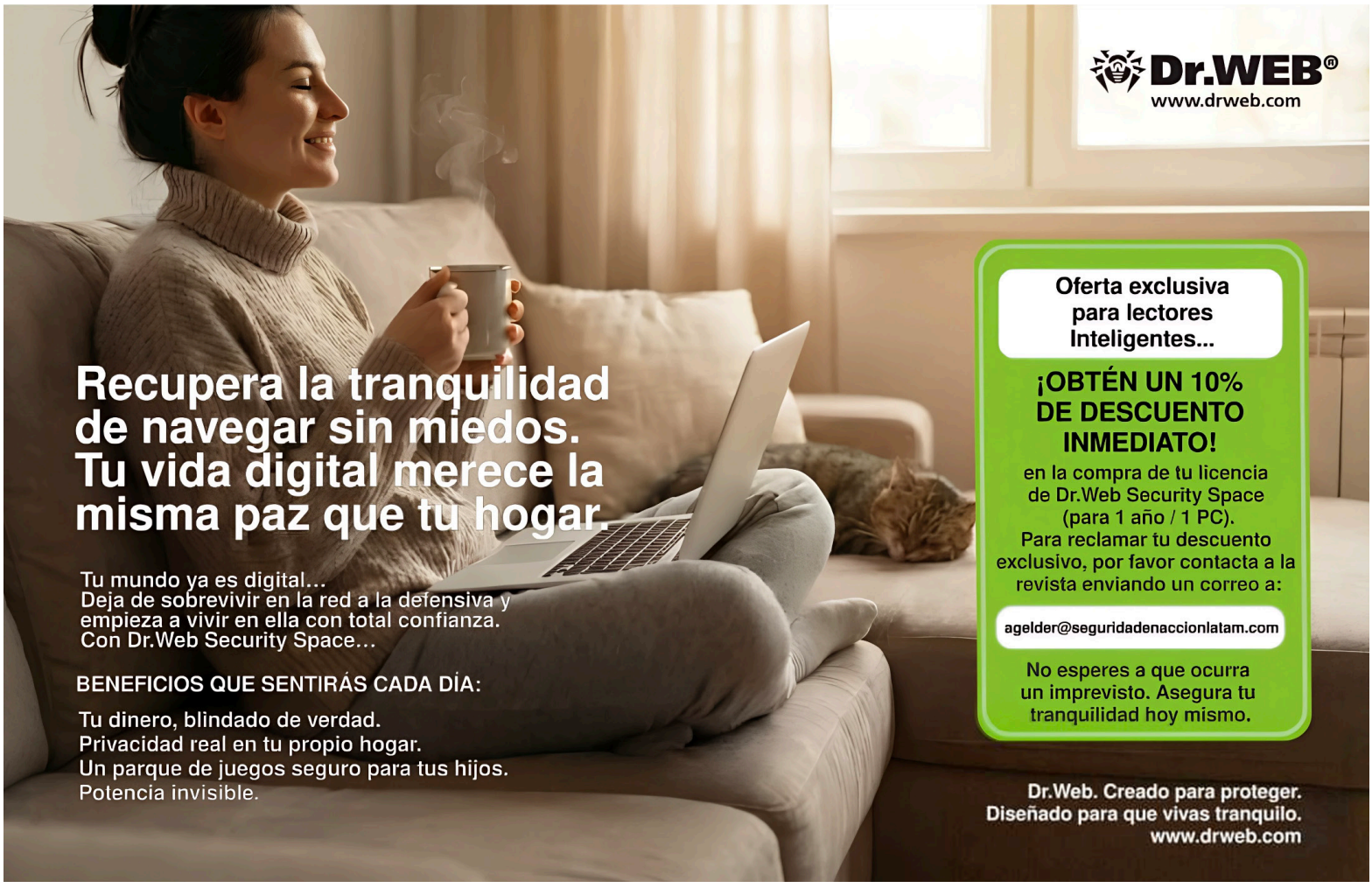
Requisitos: verificación curricular, contratos con cláusulas de confidencialidad.

Formación: inducción, entrenamientos según riesgos, ética y políticas internas.

Liderazgo: delegar, asignar responsabilidades, rendir cuentas.

Principio rector: Nada reemplaza a la experiencia.

Cnel. (B) Dr. Henry Carracedo
Henry Carracedo es un apasionado de la seguridad y la protección integral, se graduó en la ESINFA, es TSU en Riesgos, licenciado, Técnico Medio mención Bomberos, cuenta con una especialización en protección integral, es especialista, magíster y doctor en seguridad ciudadana.


Dr.WEB®
www.drweb.com
Recupera la tranquilidad de navegar sin miedos. Tu vida digital merece la misma paz que tu hogar.
Tu mundo ya es digital...
Deja de sobrevivir en la red a la defensiva y empieza a vivir en ella con total confianza.
Con Dr.Web Security Space...
BENEFICIOS QUE SENTIRÁS CADA DÍA:
Tu dinero, blindado de verdad.
Privacidad real en tu propio hogar.
Un parque de juegos seguro para tus hijos.
Potencia invisible.
Oferta exclusiva para lectores Inteligentes...
¡OBTÉN UN 10% DE DESCUENTO INMEDIATO!
en la compra de tu licencia de Dr.Web Security Space (para 1 año / 1 PC).
Para reclamar tu descuento exclusivo, por favor contacta a la revista enviando un correo a:
agelder@seguridadenaccionlatam.com
No esperes a que ocurra un imprevisto. Asegura tu tranquilidad hoy mismo.
Dr.Web. Creado para proteger.
Diseñado para que vivas tranquilo.
www.drweb.com


Multiservicios·RBJG
J - 409037959
MULTISERVICIOS
RBJG 2000 C.A.
Expertos en Seguridad Laboral, Seguridad Industrial, Higiene y Ambiente.
Seguridad Laboral
Seguridad Industrial
Higiene
Ambiente
"Nuestro trabajo es hacer más fácil tu trabajo"
+58 412 5784756
multiserviciosrbjg2000@gmail.com
@multiserviciosrbjg2000

La Batalla Cognitiva de Junio

El mes de junio evoca en la memoria colectiva venezolana dos conceptos que, a primera vista, pertenecen a mundos diametralmente opuestos: el heroísmo estratégico de la Batalla de Carabobo y la figura protectora, proveedora y orientadora del Día del Padre. Sin embargo, cuando analizamos los desafíos de la seguridad de la información en este año 2026, ambos elementos convergen de forma natural en el centro de la matriz de riesgo. La ciberseguridad ha dejado de ser un asunto meramente técnico —restringido a cortafuegos, parches de software o configuraciones de red— para transformarse en una disciplina profundamente humana, táctica y cultural. Hoy, la protección de una organización se decide en la mente de sus integrantes, bajo una doctrina que exige tanto la genialidad estratégica del despliegue en el terreno como el compromiso ético de transferir un legado de resguardo a las siguientes generaciones.

El 24 de junio de 1821, el ejército patriota no venció por acumulación de fuerza bruta, sino por un diseño táctico disruptivo que rompió las líneas convencionales del adversario mediante el flanqueo, la sorpresa y la sincronización perfecta de sus divisiones. En el panorama de las amenazas informáticas proyectadas para este próximo mes de junio, las organizaciones enfrentan un paralelismo exacto. Los ciberatacantes ya no realizan ofensivas lineales ni predecibles; emplean tácticas de "quinta generación" donde el perímetro físico y los firewalls tradicionales equivalen a las posiciones estáticas que el ejército realista no pudo defender.

Las tendencias para junio muestran un incremento agresivo en ataques de denegación de servicio distribuidos (*DDoS*) potenciados por botnets de Inteligencia Artificial, combinados simultáneamente con campañas quirúrgicas de phishing dirigido (*Spear-Phishing*). Esta es la versión digital del flanqueo por la retaguardia. Mientras el equipo de respuesta a incidentes (*SOC*) concentra toda su atención y recursos en mitigar un ataque volumétrico en la capa de red, los atacantes vulneran la infraestructura crítica a través de un único eslabón comprometido en la cadena de suministro o mediante la suplantación de identidad de un alto directivo.

Para ganar esta nueva "Batalla de Carabobo" tecnológica, los directores de seguridad (*CISO*) deben abandonar la mentalidad de la "seguridad por oscuridad" o la falsa confianza en las murallas digitales. La estrategia moderna exige implementar una arquitectura de Confianza Cero (*Zero Trust*), donde cada usuario, dispositivo y flujo de datos debe ser verificado continuamente. Al igual que la coordinación de las divisiones patriotas en la sabana de Carabobo, los sistemas de seguridad electrónica, la infraestructura de red y los protocolos de ciberseguridad deben operar de manera unificada, interoperable y bajo un mando centralizado capaz de tomar decisiones en milisegundos.

Tradicionalmente, la figura paterna se asocia con la protección activa, la guía, la provisión de herramientas para afrontar el peligro y la responsabilidad de transferir un legado de supervivencia y valores.

Por otro lado, junio es el mes en el que honramos el Día del Padre. En el contexto de la seguridad de la información, este rol adquiere una dimensión profundamente estratégica. Tradicionalmente, la figura paterna se asocia con la protección activa, la guía, la provisión de herramientas para afrontar el peligro y la responsabilidad de transferir un legado de supervivencia y valores. En el ecosistema empresarial, el especialista en ciberseguridad debe encarnar estas mismas cualidades.

Durante décadas, los departamentos de seguridad de la información operaron bajo una doctrina punitiva y restrictiva, actuando como un "juez" que bloqueaba procesos y castigaba los errores de los usuarios. Ese modelo ha fracasado. El líder de seguridad moderno

debe evolucionar hacia un rol de mentor y protector; debe proveer "Inmunidad Cognitiva" a su organización. Esto implica educar y concienciar al capital humano no mediante manuales áridos que se quedan guardados en una carpeta para cumplir con una formalidad burocrática, sino transformando la conducta diaria del empleado.

El riesgo cero no existe, y la incertidumbre es una constante con la que debemos aprender a convivir. Por lo tanto, el legado más valioso que un especialista puede dejar en su organización es una cultura de resiliencia orgánica. Así como un padre prepara a sus hijos para tomar decisiones correctas en un mundo lleno de riesgos inherentes, el líder de seguridad debe capacitar a sus colaboradores para que dejen de ser considerados de forma pasiva como "el eslabón más débil de la cadena" y se conviertan en la primera línea de defensa activa: la barrera humana que detecta, reporta y neutraliza una anomalía antes de que afecte los sistemas centrales.

Al mirar hacia las semanas que componen el mes de junio, se identifican tres vectores de ataque y tendencias tecnológicas que dominarán la agenda de los comités de riesgo en Venezuela y la región:

Ataques de ingeniería social con deepfakes de voz y video: La Inteligencia Artificial generativa ha abaratado el costo de clonar identidades. Veremos un aumento en fraudes basados en la suplantación de directivos mediante llamadas de audio generadas sintéticamente en tiempo real, exigiendo transferencias de fondos urgentes o la liberación de credenciales críticas. La seguridad ya no es solo técnica; es cognitiva. Debemos implementar canales de verificación de doble factor fuera de banda para cualquier instrucción operativa crítica.

La Fragilidad de la Cadena de Suministro Digital: El acceso de terceros a la infraestructura interna representa una de las mayores vulnerabilidades actuales. Los atacantes no buscan derribar la puerta principal de la corporación; buscan las credenciales del proveedor de servicios externos, de climatización o del sistema de gestión logística para infiltrarse lateralmente. La auditoría continua de los niveles de privilegio y el aislamiento de redes (*Network Segmentation*) son imperativos.

La Convergencia entre Seguridad Física, Electrónica y Digital: El mantenimiento y sincronismo de los sistemas críticos de energía (*como ATS y grupos electrógenos*) y los Centros de Control (*CECOM*) ya no pueden gestionarse de forma aislada a la ciberseguridad.

Garantizar la soberanía operativa de nuestras industrias y comercios en este entorno tan cambiante exige una actualización gerencial y un cambio definitivo de paradigma. No podemos seguir comprando soluciones tecnológicas desarticuladas creyendo que el software resolverá las debilidades de la cultura organizacional.

Un Centro de Control de videovigilancia o un sistema de control de acceso físico que esté conectado a la red de datos es un objetivo digital directo. Si los atacantes logran cegar los ojos electrónicos de la empresa o comprometer su soporte vital energético, la seguridad de los activos tangibles e intangibles se desmorona simultáneamente.

La verdadera inmunidad digital se alcanza cuando fusionamos la genialidad táctica de Carabobo — coordinación, agilidad y adaptabilidad ante entornos saturados de incertidumbre— con la visión responsable y formativa del Día del Padre, enfocada en sembrar resiliencia en el factor humano. La batalla por la seguridad de la información en este mes de junio no se ganará esperando pasivamente detrás de una muralla digital; se ganará saliendo al frente, educando con el ejemplo, integrando la tecnología de infraestructura con la ciberseguridad y liderando con una estrategia que convierta la complejidad del entorno en nuestra mayor ventaja competitiva. El futuro de nuestras organizaciones depende de la firmeza con la que diseñemos hoy nuestras defensas.

Adolfo M. Gelder

Especialista en Ciberseguridad y Editor de Seguridad en Acción Venezuela

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

APRENDOYA

APRENDIZAJE SIN LÍMITES Y FRONTERAS

CURSO ESPECIALIZADO

INTELIGENCIA ARTIFICIAL

APLICA A LA

SEGURIDAD PÚBLICA Y PRIVADA

IDENTIFICACIÓN DE AMENAZAS
Detecta, anticipa y previene.

ANÁLISIS Y EVALUACIÓN DE RIESGOS
Evalúa escenarios, reduce vulnerabilidades y toma mejores decisiones

Inscripciones ABIERTAS

Fecha de inicio: 25 de julio

RESERVA TU CUPO AHORA

TRANSFORMA INFORMACIÓN EN INTELIGENCIA.
PROTEGE LO QUE MÁS TE IMPORTA.

ESCANEA Y OBTÉN MÁS INFORMACIÓN

www.corporacionrojo.com +591 75880349 info@corporacionrojo.com