Venezuela | Octubre de 2026 | Año 1 | Número 4

SEGURIDAD EN ACCIÓN VENEZUELA

FRONTERA CERO
Nuestra Huella en el resguardo internacional

SEGURIDAD ELECTRÓNICA

ALIANZA ETICA EN VENEZUELA
Cuando la seguridad se pacta con confianza, no con horas

TERREMOTOS Y CIBERAMENAZAS:
Del sismo físico al fraude en tiempos de crisis

GESTIÓN DE RIESGOS VS GESTIÓN DE CRISIS
Debido a desastres imprevistos



ALFREDO ATTADIA
Presidente ALAS Internacional Venezuela



ADOLFO M. GELDER

PROLOGO

RESILIENCIA, LIDERAZGO Y FE EN EL FUTURO: LA SEGURIDAD COMO VOCACIÓN REGIONAL

Octubre es un mes de profundos significados en el imaginario y en la historia de nuestra nación. En el calendario venezolano, este mes nos convoca a conmemorar el Día de la Resistencia Indígena, un recordatorio permanente de la tenacidad, el arraigo y la capacidad ancestral de nuestros pueblos para sobreponerse a la adversidad y resguardar su identidad. Asimismo, el espíritu del país se viste de devoción y humanidad al celebrar el día de San José Gregorio Hernández, la figura del "médico de los pobres", cuyo legado encarna la vocación inquebrantable de servicio, la ciencia al servicio del prójimo y la protección de la vida en sus momentos más vulnerables.

Ambas efemérides, aparentemente distintas, convergen en la esencia de lo que significa gestionar el riesgo y la seguridad en los tiempos actuales: fortaleza para resistir ante la crisis y vocación humana para proteger al entorno.

En esta 4.ª edición de Seguridad en Acción, ese espíritu de resiliencia y servicio adquiere una dimensión técnica y estratégica renovada. Nos llena de orgullo presentar la Guía de Resiliencia Sísmica y Respuesta Operativa, una entrega especial diseñada no solo para responder desde la ingeniería estructural y la continuidad de negocios, sino para abordar la dimensión humana, neurobiológica y comunitaria que demanda afrontar un desastre natural.

Esta edición marca además un hito en nuestro compromiso con la inclusión y la transformación gerencial mediante el lanzamiento de nuestra nueva sección permanente: Mujeres en Acción. Este espacio nace para visibilizar y honrar el liderazgo, la visión estratégica y la huella imborrable que las profesionales de la seguridad, la criminología y la gestión corporativa están consolidando en nuestra industria.

La seguridad ya no puede entenderse desde fronteras cerradas. Por ello, celebramos con especial entusiasmo el valioso punto de encuentro que logramos en estas páginas: una alianza del pensamiento donde conviven las reflexiones y análisis de destacados colegas venezolanos con los valiosos aportes de expertos y firmas invitadas de América Latina. Esta integración de visiones latinoamericanas demuestra que, frente a las amenazas dinámicas de nuestra región, la colaboración gremial y el intercambio de conocimientos son la mejor herramienta de prevención.

Acompañados de nuestras secciones habituales, este número es una invitación a la reflexión, al rigor técnico y a la acción. Que la tenacidad histórica de nuestra tierra y el ejemplo de servicio dedicado guíen cada decisión operativa y cada estrategia de resguardo.

¡Bienvenidos a la cuarta edición de Seguridad en Acción!

STAFF



HUMBERTO COPA CANDIA
DIRECTOR GENERAL



LUCIEL RÍOS CAMACHO
COORDINADORA ACADÉMICA Y OPERATIVA



BLANCA EMMA CONDORI
DISEÑADORA Y DIAGRAMADORA GRÁFICA

Seguridad en Acción es una revista especializada en seguridad integral, abordando temas de seguridad corporativa, industrial, electrónica, cibernética y personal. Invitamos a lectores y expertos a compartir conocimientos y experiencias, y ofrecemos a empresas del sector una plataforma para potenciar su visibilidad. ¡Súmate a esta iniciativa y construyamos juntos un entorno más seguro!

CONTENIDO

01 FRONTERA CERO: NUESTRA HUELLA EN EL RESGUARDO INTERNACIONAL
PÁG. 5

02 DEFINIENDO LA SEGURIDAD EN CLAVE FEMENINA
PÁG. 10

03 LA SEGURIDAD NO DEPENDE DE IMPROVISACIÓN
PÁG. 16

04 UNA CONVERSACIÓN SOBRE GOBIERNO, CRITERIO Y CONFIANZA CUANDO LA ORGANIZACIÓN ENTRA EN CRISIS
PÁG. 20

05 SEGURIDAD ELECTRÓNICA
PÁG. 25

06 LA ALIANZA ÉTICA EN VENEZUELA: CUANDO LA SEGURIDAD SE PACTA CON CONFIANZA, NO CON HORAS
PÁG.31

07 CUANDO LA TIERRA TIEMBLA EN CASA Y EL CORAZÓN LO HACE EN EL EXILIO UNA MIRADA MÉDICA AL IMPACTO PSICOLÓGICO DE UN TERREMOTO EN EL VENEZOLANO QUE VIVE LEJOS DE SU PAÍS.
PÁG. 37

08 TERREMOTOS Y CIBERAMENAZAS: DEL SISMO FÍSICO AL FRAUDE DIGITAL EN TIEMPOS DE CRISIS
PÁG. 42

09 GESTIÓN DE RIESGOS VS. GESTIÓN DE CRISIS DEBIDO A DESASTRES IMPREVISTOS: CASOS REALES QUE DEMUESTRAN LA IMPROVISACIÓN EN AMÉRICA LATINA.
PÁG. 45

10 LA EVOLUCIÓN DE LA PROTECCIÓN COMO DISCIPLINA PROFESIONAL EN VENEZUELA: UN ANÁLISIS CRÍTICO DEL CONTEXTO VENEZOLANO
PÁG. 50

11 RIESGOS INVISIBLES DESPUÉS DEL TERREMOTO EN VENEZUELA
PÁG. 53

12 LAS ARMAS VUELVEN A LA SEGURIDAD PRIVADA EN VENEZUELA
PÁG. 57

13 LÍDERES DE PENSAMIENTO
PÁG. 60

14 GUÍA DE RESILIENCIA SÍSMICA Y RESPUESTA OPERATIVA DE LA MITIGACIÓN DEL RIESGO A LA CONTINUIDAD DEL NEGOCIO Y LA PROTECCIÓN HUMANA
PÁG. 63

15 GPS TRANQUILIDAD SATELITAL
PÁG. 70

16 EL ESCAPE DEL ENTORNO AISLADO: EL INCIDENTE DE INTELIGENCIA ARTIFICIAL AUTÓNOMO ENTRE OPENAI Y HUGGING FACE
PÁG. 73

17 UN HACKER PACEÑO
PÁG. 77

18 ¿Y SI EL PROBLEMA NO ES LA SEGURIDAD?
PÁG. 81

19 SEGURIDAD INTEGRAL EN RETAIL 2026–2030
PÁG. 88

20 POR QUÉ PIERDE CONTRATOS QUE DEBERÍA GANAR
PÁG. 94

21 CIBERRESILIENCIA EN Q4 DE LA RESISTENCIA ANCESTRAL A LA INMUNIDAD DIGITAL INTEGRAL
PÁG. 97









FRONTERA CERO

NUESTRA HUELLA

EN EL RESGUARDO INTERNACIONAL

ENTREVISTA

ESTEBAN BALTHAZAR



SOBRE EL AUTOR

Destacado poligrafista profesional, consultor en evaluación de la credibilidad y especialista en análisis conductual aplicado a la seguridad corporativa e internacional. Formado en estándares internacionales de poligrafía y evaluación psicofisiológica.

1. Esteban, en la Poligrafía moderna, ¿hasta qué punto el análisis de microexpresiones e intuición del evaluador sigue siendo insustituible frente a la irrupción de la inteligencia artificial y el análisis biométrico?

La pregunta es muy interesante y pertinente, pero permíteme retroceder un poco en el tiempo, antes de abordar la era moderna. A lo largo de la Historia nos percatamos que la detección de quien miente y quien dice la verdad ha preocupado al ser humano. Ya los Hindúes, en el 900 A.C., escribieron los "Papiros Vedas", documento que contien una serie de conductas / gestos / expresiones, que según ellos, develaban al mentiroso. En los últimos 120 años, la búsqueda de la detección del engaño a tenido sucesivos y vertiginosos progresos gracias a la Wilhelm Wundt, Padre de la Psicología Científica, y creador de la Psicofisiología, que estudia la relación entre los estímulos psicológicos y las respuestas fisiológicas para entender las relaciones entre procesos mentales y corporales.

A principios del siglo pasado hubo varios científicos que estudiaron las reacciones fisiológicas vinculadas a la posible intención de engaño, entre ellos Martson, y Keeler, pero fue John Larson quien creó, en la Universidad de California, en Berkeley, el primer aparato que registraba simultáneamente el pulso, la presión arterial y la respiración. Hoy día se registra la respuesta electrodérmica ***(sudoración)***, la variación de la tensión sanguínea, y el movimiento de la caja toráxica, a niveles alto y bajo. Adicionalmente se utilizan otros sensores para detectar los posibles intentos del examinado para

crear artificiosamente reacciones fisiológicas ante algunas preguntas en particular, con el objeto de confundir al examinador.

También es importante resaltar que la American Polygraph Association ***(APA)*** editó en el 2011, un trabajo realizado durante varios años de estudio, denominado ***Estudio Meta Analítico del Criterio de Exactitud de las Técnicas Poligráficas Validadas***. En este estudio se detallan, entre otros parámetros, las probabilidades de detectar engaño en diversas técnicas poligráficas. Durante la entrevista / interrogatorio, el examinador ya debe decidir que técnica va a utilizar y las preguntas relevantes del examen. Por todas estas razones podemos decir que es insustituible.

2. La infiltración y la deslealtad son dos de las mayores amenazas corporativas. ¿Cómo se utiliza hoy la prueba poligráfica como un filtro preventivo efectivo en el reclutamiento de personal crítico sin romper la cultura de confianza en la empresa?

Hay que distinguir entre estas dos situaciones; infiltración y deslealtad. En la primera, el sujeto es un aspirante a ingresar en la empresa. El segundo caso, el desleal ya trabaja en la misma.

Partiendo que la prueba poligráfica debe ser consensual, en ambos casos, el aspirante debe dar su consentimiento escrito a someterse al examen, bien para su eventual ingreso, como tambien, para evaluaciones regulares una vez contratado. Si bien el empleado ya contratado, puede en el futuro negar su consentimiento a ser nuevamente examinado, el mismo hecho ya daría a la Gerencia un indicio de que algo oculta ***(quien no la debe, no la teme!)***. En México, la Procuraduría General de la República, por Ley, podía examinar a los funcionarios públicos una vez al año. Su negativa daba inicio a su desincorporación como funcionario o reubicación a otro puesto de menor riesgo de seguridad. Por esto es tan interesante cumplir con estas exigencias dentro de las organizaciones.

3. Residiendo en Hungría y conociendo bien la realidad venezolana, ¿cuáles son las principales diferencias en la percepción de la amenaza? ¿Qué lección de la seguridad hipervigilante latinoamericana le sirve a Europa y qué criterio europeo debería aplicarse en nuestra región?



En cuanto a Europa, el conflicto Ruso-Ucraniano crea un ambiente de tensión y permanente rastreo de drones o misiles que han impactado, por ejemplo en Polonia y Rumania, e inclusive volado en dirección hacia el Reino Unido. La OTAN está en permanente alerta y monitoreo de esa guerra, en la cual participa indirectamente suministrando armas y municiones a Ucrania, amén de las sanciones financieras a Rusia. Por otra parte, la amenaza de Trump de retirar tropas estadounidenses del territorio europeo y el poco interés que ha demostrado la OTAN de gastar en Defensa, basándose casi exclusivamente en el apoyo norteamericano, lo convierte en más vulnerable ante un eventual ataque directo ruso. Frente esa realidad, ahora los paises de la OTAN han aumentado su presupuesto de defensa, pero pasarán años antes de estar realmente preparados a esa posible confrontación.

Hungría, bajo la gestión de Primer Ministro Orban, ha tratado de mantenerse neutral en ese conflicto, y abogando por el cese de la guerra. Esperemos que se mantenga esa postura ahora con el nuevo gobierno del PM Magyar. Para el hombre de a pié, las calles y los hogares están tranquilos, realmente Budapest es una ciudad segura con un bajísimo indice delictivo. Por su parte las empresas y especialmente las transnacionales invierten más en la protección contra los ataques cibernéticos, que, a los físicos, estafas o sabotajes, que son muy escasos, por no decir nulos.

4. En un mercado donde muchas organizaciones compran seguridad de escaparate, desde la perspectiva de Frontera Cero, ¿cuál es la mentira más grande que vende hoy la industria de la seguridad y que nadie se atreve a admitir?



La seguridad de escaparate consiste en la creación e implementación de una serie de protocolos y mecanismos, que en teoría, deben ser suficientes para evitar que ocurra una evento disruptivo, un incidente. Eso conlleva a trabajar y hacer todo el esfuerzo en seguridad para evitar que ocurra ese evento disruptivo; se implementan más controles, auditorias y por un buen tiempo, probablemente se logre que no ocurra ningún incidente, el personal se siente cómodo y seguro en la empresa. Todo está bien planificado, documentado, y probado... y ahí viene la mentira más grande...

"En mi empresa estamos preparados para evitar que ocurra algún incidente relevante o de gravedad." Esta creo que es la mentira más grande, ya que siempre existe la probabilidad de que fallen eslabones en la cadena de reación ante una contingencia y se produzcan daños severos, no previstos, y de difícil solución. Ahí es cuando se medirá la capacidad de reacción y resilencia de la organización.

5. Cuando todo falla y el protocolo se rompe en el terreno o en una crisis operativa, ¿qué cualidad psicológica o técnica separa al profesional que logra reaccionar y sobrevivir del que se paraliza?

La diferencia la marcará el responsable de seguridad que pueda seguir los siguientes pasos:

- El primer paso es realizar / darse cuenta, que el protocolo previsto para actuar en este tipo de incidente, ha fracasado, ya no opera, y hay que improvisar un plan B urgentemente.

- Analizar lo ocurrido en el desastre, y en base a la información disponible, priorizar las respuestas al incidente, tomando en cuenta la urgencia/ gravedad de los mismos.

- Tratar de mantener y transmitir la calma en todas las instancias, no dejarse llevar por el estrés, y recuperar la comunicación con las distintas estructuras de la organización, impartir las nuevas instrucciones en forma ordenada y coherente.

EDITOR

ADOLFO M. GELDER



¿Sabes dónde están TUS GUARDIAS?





ROJO TRACK
UBICA - VIGILA - PROTEGE



TRANSFORMAMOS GUARDIAS EN OPERACIONES CONTROLADAS

Cobertura Internacional

Tecnología aplicada a operaciones de seguridad en Latinoamérica y el mundo

- BOLIVIA
- PERÚ
- PARAGUAY
- CHILE
- Y MAS

Monitoreo GPS EN TIEMPO REAL
Ubicación exacta de cada guardia.

CONTROL DE RONDAS Y PUNTOS DE MARCACIÓN
Verificación de recorrido con QR o NFC.

COBERTURA NACIONAL E INTERNACIONAL
Operaciones seguras sin fronteras

ALERTAS INMEDIATAS Y REPORTES AUTOMÁTICOS
Notificaciones en tiempo real ante cualquier incidente.

SUPERVISIÓN DESDE CENTRO DE CONTROL
Información en vivo para decisiones efectivas.

ROJO TRACK
Auspiciador oficial de

SEGURIDAD EN ACCIÓN
Revista Internacional

CONTACTO: +591 - 75880349 | www.rojotrackservicios.com | info@corporacionrojo.com



ENTREVISTA

Dra. H.C. MERCEDES ESCUDERO CARMONA

SOBRE EL AUTOR

Presidente del Capítulo México de la International CPTED Association (ICA) · Directora en el ICA Global Executive Board · Presidente del Capítulo 311 de ASIS International · Directora General e Investigadora del Centro de Estudios en Seguridad Ciudadana y Humana, S.C. (CESCH).

REDEFINIENDO LA SEGURIDAD *en clave femenina*

1. Desde la criminología aplicada, tradicionalmente dominada por enfoques reactivos, ¿cómo aporta la mirada femenina a la construcción de diagnósticos de riesgo más humanos, analíticos y enfocados en la prevención real del delito en nuestras ciudades?

Empiezo por precisar un punto técnico: la mirada femenina no es un adjetivo sensible que se le agrega al diagnóstico; es una variable de análisis que modifica el resultado. Un enfoque reactivo cuenta cuerpos, carpetas de investigación y eventos consumados. La prevención, en cambio, cuenta oportunidades: mide las condiciones del entorno construido y del tejido social que hicieron posible que ese delito ocurriera ahí, a esa hora y contra esa persona.

La Norma ISO 22341:2021 define a la Metodología Crime Prevention Through Environmental Design, o Prevención del Delito a través del Diseño Ambiental (CPTED por sus siglas en inglés) como el proceso

para analizar y evaluar los riesgos de delincuencia y seguridad, con el fin de orientar el desarrollo, el diseño urbano, la gestión del sitio y el uso del medio ambiente construido para prevenir y reducir la delincuencia y el miedo a la delincuencia, y para promover la salud pública, la calidad de vida y la sostenibilidad. Ese último tramo de la definición —el miedo y la calidad de vida— es la puerta por donde entra, con rigor normativo y no como concesión, la perspectiva de género.

2. Ha liderado comisiones e iniciativas de seguridad en cúpulas empresariales e instituciones de alto nivel. ¿Cuáles han sido los mayores desafíos y ventajas de ejercer un liderazgo femenino en mesas de decisión históricamente masculinas dentro del sector corporativo latinoamericano?

Le respondo con franqueza y sin victimización, porque no me parece útil ninguna de las dos cosas. Siempre digo:

"BIENVENIDOS AL MUNDO DE LAS PERSONAS, YA QUE LOS HOMBRES Y MUJERES ESTAMOS UNIDOS POR NUESTRA DIFERENCIAS PARA DISEÑAR Y CONTRUIR SEGURIDAD".



Los Desafíos

- **La doble acreditación.** Durante algunos años si importaba el solo hecho der ser mujer. Hoy debemos validar de otra manera. La técnica de una mujer en el sector de la seguridad se valida dos veces: primero la persona y después el argumento. La respuesta que me ha funcionado no es alzar la voz, es alzar el estándar: llegar a la mesa con marco normativo, con evidencia y con trazabilidad. Cuando sustentamos con argumentos y evidencia científica la discusión deja de ser sobre quién habla y pasa a ser sobre qué se propone.

- **La prevención vista como gasto en lugar de inversión.** En muchas mesas la seguridad todavía se traduce en hardware: cámaras, bardas, guardias. Explicar que un diagnóstico CPTED reduce el costo de operación, la rotación, el ausentismo y la prima de riesgo exige hablar el idioma financiero, no sólo el social.

Las ventajas:

- **Capacidad de convocatoria.** Las intervenciones serias exigen articular a gobierno, iniciativa privada, academia y comunidad. Esa gestión de partes interesadas —que ISO 22341 e ISO 18091 exigen formalmente— demanda escucha, paciencia y construcción de confianza. Es un terreno donde el liderazgo femenino suele tener ventaja comparativa real.

- **Visión de largo plazo.** La prevención no da resultados en un trimestre. Sostener un proceso de seis fases —planeación, diagnóstico, diseño, implementación, gestión y evaluación— requiere una tolerancia al proceso que no siempre convive con la lógica del resultado inmediato.

3. Usted impulsa con fuerza la participación ciudadana y la inteligencia social. ¿Qué rol clave juegan hoy las mujeres en la articulación de redes de prevención vecinal y en la reconstrucción del tejido social frente a la delincuencia?

Un rol determinante, y lo digo desde la evidencia de campo: cuando una intervención socio-urbana se sostiene en el tiempo, casi siempre hay mujeres sosteniéndola. Son ellas quienes conocen a los vecinos, quienes identifican al niño que dejó de ir a la escuela, quienes detectan el cambio de patrón en las calles, en el barrio y en la ciudad. Esto se da porque culturamente la mujer es a la que se le asiga la educación de los hijos y familia; además de la comunidad de su entorno.

Por eso insisto en la coproducción de la seguridad de la mano ciudadana y comunitaria. No es tarea exclusiva de las policías ni de las fuerzas armadas; todos somos corresponsables de diseñar y proveer seguridad. Para ordenar esa corresponsabilidad utilizo las 5 "D" de la Prevención:

5 "D" DE LA PREVENCIÓN



1. **Detectar el factor de riesgo antes de que se convierta en incidente.**
2. **Documentar con evidencia, no con rumor.**
3. **Difundir la información verificada dentro de la red vecinal.**
4. **Denunciar por el canal institucional correspondiente.**
5. **Disuadir mediante el diseño, la apropiación del espacio y la presencia comunitaria.**

4. En el terreno de la ciberseguridad, donde la ingeniería social y el fraude explotan la vulnerabilidad del usuario, ¿cómo se aplica la criminología y la concientización con perspectiva de género para proteger a familias y organizaciones de las nuevas amenazas digitales?

Parto de una convicción: el entorno digital es un espacio, y como todo espacio puede diseñarse de forma segura o insegura. Por eso, algunos especialistas de CPTED hemos empezado a proponer bases para evolucionar hacia una cuarta generación de CPTED, de carácter socio-digital, donde los principios clásicos se transponen al ecosistema digital:

- **Vigilancia natural:** visibilidad y trazabilidad de lo que ocurre en nuestros entornos digitales; monitoreo, registros y alertas comprensibles para el usuario. Además de que hay herramientas para hacer monitoreo y registro de nuestros territorios de forma digital.

- **Control de acceso:** gestión de identidades, autenticación multifactor, principio de mínimo privilegio.

- **Refuerzo territorial:** soberanía sobre el dato propio. Los ciudadanos debemos ser productores y gestores de nuestro propio rastro humano y digital.

Permítame detenerme aquí, porque es la pregunta que más me interesa y la que menos se hace. La IAH® no es una postura tecnófoba ni una nostalgia artesanal: es un marco ético de gobernanza del criterio. Nace de una premisa que sostenemos el Dr. H.C. Octavio Contreras y yo: la innovación no es meramente tecnológica, sino profundamente humana. El algoritmo no debe ser el guía, sino el pincel manejado por la sabiduría del artesano social. De ahí se desprenden principios de los cuales hare mención a algunos que aplicamos en todo entregable del Sistema de Gestión de Riesgos Socio-Urbanos (SGRSU):

- **Primacía del juicio humano.** La decisión que afecta la vida, la libertad o el patrimonio de una persona no se delega a un modelo. La supervisión humana debe ser significativa, no ceremonial: quien firma debe poder explicar por qué.

- **Honestidad normativa.** En cada dictamen distinguimos de manera expresa lo que constituye obligación legal vinculante de lo que es estándar internacional aplicado por analogía o buena práctica de referencia. Confundirlos deliberadamente para vender un servicio es una falta ética, no un matiz técnico.

- **Trazabilidad y explicabilidad.** Todo hallazgo debe poder rastrearse hasta su fuente, su método y su fecha. Un diagnóstico que no se puede auditar no es un diagnóstico: es una opinión con formato profesional.



5. Para cerrar y haciendo honor al lema de nuestra sección: ¿Qué significa hoy "redefinir la seguridad en clave femenina" en América Latina y cuál es su mensaje para la nueva generación de mujeres que aspiran a dirigir la seguridad pública y privada en la región?

Durante décadas la seguridad se midió por la ausencia de delito. En clave femenina se mide por algo más exigente: por la posibilidad real de habitar. Una ciudad no es segura porque bajó una estadística; es segura cuando una mujer puede volver caminando de noche, cuando una niña puede jugar en la calle, cuando una adulta mayor puede ir sola al mercado, cuando una trabajadora no calcula la ruta en función del miedo. Eso es seguridad humana, y es un estándar más alto, no más blando.

En América Latina esto tiene una urgencia particular: enfrentamos desigualdad, urbanización acelerada, brechas digitales y una crisis de confianza institucional. No existe una receta única. Cada territorio exige respuestas específicas a su contexto, orientadas a revertir factores de riesgo, restablecer la gobernanza legítima, reducir la desigualdad y promover la resiliencia individual y comunitaria.

MI MENSAJE A LA NUEVA GENERACIÓN

- **Formarse con rigor técnico.**
  La vocación es indispensable, pero no sustituye al método. Aprendan normas, análisis de riesgos, estadística, presupuesto y marco jurídico. En esta industria, el conocimiento verificable es la forma más rápida de ganar autoridad.

- **Practiquen la honestidad normativa.**
  Distingan siempre lo que es obligación legal vinculante de lo que es estándar de referencia aplicado por analogía. Quien confunde deliberadamente ambas cosas para vender un servicio, daña a su cliente y a la profesión.

- **No acepten entrar como cuota.**
  Las mejores debemos entrar como autoridad técnica. Y una vez adentro, abrir la puerta: la que llega sola y cierra detrás de sí no transformó nada. Hay que ser sororas y trabajr de forma colaborativa.



NUESTRA MISIÓN ES IR MÁS ALLÁ DE LA OBRA FÍSICA: construir territorios de paz, ciudades sanas, seguras, productivas, incluyentes y sostenibles. Porque de eso se trata de vivir y convivir, no solamente de sobrevivir.

EDITOR

ADOLFO M. GELDER



CORINPROINCA

Su protección, nuestra profesión

41 Años

EVOLUCIONANDO PARA PROTEGER MEJOR

Permanecer fue un logro
Evolucionar ha sido una decisión
Trascender es el siguiente paso

Integramos experiencia, inteligencia y tecnología para anticiparnos al riesgo y proteger lo que impulsa tu crecimiento: **tu gente, tus operaciones y tus activos.**

NUESTRAS CAPACIDADES

PROTECCIÓN FÍSICA Y EJECUTIVA

Presencia, Criterio y Control

INTELIGENCIA Y VERIFICACIÓN

Conocer el riesgo antes de que impacte

TECNOLOGÍA E IoT

Tecnología aplicada a la prevención y gestión de la seguridad

PROTECTER

METODOLOGÍA QUE TRANSFORMA LA SEGURIDAD

Prevenir ▶ Analizar ▶ Supervisar ▶ Comunicar ▶ Responder ▶ Mejorar

- **TRANSFORMACIÓN DIGITAL**
- **INTEGRACIÓN INTELIGENTE**
- **INFORMACIÓN PARA DECIDIR**

TRANSFORMACIÓN DIGITAL QUE GENERA

VISIBILIDAD - TRAZABILIDAD - CONTROL

Corinproinca.com Corinproinca +0412-239-0004 Central: 0212-771-9088 / 720-3991

LA SEGURIDAD NO DEPENDE DE IMPROVISACIÓN

ENTREVISTA

ALEJANDRA FRANCO

SOBRE EL AUTOR

Destacada ejecutiva y líder empresarial en el sector de la seguridad privada en Venezuela. Como Gerente General de CORINPROINCA, encabeza una de las organizaciones referentes en servicios de resguardo, vigilancia corporativa y protección patrimonial, destacándose por promover una gestión estratégica caracterizada por la innovación operativa y un alto estándar de calidad de servicio.

1. Alejandra, desde la Gerencia General de CORINPROINCA, ¿cómo se diseña y mantiene una estructura de procesos eficiente que garantice que la logística, el despliegue de personal y el control de calidad funcionen de manera óptima en cada instalación protegida?

En CORINPROINCA partimos de un principio muy claro: **la seguridad no puede depender de la improvisación; tiene que depender de procesos.**

Por eso nuestra estructura operacional está diseñada para que cada servicio tenga planificación, responsables definidos, supervisión y trazabilidad. Antes de desplegar personal analizamos las características de la instalación, sus riesgos, horarios, puntos críticos, requerimientos del cliente y recursos necesarios. A partir de allí estructuramos puestos, consignas, recorridos, protocolos de actuación y mecanismos de supervisión.

A esto incorporamos tecnología mediante nuestra plataforma **Protecter**, que nos permite obtener mayor visibilidad de la operación, registrar actividades, generar evidencias y disponer de información que facilite la toma de decisiones.



2. La alta dirección en empresas de vigilancia y resguardo tradicionalmente ha estado liderada por hombres. Desde su rol ejecutivo, ¿cómo aporta la visión gerencial femenina a la resolución de conflictos, la negociación corporativa y la construcción de una cultura organizacional más sólida e inclusiva?

Considero que el liderazgo no debería definirse por género, **sino por capacidad, preparación, criterio y resultados**. Sin embargo, también creo que incorporar diferentes perspectivas en la alta dirección enriquece considerablemente la forma en que una organización toma decisiones.

Desde mi experiencia, la visión femenina puede aportar una sensibilidad particular hacia la comunicación, la escucha y la construcción de consensos, sin que eso signifique renunciar a la firmeza que requiere dirigir una empresa de seguridad.

En nuestra actividad enfrentamos permanentemente situaciones que exigen negociar, resolver conflictos y tomar decisiones bajo presión. Mi enfoque consiste en escuchar primero, analizar los hechos y posteriormente decidir con claridad. **Empatía y firmeza no son conceptos opuestos; un buen gerente debe saber utilizar ambos.**

3. En la administración moderna de una empresa de seguridad, la gestión de datos de clientes, la nómina en la nube y las comunicaciones de campo están interconectadas. ¿Cómo integran la ciberseguridad dentro de los procesos administrativos y operativos de CORINPROINCA para blindar la información confidencial de la empresa y de sus contratantes?

Hoy sería un error pensar que una empresa de seguridad solamente protege instalaciones físicas. **También tenemos la responsabilidad de proteger información.**

La transformación digital ha conectado la administración, las operaciones de campo, la supervisión y la información de nuestros clientes. Por eso en CORINPROINCA entendemos la ciberseguridad como parte integral de la operación y no exclusivamente como una responsabilidad del departamento de tecnología.

Nuestro modelo busca que la información sea administrada bajo criterios de **control de acceso, trazabilidad, disponibilidad, respaldo y confidencialidad**, estableciendo responsabilidades según las funciones que desempeña cada persona dentro de la organización.

Protecter forma parte de esta evolución tecnológica, permitiéndonos digitalizar y centralizar información operacional que anteriormente dependía de procesos manuales y registros dispersos. Esto proporciona mayor trazabilidad y capacidad de control.

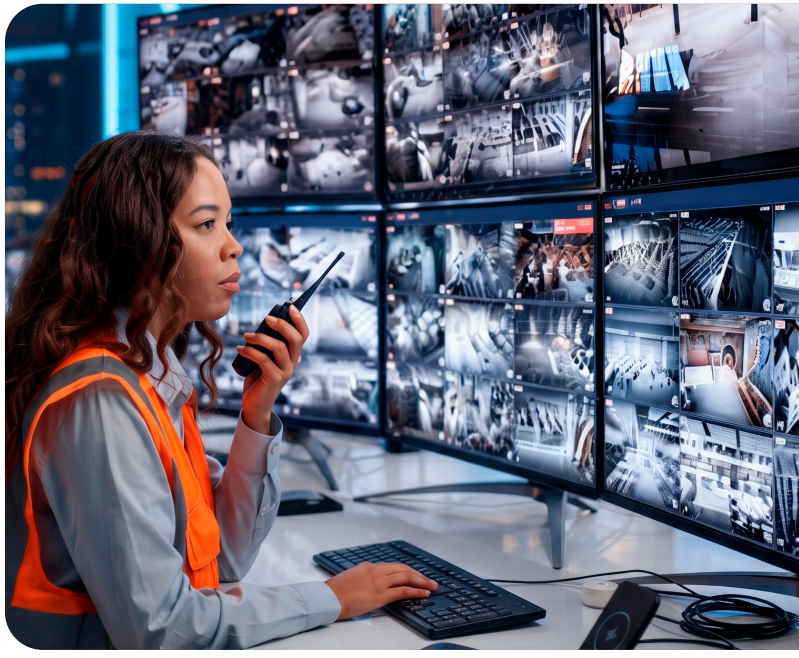
4. A raíz de los eventos sísmicos registrados recientemente en Venezuela, la actuación de la seguridad privada resultó crucial en los primeros minutos de emergencia. ¿Cómo respondió CORINPROINCA en el terreno durante esta contingencia y qué lecciones operativas y de evacuación han incorporado a sus protocolos para fortalecer la resiliencia en los clientes que protegen?

Los eventos sísmicos recientes nos recuerdan algo fundamental: **el agente de seguridad suele ser una de las primeras personas disponibles cuando ocurre una emergencia en una instalación**. Por eso su responsabilidad va mucho más allá del control de accesos.

Este tipo de acontecimientos nos obliga a revisar permanentemente los protocolos de emergencia de cada servicio, especialmente las rutas de evacuación, puntos de encuentro, mecanismos de comunicación, identificación de personas vulnerables y coordinación entre el personal de seguridad y los responsables de emergencia del cliente.

Una de las principales lecciones es que durante una contingencia los primeros minutos son determinantes. El personal necesita saber qué hacer sin depender de instrucciones improvisadas. Para lograrlo hacen falta procedimientos sencillos, entrenamiento y ejercicios periódicos.





También es importante entender que cada instalación tiene condiciones diferentes. No puede aplicarse exactamente el mismo protocolo a una torre empresarial, una planta industrial, una residencia o una instalación diplomática.

5. Con la constante evolución de las amenazas y las exigencias del mercado corporativo, ¿cuál considera que es el principal desafío que enfrentarán los gerentes generales de seguridad privada en los próximos cinco años para equilibrar la rentabilidad del negocio con la excelencia operativa?

El principal desafío será **transformar el modelo tradicional de seguridad privada sin destruir la sostenibilidad económica del servicio.**

Durante muchos años nuestra industria estuvo concentrada principalmente en colocar personal en puestos de vigilancia. Ese modelo está evolucionando. Los clientes esperan ahora prevención, tecnología, indicadores, trazabilidad, análisis de riesgos, capacidad de respuesta y resultados medibles.

Al mismo tiempo tenemos una responsabilidad que no podemos ignorar: la seguridad continúa dependiendo en gran medida del factor humano. Pretender reducir permanentemente los precios mientras aumentan las exigencias termina afectando salarios, capacitación, supervisión y, finalmente, la calidad del servicio.

El reto de los gerentes generales será demostrar que **seguridad no es solamente un costo: es una inversión en continuidad del negocio y gestión del riesgo.**

EDITOR

ADOLFO M. GELDER



FERIA
DIGITAL
ALAS

Cierre del año tecnológico

CON PRESENTACIONES TECNOLÓGICAS DE:

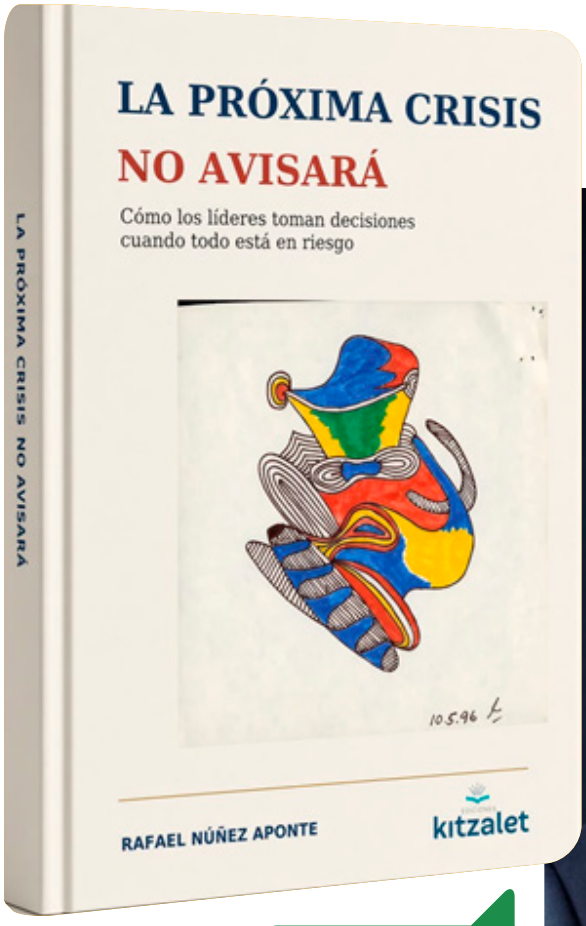
AJAX
ALARM.COM
ALCEA ASSA ABLOY
Altronix
AXIS COMMUNICATIONS
BOLIDE TECHNOLOGY GROUP
CAME
dahua TECHNOLOGY
GARNET TECHNOLOGY
Genetec
gigas CLOUD
HID
IDIS
One Solution. One Company.
MOTOROLA SOLUTIONS
OpenEye
rhombus
resideo
SoftGuard
Verkada
ZKTeco

14-15 OCTUBRE

8:00 - CDMX / 9:00 - Btá, Lima / 10:Miami / 11:00 - B.Aires

UNA CONVERSACIÓN SOBRE GOBIERNO, CRITERIO Y CONFIANZA

CUANDO LA ORGANIZACIÓN ENTRA EN CRISIS





ENTREVISTA

RAFAEL NÚÑEZ APONTE

1. En el primer movimiento del libro afirmas que un tablero con todos los indicadores en verde no significa estar preparado y que el problema real no es un clic por error, sino que ese clic tenga el poder de detener una empresa. ¿Cómo puede un CEO o una junta directiva romper la falsa sensación de control de sus departamentos de TI y auditores para medir el verdadero criterio de respuesta del equipo humano antes de que ocurra el desastre?

No se rompe esa falsa sensación peleando con TI ni despreciando una auditoría. Se rompe cambiando lo que la junta exige. Un tablero verde puede demostrar que una herramienta funciona o que un control cumple; no demuestra que la empresa sabrá decidir con información incompleta. La primera pregunta debería ser: si hoy perdemos identidad digital, pagos, correo o acceso a los datos, ¿qué parte del negocio sigue viva, quién decide y durante cuánto tiempo podemos sostenerla?

Luego hay que producir evidencia, no más presentaciones. Yo escogería un proceso crítico y sometería al equipo a un ejercicio controlado, interfuncional y sin respuestas ensayadas: el CEO no está disponible, un proveedor no responde, aparece un clic equivocado y el respaldo aún no ha sido validado. Allí se mide cuánto tarda la organización en declarar la crisis, quién tiene autoridad, cómo separa hechos de hipótesis, qué servicio mínimo puede mantener y si registra las decisiones. Eso revela criterio humano mucho mejor que contar alertas atendidas.

Finalmente, hay que rediseñar el proceso para que un error normal no produzca un daño extraordinario. Verificación por otro canal, doble aprobación, privilegios limitados, alternativas manuales y restauraciones probadas. La junta no debería conformarse con saber cuántos controles existen; debería pedir qué proceso fue recuperado, qué dependencia se redujo y qué decisión todavía no tiene dueño. Un tablero verde mide controles; una crisis mide criterio.

2. Propones un protocolo estricto para gobernar las primeras dos horas de un incidente crítico a través de cuatro carriles: ejecutivo, técnico, legal y comunicacional. En la práctica corporativa de América Latina, donde suele predominar la improvisación o la tentación del silencio, ¿cuál es la decisión más difícil pero indispensable que debe tomar un líder en los primeros 120 minutos para proteger la viabilidad de la empresa?

La decisión más difícil es declarar que la organización entró en modo crisis antes de tener certeza total. No significa alarmar al mercado ni hablar sin verificar. Significa reconocer internamente que ya no se está frente a una falla ordinaria y activar gobierno: quién coordina, qué se protege primero, qué información está confirmada y cuándo será el próximo corte de situación. Muchas organizaciones postergan ese paso para no parecer alarmistas; mientras esperan la explicación perfecta, cada área empieza a improvisar su propia respuesta.

Los cuatro carriles existen precisamente para impedir esa fragmentación. El técnico contiene, preserva evidencia y recupera; el legal identifica obligaciones y límites; el comunicacional ordena audiencias, mensajes y próximas actualizaciones; y el ejecutivo prioriza personas, continuidad, recursos y autoridad. Todos avanzan en paralelo, con una sola versión de la realidad y dejando registro de cada decisión.





Apagar, aislar o comunicar públicamente dependerá del caso; recuperar la capacidad de decidir no es opcional. El silencio puede ser prudente durante un tiempo si tiene una razón, una audiencia y una hora de actualización. El silencio sin gobierno se convierte en vacío, y el vacío lo llenan el rumor y la desconfianza. La certeza total casi siempre llega tarde; el gobierno de la crisis tiene que llegar primero.

3. Planteas que la ciberseguridad debe sentarse en la junta directiva y que es vital "proteger a quien trae una mala noticia". ¿De qué manera la cultura punitiva de una organización incrementa el riesgo cibernético y qué pasos concretos debe dar la alta gerencia para transformar a los especialistas en seguridad en aliados estratégicos del negocio y no en un área de contención o culpables del colapso?

Una cultura que castiga la alerta compra silencio, y ese silencio le regala tiempo al atacante. El minuto más importante después de un error es aquel en que la persona decide si lo reporta. Si teme ser humillada, despedida o convertida en ejemplo, puede callar, suavizar lo ocurrido o esperar una certeza que nunca llega a tiempo. La tecnología pierde entonces horas valiosas por un problema cultural.

La alta gerencia debe convertir la protección del reporte de buena fe en una regla visible. Primero se contiene; después se investiga y se determina responsabilidad. Eso no significa impunidad: hay que distinguir entre un error honesto, negligencia repetida, ocultamiento y conducta deliberada. También hace falta una vía para que los riesgos materiales lleguen a la alta dirección o a la junta sin filtros impropios, y que seguridad participe desde el inicio en productos, proveedores, adquisiciones y nuevos negocios.

El especialista se vuelve aliado cuando traduce su hallazgo a una decisión de negocio. No basta con decir que existe una vulnerabilidad crítica; debe explicar qué proceso puede detenerse, cuáles son las opciones, cuánto cuestan, cuánto tardan y qué riesgo queda. La gerencia, a su vez, debe medir tiempo de escalamiento, restauraciones probadas, dependencias reducidas y acciones correctivas cerradas, no solo actividad técnica. Si castigas al mensajero, conviertes cada alerta en un secreto.

4. Una de las sentencias más contundentes del libro señala que "un respaldo que nunca se restauró es una promesa, no una capacidad". Más allá de la auditoría técnica o los certificados ISO, ¿cómo se diseña un simulacro real para la junta directiva que ponga a prueba la continuidad operativa de los procesos de negocio cuando la tecnología simplemente no responde?

Un simulacro real empieza por el proceso de negocio, no por el servidor. Hay que escoger un servicio que sostenga ingresos, atención, liquidez o cumplimiento; definir su versión mínima viable y nombrar a su propietario ejecutivo. Luego se plantea, durante noventa minutos o hasta tres horas, un escenario progresivo: fallas de autenticación, un proveedor que reporta actividad irregular, posible exposición de datos, el CEO incomunicado, un respaldo que falla la primera prueba y un periodista que pide confirmación.

La junta no está allí para dirigir la restauración técnica. Está para declarar la crisis, priorizar qué vuelve primero, decidir qué nivel de operación puede sostenerse manualmente, autorizar medidas con impacto, coordinar obligaciones legales y gobernar la comunicación. El facilitador entrega información por etapas y no resuelve preguntas que en la vida real tampoco tendrían respuesta inmediata. Así se observa la calidad de las preguntas, la claridad de la autoridad y la forma de decidir bajo incertidumbre.

En paralelo, el equipo técnico debe restaurar de verdad en un entorno aislado y el negocio debe validar el proceso de punta a punta. Un servidor encendido no significa que la empresa volvió: hay que poder atender, facturar, pagar, despachar o prestar el servicio con datos íntegros. El tiempo incluye credenciales, autorizaciones, terceros y validación. El ejercicio termina con brechas, responsables, fechas y una nueva prueba. Los estándares ISO aportan disciplina; la capacidad se demuestra ejecutando. Un simulacro que no incomoda es una presentación.

5. Explicas que los sistemas informáticos pueden levantarse en cuestión de horas, pero la confianza perdida del mercado, clientes y accionistas tarda años en recuperarse. Habiendo transitado más de 26 años en el sector y conociendo de cerca el ecosistema latinoamericano, ¿cuál es la diferencia determinante entre las organizaciones cuyo carácter se fortalece tras una crisis y aquellas que terminan desmanteladas reputacionalmente?

La diferencia determinante es la coherencia bajo presión. La crisis no crea el carácter de una organización; lo hace visible. Dos empresas con tecnologías parecidas pueden enfrentar incidentes similares y obtener resultados completamente distintos. Una busca culpables, niega demasiado pronto, comunica tarde y permite versiones contradictorias. La otra reconoce la situación, activa un comité pertinente, registra decisiones, protege la dignidad de quien reporta y corrige cuando los hechos cambian.

La tecnología y la confianza operan con relojes distintos. Un sistema puede recuperarse relativamente rápido, pero clientes, empleados, aliados y accionistas seguirán preguntándose si la organización merece ser creída. La confianza no vuelve por un comunicado aislado. Vuelve cuando se dice con claridad



qué se sabe y qué no, se fija una próxima actualización, se cumplen los compromisos y la reparación confirma el mensaje. El mercado no exige invulnerabilidad; exige gobierno, responsabilidad y humanidad.

Por eso las ilustraciones de mi padre, Rafael Ambrosio Núñez, no son decoración dentro del libro. Introducen memoria y legado en una conversación que podría parecer puramente técnica. Detrás de cada sistema hay personas, familias, clientes y años de trabajo. Eso es lo que realmente se protege. Una crisis termina dos veces: cuando la tecnología vuelve y cuando la organización vuelve a ser creída. La próxima crisis no avisará fue escrita también para esa segunda recuperación.

EDITOR

ADOLFO M. GELDER



SEGURIDAD ELECTRÓNICA





ENTREVISTA

ALFREDO ATTADIA

SOBRE EL AUTOR

Destacado empresario, integrador de tecnología y referente gremial de la industria de la seguridad electrónica en Venezuela. Como CEO de Sistealarmas y presidente del Capítulo Venezuela de la Asociación Latinoamericana de Seguridad *(ALAS)*, lidera el impulso hacia la modernización tecnológica del sector, la estandarización técnica y el fortalecimiento de las redes internacionales de cooperación en el país.

1. Alfredo, al frente de Sistealarmas, has vivido la transformación desde la seguridad electrónica basada en sensores analógicos hasta la era de las ciudades inteligentes y los centros de control integrados. ¿Cómo ha evolucionado la arquitectura de proyectos de Sistealarmas para migrar del simple monitoreo reactivo a la analítica predictiva de alto nivel para el sector corporativo e industrial?

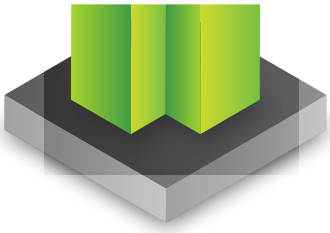
R.- La arquitectura de los proyectos de Sistealarmas ha experimentado una transformación estructural profunda, evolucionando desde un modelo clásico de **monitoreo reactivo** *(basado en la recepción de señales de intrusión locales y el despacho posterior de asistencia)* hacia un ecosistema de **seguridad proactiva y analítica predictiva de alto nivel** optimizado para entornos corporativos, financieros e industriales complejos.

ESTA EVOLUCIÓN SE SUSTENTA SOBRE CUATRO PILARES ARQUITECTÓNICOS CLAVE:

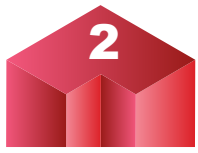
Migracion a Arquitecturas distribuidas e integradas.



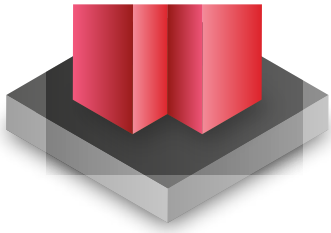
Los proyectos corporativos de Sistealarmas pasaron de depender de paneles analógicos aislados a implementar unidades de control autónomas en el borde conectadas con plataformas en la nube.



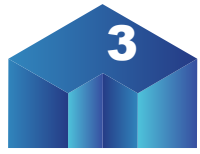
De la simple video verificacion a la videoanalitica con IA.



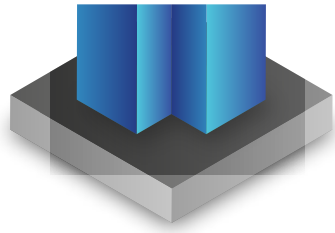
El uso tradicional del circuito cerrado de televisión (CCTV) se limitaba a registrar visualmente un incidente después de que un sensor de movimiento disparaba la alerta. Hoy, el video es un sensor activo e inteligente.



Analitica predictiva de habitos y Operaciones.



En el sector corporativo y logístico, la evolución arquitectónica incorpora el rastreo de activos mediante GPS avanzados combinados con herramientas telemáticas.



2. El regreso formal del capítulo de ALAS Internacional a Venezuela bajo tu presidencia representa un hito institucional para la industria. ¿Qué mensaje estratégico le envía este retorno al mercado nacional e internacional, y cuáles son los objetivos prioritarios que asume para reimpulsar el gremio, elevar los estándares técnicos y reconectar al país con las grandes tendencias globales?

R.- A nivel nacional: Representa el fin del aislamiento gremial, ofreciendo un entorno de respaldo institucional, formalidad y combate a la informalidad técnica en beneficio de empresas, usuarios y especialistas locales.

R.- A nivel internacional: Declara que **Venezuela está lista para la inversión**, la transferencia tecnológica de vanguardia y la adopción de normativas globales en materia de seguridad física y electrónica.



3. Convertirse y mantenerse como un referente tecnológico en Venezuela requiere equilibrar innovación, resiliencia y adaptabilidad. Desde tu posición, ¿qué significa realmente liderar la vanguardia tecnológica en el país hoy en día: se trata de importar la última tecnología o de saber adaptar la ingeniería a las necesidades reales y operativas de nuestra infraestructura?

R.- Liderar la vanguardia tecnológica en Venezuela hoy en día no consiste en importar la última tecnología de forma ciega. El verdadero liderazgo radica en **saber adaptar la ingeniería a las necesidades reales, operativas y críticas de la infraestructura nacional**, construyendo un puente entre la innovación global y la resiliencia local.

Este enfoque esta basado en algunos pilares que nombrare a continuación:

1 La trampa de la importación lineal.

Desconexión del entorno: Traer soluciones de última generación diseñadas para entornos con servicios públicos perfectos (electricidad continua, conectividad simétrica) suele estar destinado al fracaso en el contexto local.

2 La ingeniería de adaptación como ventaja competitiva.

Optimización de recursos: El valor real del ingeniero en Venezuela está en su capacidad para hacer que la tecnología funcione de manera óptima bajo condiciones adversas o fluctuantes.

4. Los sistemas de seguridad electrónica, las alarmas y las cámaras de vigilancia hoy son nodos conectados a la red (IoT). ¿Cómo integra la ciberseguridad tanto en la protección del hardware y los centros de control que instala Sistealarmas, como en las normativas y capacitaciones que promueve desde la presidencia de ALAS Venezuela para evitar que la seguridad física sea la puerta de entrada de un ciberataque?

R.- La integración de la ciberseguridad en la convergencia de la seguridad física y electrónica se aborda bajo una estrategia bidireccional: la ejecución técnica rigurosa en el terreno con empresas establecidas y cuyo compliance sea verificado, y el impulso institucional, normativo y educativo desde **ALAS Venezuela** ***(Asociación Latinoamericana de Seguridad).***



1 En Protección del Hardware y Centros (CRA)

En la implementación de nodos IoT (cámaras de seguridad, sensores y paneles de alarma), las vulnerabilidades del hardware se mitigan mediante protocolos estrictos que evitan que un dispositivo físico sea el eslabón débil de la red institucional o residencial.

- **Bastionado de Dispositivos (Hardening):** Todo hardware instalado pasa por un proceso de cambio obligatorio de credenciales de fábrica por contraseñas robustas y únicas. Se deshabilitan puertos y protocolos innecesarios (como Telnet o HTTP no seguro) para reducir la superficie de ataque.

2 Desde ALAS Venezuela: Normativas y Capacitaciones

Desde la presidencia del capítulo nacional de la Asociación Latinoamericana de Seguridad se promueve la estandarización y profesionalización del sector para concientizar sobre el riesgo de la **"puerta trasera"** cibernética:

- **Promoción de Estándares Internacionales:** Se impulsa la adopción de normativas y buenas prácticas globales (como principios de la ISO 27001 o guías del NIST para IoT) dentro del ecosistema de integradores en Venezuela. Esto incentiva a las empresas de seguridad física a certificar que sus ingenieros y técnicos entiendan la infraestructura IP.

5. Frente a la rápida aceleración tecnológica y la automatización, existe una brecha importante en la formación de nuevos profesionales. Desde la vitrina gremial que representa ALAS y su experiencia empresarial, ¿cuál es tu visión para formar a la nueva generación de ingenieros e integradores de seguridad en Venezuela y garantizar que el sector privado siga siendo un motor de resiliencia para el país?

R.- La visión para formar a la próxima generación de ingenieros e integradores de seguridad en Venezuela, bajo la perspectiva gremial de ALAS (Asociación Latinoamericana de Seguridad) y la experiencia empresarial local, se fundamenta en la **actualización curricular, la alianza academia-empresa y la especialización tecnológica.** En un entorno de rápida automatización, el sector privado no solo debe adoptar tecnología, sino liderar la capacitación del talento para mantener su rol como motor de resiliencia.

PILARES CLAVES PARA LOGRAR ESA TRANSFORMACIÓN:

1 Modernización Curricular y Enfoque Multidisciplinario

El perfil del instalador de alarmas tradicional ha quedado obsoleto. La nueva generación de ingenieros debe dominar un ecosistema interconectado:

Convergencia de tecnologías: Integrar la seguridad electrónica física (cámaras, control de acceso) con la ciberseguridad, la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT).

2 El Ecosistema "Triple Hélice" (Gremio - Academia - Empresa)

Para cerrar la brecha de formación rápidamente, el sector privado debe involucrarse directamente en las aulas:

Pasantías de inmersión temprana: Crear programas donde los estudiantes de ingeniería resuelvan problemas reales de automatización y seguridad en empresas locales desde la mitad de su carrera.

EDITOR

ADOLFO M. GELDER

29 AÑOS

PROTEGIENDO LO QUE MÁS TE IMPORTA

Tecnología, experiencia y compromiso que nos permiten ofrecer soluciones integrales de seguridad electrónica con los más altos estándares de calidad.





CUMPLIMIENTO Y CALIDAD CERTIFICADA

UL827 | UL681 | UL1076 | UL1641 | UL1981 | NFPA72

CASI TRES DÉCADAS DE EXPERIENCIA

Comprometidos con tu seguridad, innovando cada día para que vivas tranquilo.

NUESTROS ALIADOS

0800-ALARMA0

sistealarmas.com

@sistealarmas

Calle Las Flores entre calles 12 y 13, Colinas del Neverí, Barcelona 6001, Anzoátegui - Venezuela.

RIF: J-31049552-1

Resolución CONATEL # HGTS-00450

Sistealarmas

Vive tranquilo

FORMACIÓN ALAS



LA INDUSTRIA DE LA SEGURIDAD EVOLUCIONA. TU CONOCIMIENTO TAMBIÉN.

Actualiza tus conocimientos, fortalece tus habilidades y sigue creciendo con Formación ALAS. Descubre programas especializados para profesionales de la seguridad.

FORMACIÓN OPERATIVA

- Alarmas y Detección de incendios
- Alarmas y Detección de Intrusión
- Control de Acceso
- Fundamentos de Seguridad Electrónica
- Integración de Sistemas de Seguridad
- Operadores de Cuartos de Control
- Redes IP e Inalámbricas
- Seguridad Perimetral
- Video Vigilancia

FORMACIÓN GERENCIAL

- Ciberseguridad para Alta Gerencia
- Evaluación de Riesgos de Seguridad
- Evaluación del Retorno de la Inversión en Seguridad
- Gerencia de Proyectos
- Management 3.0
- Ventas para la Industria de la Seguridad

NUEVAS TECNOLOGÍAS

- Drones en Seguridad
- Inteligencia Artificial en Seguridad
- Hacking Ético

CAPACITA A TU EQUIPO CON CURSOS IN COMPANY

Desde 6 participantes, con contenidos, fechas y horarios adaptados a tu organización.

APRENDE. ACTUALÍZATE. SIGUE CRECIENDO.



MANUELA RIVERA
Encargada de Cursos
WhatsApp: +57 304 2738724
Email: cursos@alas-la.org

CURSOS ALAS

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

Síguenos en nuestras redes sociales como **@alasseguridad**

LA ALIANZA ÉTICA

Cuando la Seguridad se Pacta con Confianza, no con Horas.



La seguridad privada enfrenta el desafío de superar un modelo centrado en la presencia física y avanzar hacia alianzas estratégicas capaces de anticipar riesgos, gestionar contingencias y proteger personas, activos y continuidad operativa. La propuesta es sustituir la lógica de las horas contratadas por una relación basada en capacidades, confianza, corresponsabilidad y resultados verificables.

En contextos de incertidumbre, existe una coreografía silenciosa que se repite cada día. En oficinas corporativas, complejos residenciales, centros comerciales e instalaciones industriales, la actividad transcurre bajo una promesa tácita: alguien está vigilando. La presencia de un operador uniformado representa para muchos usuarios la expresión visible de esa promesa.

Sin embargo, cuando una emergencia modifica el entorno en cuestión de segundos, esa representación puede revelar sus límites. Una evacuación, una concentración inesperada de personas, un incendio, un evento climático extremo, una interrupción tecnológica o cualquier otra contingencia puede convertir un puesto de vigilancia en el centro de una situación que exige mucho más que presencia. En ese instante, el operador debe interpretar información, tomar decisiones, comunicar, orientar, contener y activar procedimientos, muchas veces bajo presión y con recursos limitados.

EL PACTO DE CONFIANZA COMO FUNDAMENTO DE LA SEGURIDAD

Para comprender esta transformación conviene mirar más allá de la operación cotidiana. La seguridad está vinculada con una necesidad humana elemental: reducir la incertidumbre que amenaza la vida en común. Thomas Hobbes, en Leviatán (1651), colocó la búsqueda de seguridad en el centro de su reflexión sobre la organización política. Aunque la seguridad privada contemporánea no puede equipararse al Estado ni a sus funciones, la referencia permite reconocer una idea fundamental: **la protección constituye una condición para que las personas y las organizaciones puedan desarrollar sus actividades con un mínimo de previsibilidad.**

En el ámbito privado, esa necesidad se traduce en relaciones contractuales y operativas mediante las cuales una organización confía a terceros determinadas funciones de protección. La contratación de vigilancia supone, entonces, algo más profundo que la adquisición de horas de trabajo: supone depositar confianza en personas, procedimientos, sistemas y capacidades institucionales.

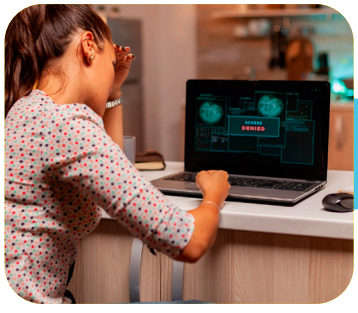


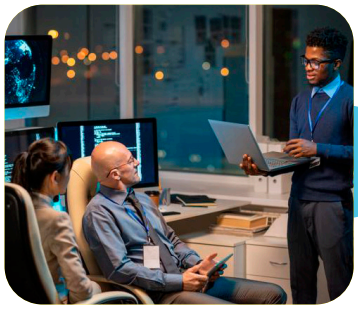
Esta distinción es decisiva. Si el servicio se diseña exclusivamente alrededor del número de puestos, jornadas y horas facturables, existe el riesgo de convertir la seguridad en un commodity indiferenciado. En cambio, cuando el proveedor comprende el contexto operativo del cliente, identifica vulnerabilidades, establece procedimientos de respuesta, capacita al personal y evalúa resultados, el servicio adquiere una dimensión estratégica.



ISO 31000:2018 concibe la gestión del riesgo como un proceso que comprende identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos, y recomienda integrarla en la gobernanza, la estrategia, la planificación y los procesos de la organización. La seguridad privada no sustituye ese sistema, pero puede convertirse en un componente operativo cuando sus capacidades se diseñan a partir del contexto y de los riesgos reales.

EL OPERADOR: PRIMER ESLABÓN DE UNA ARQUITECTURA INTEGRAL





La paradoja aparece cuando se exige al operador de primera línea una capacidad extraordinaria, pero se le proporciona una estructura insuficiente para ejercerla. Se espera que observe, comunique, controle accesos, atienda incidentes, aplique protocolos, gestione situaciones de tensión y actúe con criterio ante acontecimientos inesperados. **No obstante, en algunos modelos de contratación, la selección, formación, supervisión y dotación terminan subordinadas a una lógica de reducción de costos.**

La consecuencia es una contradicción organizacional: se demanda alto desempeño a quien ocupa la primera línea, pero no siempre se construye el sistema que permita alcanzarlo. La voluntad y experiencia del operador no sustituyen capacitación, procedimientos, equipos, comunicaciones y liderazgo.

Una arquitectura de seguridad sólida requiere, al menos, tres componentes articulados. El primero es la selección con rigor humano y profesional. No se trata únicamente de verificar requisitos administrativos, sino de procurar que las personas destinadas a funciones de vigilancia posean las condiciones compatibles con la responsabilidad que asumirán. El segundo es la formación continua, orientada no solo a rutinas ordinarias, sino también a primeros auxilios, evacuación, manejo de crisis, comunicación de incidentes, atención al usuario, prevención de conflictos y otros contenidos pertinentes al perfil de riesgo de cada instalación. El tercero es la supervisión efectiva, entendida como acompañamiento operativo, evaluación y corrección, no exclusivamente como mecanismo disciplinario.



DE LA CONTRATACIÓN DE HORAS A LA ALIANZA DE VALOR

El cambio de paradigma requiere modificar la conducta del cliente. La competencia basada exclusivamente en el menor precio puede producir una ilusión de ahorro que termina trasladando costos al futuro. Cuando el presupuesto de seguridad se determina sin considerar la exposición real al riesgo, la organización puede contratar una presencia nominalmente suficiente, pero operacionalmente incapaz de responder a escenarios críticos.

El cliente corporativo debe pasar de preguntar únicamente cuántos puestos y cuántas horas ofrece un proveedor a preguntar qué riesgos ha identificado, qué procedimientos propone, cómo capacita a su personal, cómo mide el desempeño, qué mecanismos de supervisión utiliza y qué ocurre cuando se presenta una contingencia. Estas preguntas cambian la conversación comercial: dejan de comparar solamente tarifas y comienzan a comparar capacidades.

La empresa de seguridad, por su parte, debe abandonar la prestación indiferenciada. Su propuesta de valor debe partir de un diagnóstico del entorno, identificar vulnerabilidades y definir objetivos verificables. No todos los clientes enfrentan los mismos riesgos ni requieren la misma arquitectura de protección.

De esta manera, la relación contractual puede evolucionar hacia un modelo de doble vía. **El proveedor aporta conocimiento especializado, personal competente, procedimientos, supervisión, tecnología y asesoramiento.** El cliente aporta información, facilita condiciones adecuadas, participa en simulacros y entiende que la seguridad constituye una responsabilidad organizacional transversal.

La alianza de valor exige además indicadores que permitan evaluar resultados. El número de horas cubiertas puede seguir siendo un dato operativo, pero no debería constituir el único indicador. Pueden incorporarse métricas como tiempos de respuesta, cumplimiento de rondas, porcentaje de personal capacitado, ejecución de simulacros, cierre de hallazgos, incidentes recurrentes, disponibilidad de equipos y cumplimiento de protocolos. La selección dependerá del contexto y del acuerdo entre las partes.

Esta lógica también se relaciona con la continuidad del negocio. ISO 22301:2019 proporciona un marco para planificar, implementar, mantener y mejorar un sistema de gestión que permita prepararse, responder y recuperarse frente a interrupciones. Su enfoque refuerza una idea central: **la seguridad privada genera mayor valor cuando sus procedimientos se articulan con los planes de emergencia y continuidad de la organización, en lugar de funcionar como una actividad aislada.**

La corresponsabilidad es esencial. La empresa de seguridad no puede garantizar por sí sola la continuidad de un negocio, ni el cliente transferir íntegramente su responsabilidad de gestión del riesgo. **La protección eficaz surge de la interacción entre personas, procesos, tecnología, liderazgo e información.**

La seguridad privada se encuentra ante una oportunidad de madurez. El sector puede continuar compitiendo principalmente por precio y volumen, o puede avanzar hacia una lógica de especialización, confianza y generación de valor. La segunda alternativa exige más conocimiento, más transparencia y una mayor responsabilidad de todos los actores.

AUTOR

GREGORIO GONZÁLEZ



SOBRE EL AUTOR

Coronel del Ejército en situación de reserva activa, Técnico Superior e Ingeniero en Comunicaciones y Electrónica, abogado, especialista en Ciencias Penales y Criminológicas, Magister Scientiarum en Ciencias Jurídicas y doctorante en Desarrollo Social. Docente universitario en Derecho y Psicología.

S&S
CONSULTORES CORPORATIVOS
RIF: J-502805737

DE LA SEGURIDAD AL CRECIMIENTO

PROTEGEMOS SU ESTRUCTURA. POTENCIAMOS SU MERCADO.

SEGURIDAD CORPORATIVA

- Ciberseguridad
- Gestión de Riesgos
- Inteligencia Protectiva
- Compliance
- Background Check
- Avanzada Tecnológica de Locaciones

MARKETING 360 & IA

- Branding Strategy
- Publicidad Multicanal
  Google Ads Meta in
- Automatización con IA





¿LISTOS PARA EL SIGUIENTE NIVEL?
- **ADOLFO M. GELDER,** Gerente General

CAPACITACIÓN & FORMACIÓN

- **Habilidades Gerenciales**
  - Trabajo en Equipo
  - Inteligencia Emocional
- **Ciberseguridad & Tech**
  - Detección IA
  - Blockchain
  - IoT Seguro

Cursos avanzados dara:
- Experto en Contrainteligencia
- Agente HUMINT
- Analista

SISTEMAS DE GESTIÓN ISO

- **ISO 9001**
- **ISO 27001**
- **ISO 37001**

Metodología 4 fases
- Diagnóstico
- Diseño
- Implementación
- Auditoría

Web: www.ssconsultores360.com
WhatsApp: +58 412 7241188
Numeros Telefónicos: (0239) 5111596
@solsertuy
marketing@ssconsultores360.com
Caracas - Cúa, Edo. Miranda.

CUANDO LA TIERRA TIEMBLA EN CASA Y EL CORAZÓN LO HACE EN EL EXILIO

Una mirada médica al impacto psicológico de un terremoto en el venezolano que vive lejos de su país.



Hay tragedias que destruyen edificios, carreteras y ciudades. Otras derrumban aquello que no puede fotografiarse: la tranquilidad, la esperanza y la sensación de seguridad. Un terremoto puede fracturar tanto la tierra como el equilibrio físico y emocional del ser humano.

Desde la medicina de emergencias y desastres sabemos que una emergencia no termina cuando la tierra deja de temblar. Tras las lesiones físicas, las pérdidas materiales y la separación de las familias, emerge otra dimensión, menos visible pero igualmente profunda: la respuesta neurobiológica y psicológica del ser humano ante una amenaza que puede alterar, en cuestión de segundos, su sensación de seguridad, estabilidad y control.

Para quienes viven el desastre directamente, el sufrimiento es inmediato. Pero existe otro grupo de víctimas silenciosas: quienes contemplan la tragedia desde la distancia.

Para el venezolano que vive fuera de su país, un terremoto en Venezuela no es simplemente una noticia. Puede convertirse en una experiencia emocional profundamente perturbadora, capaz de activar miedo, incertidumbre y una intensa sensación de pérdida de control.

Aquel día comenzó como cualquier otro. Miles de venezolanos en el exterior despertaron para trabajar, estudiar o continuar la rutina que impone la migración. Nadie imaginaba que, al caer la tarde, la vida volvería a dividirse en un antes y un después.

Las primeras noticias llegaron de manera confusa. Las redes sociales comenzaron a llenarse de mensajes sobre un fuerte temblor. Luego aparecieron reportes contradictorios sobre la magnitud y el número de movimientos sísmicos. La información era escasa y cambiante.

En una emergencia, la incertidumbre constituye un importante estresor. El cerebro necesita información para evaluar el riesgo y determinar si existe una amenaza. Cuando esta información no está disponible, puede mantenerse en un estado de vigilancia sostenida. Para quien está lejos de Venezuela, la distancia multiplica la angustia.



No existe la posibilidad de correr hacia el hogar de un familiar, abrazar a un amigo o comprobar personalmente que nuestros seres queridos están a salvo. Solo queda esperar, esperar una llamada, esperar un mensaje, esperar que aparezca la señal de internet.

Durante esa espera, el organismo puede activar una respuesta aguda al estrés. El sistema nervioso simpático y el eje hipotálamo-hipófisis-adrenal participan en la preparación del cuerpo ante el peligro. Aumenta la frecuencia cardíaca, aparecen palpitaciones, temblores, cefaleas, opresión torácica, dificultad respiratoria, alteraciones gastrointestinales e insomnio. Puede presentarse llanto, irritabilidad, dificultad para concentrarse, pensamientos repetitivos o incapacidad para continuar con las actividades cotidianas.

Estas manifestaciones no significan automáticamente una enfermedad psiquiátrica. Son, en muchos casos, respuestas esperables ante una situación extraordinaria. La preocupación surge cuando persisten, se intensifican o deterioran significativamente el funcionamiento de la persona.



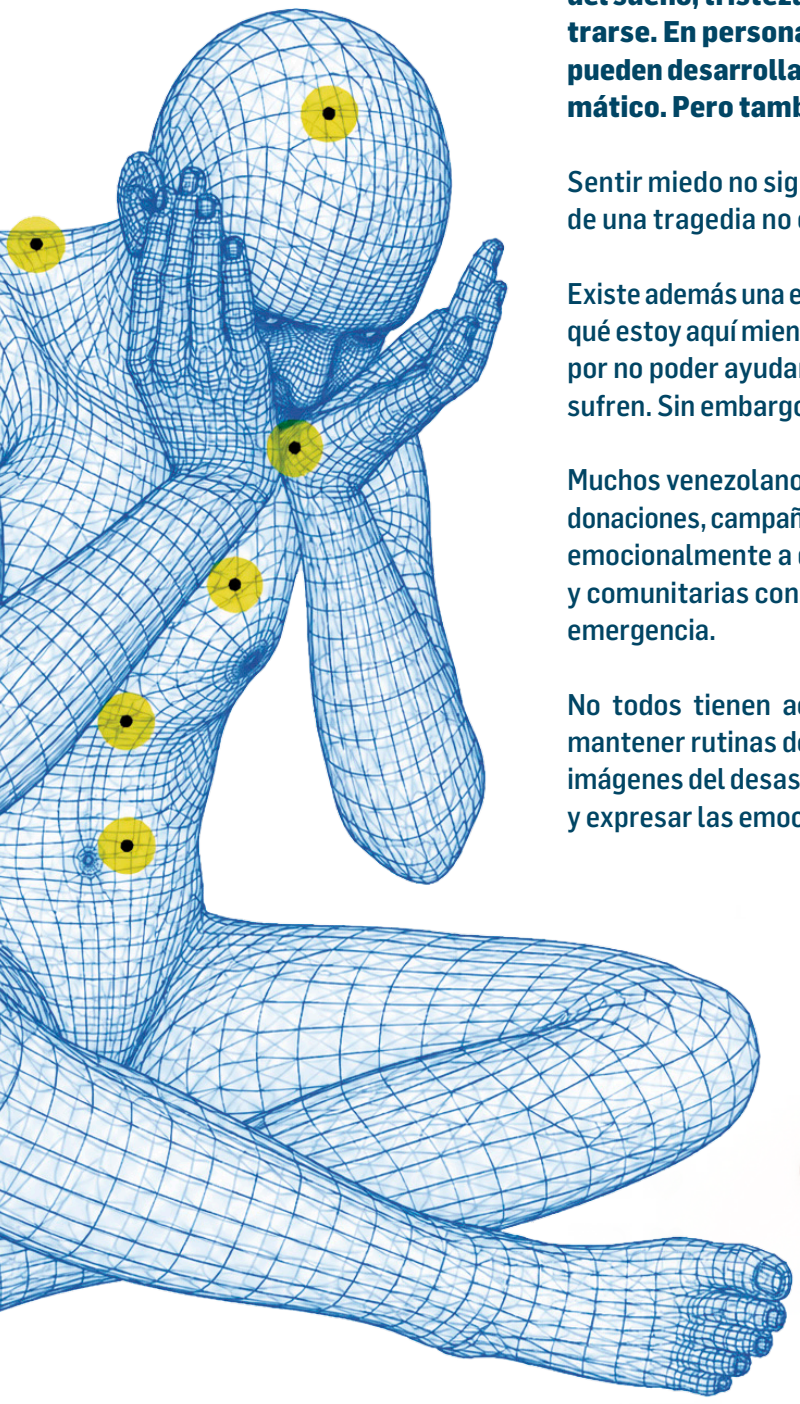
Entonces llegan tres palabras capaces de cambiarlo todo: “Estamos bien, hijo.”

La confirmación de que nuestros seres queridos están vivos y seguros permite disminuir progresivamente la respuesta de alarma. Pero no todos reciben ese mensaje. Hay quienes esperan durante horas o días. Otros reciben noticias que jamás habrían querido escuchar.

Comienza entonces otro proceso: el duelo.

El venezolano migrante ya carga consigo múltiples pérdidas: hogar, costumbres, amigos, rutinas y años de convivencia con sus seres queridos. La migración puede generar un complejo proceso de duelo y adaptación.

Cuando una catástrofe golpea el país de origen, ese duelo puede reactivarse. Pueden aparecer ansiedad persistente, alteraciones



del sueño, tristeza, aislamiento, irritabilidad y dificultad para concentrarse. En personas vulnerables o con exposición intensa al desastre pueden desarrollarse cuadros de ansiedad, depresión o estrés postraumático. Pero también es importante no patologizar el dolor.

Sentir miedo no significa padecer un trastorno de ansiedad. Llorar después de una tragedia no constituye una enfermedad.

Existe además una emoción frecuente entre quienes viven lejos: la culpa. "¿Por qué estoy aquí mientras ellos están allí?" La persona puede sentirse culpable por no poder ayudar físicamente o por continuar con su vida mientras otros sufren. Sin embargo, estar lejos no significa ser indiferente.

Muchos venezolanos transforman esa impotencia en solidaridad: organizan donaciones, campañas de ayuda, difunden información verificada o acompañan emocionalmente a quienes permanecen en Venezuela. Estas redes sociales y comunitarias constituyen importantes factores protectores durante una emergencia.

No todos tienen acceso a atención psicológica o psiquiátrica. Por ello, mantener rutinas de sueño y alimentación, limitar la exposición constante a imágenes del desastre, conservar el contacto social, realizar actividad física y expresar las emociones pueden ser medidas iniciales de autocuidado.



Cuando aparecen insomnio persistente, crisis de pánico recurrentes, ansiedad incapacitante, tristeza sostenida, aislamiento marcado, consumo problemático de sustancias o pensamientos relacionados con la muerte, se requiere valoración profesional.

La salud mental forma parte integral de la salud. Después de una catástrofe, atender las lesiones físicas es indispensable, pero también lo es reconocer las heridas emocionales que pueden permanecer cuando las cámaras se retiran.

Con el paso de las semanas llega la reconstrucción: de hogares, familias y proyectos de vida. La recuperación no es lineal y cada persona responde de manera diferente según sus pérdidas, antecedentes, recursos y redes de apoyo.

Ante esta tragedia la resiliencia no significa ausencia de dolor. Significa la capacidad de reorganizar la vida después de la adversidad sin negar aquello que se ha vivido. Algunas heridas son visibles, otras permanecen ocultas, y muchas necesitan tiempo, acompañamiento y, cuando es necesario, atención profesional para cicatrizar.

Hoy en día ser venezolano no consiste únicamente en haber nacido dentro de unas fronteras. Es llevar una memoria colectiva que viaja a cualquier lugar del mundo. Por eso, cuando la tierra tiembla en Venezuela, también tiembla el corazón de quienes viven lejos. Pero, así como los edificios pueden reconstruirse piedra sobre piedra, el ser humano también puede recuperarse y, donde haya un venezolano dispuesto a tender la mano, mantener viva la esperanza y cuidar de otro, allí seguirá latiendo Venezuela.



AUTOR

DR. JONATHAN TRUJILLO MEJÍA

SOBRE EL AUTOR

Médico Cirujano, Filántropo y Filósofo estoico, egresado de la Universidad de Carabobo (Venezuela), con certificación en Colombia y España. Durante más de 15 años, ha desarrollado su carrera en los ámbitos de urgencias, emergencias y desastres, atención prehospitalaria y gestión de servicios de salud.

TERREMOTOS Y CIBERAMENAZAS:

DEL SISMO FÍSICO AL FRAUDE DIGITAL EN TIEMPOS DE CRISIS



La naturaleza impredecible de los desastres naturales —como el devastador doble terremoto que sacudió a Venezuela el pasado 24 de junio— expone con dureza la fragilidad de nuestra infraestructura física. Sin embargo, en la era de la hiperconectividad, existe otra dimensión de vulnerabilidad que suele pasar desapercibida hasta que es demasiado tarde: la seguridad digital.

Durante una emergencia, el pánico, la necesidad urgente de información sobre seres queridos y la voluntad de ayudar crean un escenario psicológico de alta vulnerabilidad. Es en este terreno fértil donde opera la ciberdelincuencia oportunista, desplegando maniobras diseñadas no por alta sofisticación técnica, sino por una profunda manipulación emocional.

El 'Modus Operandi': Cómo Opera el Cibercrimen en Escenarios de Emergencia

Cuando ocurre una catástrofe, los delincuentes informáticos adaptan rápidamente sus vectores de ataque para explotar el contexto de caos. En lugar de crear amenazas complejas desde cero, aprovechan el flujo masivo de información para camuflar sus operaciones:

Falsas Campañas de Crowdfunding y Colectas: Aprovechando la solidaridad colectiva, los atacantes suelen crear perfiles paralelos en redes sociales o plataformas de recaudación, solicitando donaciones directas mediante transferencias o Pago Móvil a nombre de particulares. Utilizan imágenes reales de la tragedia para conmover y desviar recursos que jamás llegan a las víctimas.

Phishing de Emergencia y Mapas de Riesgo Contaminados: En la búsqueda de mapas de réplicas, estados de vías o listados de sobrevivientes, los usuarios suelen recibir enlaces masivos por mensajería instantánea. Al hacer clic, son redirigidos a sitios clonados que solicitan credenciales de correo o descargan archivos maliciosos (como ejecutables o APKs) en el dispositivo.

Usurpación de Identidad e Institucional: Es habitual la creación de cuentas falsas que imitan a organismos de rescate, ONGs o medios de comunicación para solicitar insumos o difundir información falsa. Asimismo, recurren a la suplantación de identidades personales mediante mensajería para pedir dinero a contactos argumentando urgencias médicas tras el sismo.

Ofertas Ficticias de Suministros y Servicios: Ante el temor a nuevos colapsos o fallas de servicios, proliferan ofertas fraudulentas de inspecciones estructurales, plantas eléctricas o equipos de emergencia, exigiendo pagos por adelantado y desapareciendo tras recibir la transferencia.

Guía de Prevención: ¿Qué Hacer ante un Nuevo Desastre Natural?

Para evitar que la emergencia física se traduzca en una crisis financiera o de privacidad, es vital incorporar protocolos de ciberhigiene en los planes de contingencia familiar y empresarial:

Para evitar que la emergencia física se traduzca en una crisis financiera o de privacidad, es vital incorporar protocolos de ciberhigiene en los planes de contingencia familiar y empresarial:

1 Informarse Exclusivamente por Canales Oficiales:

Ante eventos sísmicos u otras catástrofes, ignore cadenas de WhatsApp con enlaces acortados. Consulte únicamente las cuentas verificadas de los organismos de protección civil, autoridades de gestión de riesgo y medios periodísticos acreditados.

2 Verificar Antes de Donar:

Si desea aportar a causas comunitarias, hágalo únicamente a través de instituciones, fundaciones u ONGs con trayectoria comprobable.

Desconfíe sistemáticamente de solicitudes de dinero remitidas a cuentas personales de desconocidos o vías no auditables.

3 Confirmación Directa por Voz:

Si recibe un mensaje de un conocido solicitando dinero urgente debido a pérdidas causadas por el sismo, no realice transferencias de inmediato. Realice una llamada telefónica convencional o use un canal alternativo para corroborar su identidad.

4 No Descargar Archivos no Solicitados:

Evite instalar aplicaciones desconocidas que prometan “detectar réplicas” o visores de documentos que aseguren contener listas de afectados.

La Respuesta Tecnológica: La Solución Integral con Dr. Web

Aunque la prudencia es la primera línea de defensa, el estrés de una catástrofe puede llevar incluso a usuarios experimentados a cometer errores. Por ello, la verificación humana debe complementarse con una barrera tecnológica automatizada en tiempo real.

En este ámbito, Dr. Web se consolida como una herramienta clave para mitigar las amenazas digitales que surgen tras un desastre natural:

Protección Anti-Phishing en Tiempo Real: El filtro anti-phishing de Dr. Web analiza y bloquea instantáneamente accesos a sitios web fraudulentos que suplantan a entidades bancarias, plataformas de recaudación o instituciones de socorro.

Módulo Antispam y Control Web: Intercepta enlaces maliciosos contenidos en mensajes de correo masivo o chats de mensajería antes de que el usuario pueda ejecutarlos accidentalmente.

Análisis Heurístico de Malware: Detecta y aísla troyanos, aplicaciones maliciosas o descargadores encubiertos en supuestos mapas o boletines de emergencia, protegiendo la integridad del sistema operativo.

Fortaleciendo la Resiliencia Digital

Los acontecimientos vinculados al sismo del 24 de junio nos recuerdan que la preparación ciudadana debe ser integral. Así como identificamos rutas de evacuación y preparamos un bolso de emergencia, debemos proteger nuestro entorno digital contra los depredadores de la red. La combinación de un criterio informado y el respaldo de soluciones robustas como Dr. Web garantiza que nuestra solidaridad e información se mantengan a salvo en los momentos en que más las necesitamos.

AUTOR

ALEXANDRO LAURENT
CEO AYAC.LLC
AYAC LLC MAYORISTA DE DR. WEB

AYAC LLC



GESTIÓN DE RIESGOS VS. GESTIÓN DE CRISIS

DEBIDO A DESASTRES IMPREVISTOS:

CASOS REALES QUE DEMUESTRAN LA IMPROVISACIÓN EN AMÉRICA LATINA.



"LA IMPROVISACIÓN NO ES MÁS QUE EL PRÓLOGO DEL LIBRO DE UNA TRAGEDIA ANUNCIADA; CUANDO EL COSTO DE PREVENIR SE VE COMO UN GASTO INNECESARIO, EL PRECIO FINAL SIEMPRE SE PAGA CON VIDAS HUMANAS".

Existe una peligrosa tendencia en nuestra América Latina de ver el desastre como un capricho de la naturaleza o como un simple designio del destino. Sin embargo, cuando analizamos las causas estructurales de cada tragedia que enluta a nuestros pueblos, descubrimos una verdad incómoda que he venido advirtiendo en artículos anteriores para diversas revistas de seguridad del continente: la catástrofe rara vez es un accidente; es la consecuencia directa de nuestras acciones de omisión, una cultura arraigada en el ciudadano latinoamericano, donde la improvisación, el desinterés y los círculos viciosos, son sus premisas.

LA CULTURA DEL "RESOLVER" Y LA NEGLIGENCIA INSTITUCIONAL:

En el continente, nos hemos acostumbrado a malinterpretar la resiliencia. Confundimos la capacidad de sobreponernos al dolor con la irresponsabilidad de no prevenir aquello que es perfectamente previsible. Vivimos bajo la ley del "vamos viendo" y del "resolver sobre la marcha" improvisando, una mentalidad que ha permeado tanto al ciudadano de a pie como a quienes ostentan cargos de poder.

Tal como he sido enfático en mi libro **"HABLÓ EL SARGENTO MAYOR: Ante los antivalores de la humanidad",** esta falta de integridad en el ser humano no es un hecho aislado, sino un fenómeno que atenta contra la estructura misma de nuestra sociedad. Cuando la ética se ausenta, la seguridad deja de ser una prioridad técnica para convertirse en un estorbo que se intenta sortear mediante el facilismo. Las normas internacionales de seguridad no son caprichos burocráticos; son estándares diseñados con experticia por especialistas, para evitar lo irreparable.

CASOS REALES QUE NOS DAN LA RAZÓN:

Caso 1



La historia reciente nos sacude con ejemplos innegables de cómo la falta de ética se paga con vidas. El trágico colapso de la discoteca Jet Set en República Dominicana, ocurrido el pasado 8 de abril de 2025, donde lamentablemente perdieron la vida 236 personas y resultaron heridas más de 180 en el concierto del reconocido artista ***Rubby Pérez***, es un recordatorio imborrable. Permitir la remodelación y apertura de un local que había sufrido un incendio previo, burlando controles técnicos, fue un acto de irresponsabilidad criminal por parte de las autoridades de ese país. Quedo evidenciado ante el mundo, que la corrupción de las autoridades, la codicia del propietario y el desprecio por la vida de esos seres humanos inescrupulosos, transformaron esa estructura debilitada en una trampa mortal.

Caso 2



Otro caso real reciente a destacar, fue lo suscitado en las pasadas fiestas de carnavales de 2026, en la población de Guanare, estado Portuguesa, donde las autoridades venezolanas permitieron instalar una tarima de espectáculos en pleno cauce de un río y luego una crecida, el rio arrasó con todo a su paso, sin pérdida de vidas que lamentar, nos obliga a reflexionar en que estamos y hacia dónde vamos con nuestros comportamientos. Autorizar aglomeraciones en zonas de riesgo hidrológico, por cumplir con una agenda política, revela una desconexión total con la responsabilidad y la gestión de riesgos. Cuando suceden situaciones como estas, nos damos cuenta que no se trata solo de falta de conocimiento técnico; sino de la ausencia de criterio profesional, que desde INSEAL combatimos incansablemente, por medio de nuestras capacitaciones, webinar y conversatorios.

Caso 3



Lo ocurrido tras el devastador doblete sísmico del 19 de junio de 2026 en Venezuela, con más de 6.000 fallecidos, desnudó la profunda incapacidad estatal para gestionar tanto el riesgo como la crisis. Luego de la tragedia del deslave en 1.999, las autoridades priorizaron caprichos políticos y obras cosméticas, como por ejemplo el cambio de nombre del estado Vargas a La Guaira y desarrollos urbanísticos, en zonas de alto riesgo, en lugar de fortalecer la prevención. Tras el impacto, la respuesta oficial rozó la deshumanización, donde el mundo observo víctimas sepultadas masivamente en fosas comunes y sobrevivientes hacinados en refugios improvisados en plazas, canchas y escuelas, a lo que se sumó el ecocidio de vertir escombros en las playas del sector cercano a la tragedia.

Esta cadena perpetua de improvisación no solo enlutó a un país entero, sino que dejó la advertencia ineludible de que la negligencia, la falta de preparación y la indolencia institucional destruyen y deshonran con la misma fuerza que cualquier desastre natural.

Lejos de asumir autocrítica, el panorama se tornó aún más repulsivo. Quienes ejercemos la seguridad a nivel internacional fuimos testigos indignados de cómo seudoespecialistas locales, cómplices y beneficiarios del monopolio de la seguridad bajo la dictadura por más de dos décadas, se atrevieron a vanagloriarse en redes sociales, hasta con imágenes generadas por inteligencia artificial disfrazados de rescatistas, aprovechando el momento. Estos actores, cómplices silentes de una tragedia que cobró miles de vidas por su deliberada omisión de asesorar técnicamente a las autoridades a su debido tiempo, hoy posan cínicamente como expertos gestores de riesgos sobre las tumbas de miles de venezolanos, pero después de ocurrida la tragedia.

LA CORRESPONSABILIDAD CIUDADANA ANTE EL PELIGRO:

Comprender el problema no es una tarea exclusiva de expertos o gobernantes; exige una ciudadanía educada y vigilante. Cuando la sociedad naturaliza el peligro y las autoridades actúan sin rigor científico, la tragedia se vuelve inevitable. Exigir protocolos profesionales sin improvisaciones es un deber ético de la sociedad, que garantiza la preservación de nuestras comunidades.

RECOMENDACIONES DE INSEAL

Creación de un Ministerio de Gestión de Riesgos y Crisis:

Cada gobierno de determinado país, debería contar con un Ministerio de Gestión de Riesgos y Crisis, donde se priorice a nivel nacional, la gestión de riesgos sobre la reacción: Ninguna construcción, proyecto habitacional comercial, evento masivo u obra pública en el país, debe ejecutarse, sin una estricta auditoría técnica previa, que evalúe y mitigue vulnerabilidades reales. Esas auditorias, deben ser realizadas por especialistas, calificados en materia de Seguridad, Gestión de Riesgos y Crisis.

Erradicar la Corrupción Estructural mediante la ley:

La flexibilización de normas de ingeniería o la omisión de permisos bajo sobornos o conveniencias políticas debe tipificarse y combatirse como un delito contra la vida.

Capacitación Continua y Profesionalización del Personal:

La constante formación profesional y actualización de nuestro personal, incluyendo temas de liderazgo ético y efectividad grupal, debe ser una prioridad en cada institución, empresa u organización, ya que, sobre estos pilares, se sostiene la profesión.

Educación Preventiva Ciudadana:

Fomentar una cultura de autoprotección en la sociedad y realizar constantes simulacros rigurosos en comunidades y empresas frente a amenazas latentes como sismos y desastres naturales. De esa manera evitaremos la pérdida de vidas inocentes.

La seguridad de la sociedad, no es un costo innecesario; es el cimiento sagrado sobre el cual se edifica una nación civilizada. **En INSEAL seguiremos trabajando para que la improvisación deje de ser la regla y la gestión de riesgos basada en la ética sea el estándar innegociable en nuestro continente.** Quienes deseen conocer nuestra gama de servicios o integrarse a este proyecto internacional, pueden visitar nuestro portal web: www.inseal.us

Recomendaciones adicionales: En vista de que el tema del articulo está enfocado en la Gestión de Riesgos, Crisis y Administración de Desastres, respetuosamente propongo que el articulo sea acompañado por imágenes reales (adjuntas a este articulo), sobre los casos que allí se exponen.



AUTOR

DICXON RUÍZ

INSEAL LATAM – El futuro de la seguridad en Venezuela comienza con una alianza solida



- Potencia tu empresa de seguridad.
- Únete a la familia INSEAL LATAM y desarrolla nuevos negocios.
- Capitaliza nuestra reputación internacional y marca global.
- Accede directamente a nuestros robustos programas de capacitación y mejora continua.
- Únete a nuestra red global de líderes en seguridad.
- Transforma tu operación local con respaldo internacional.

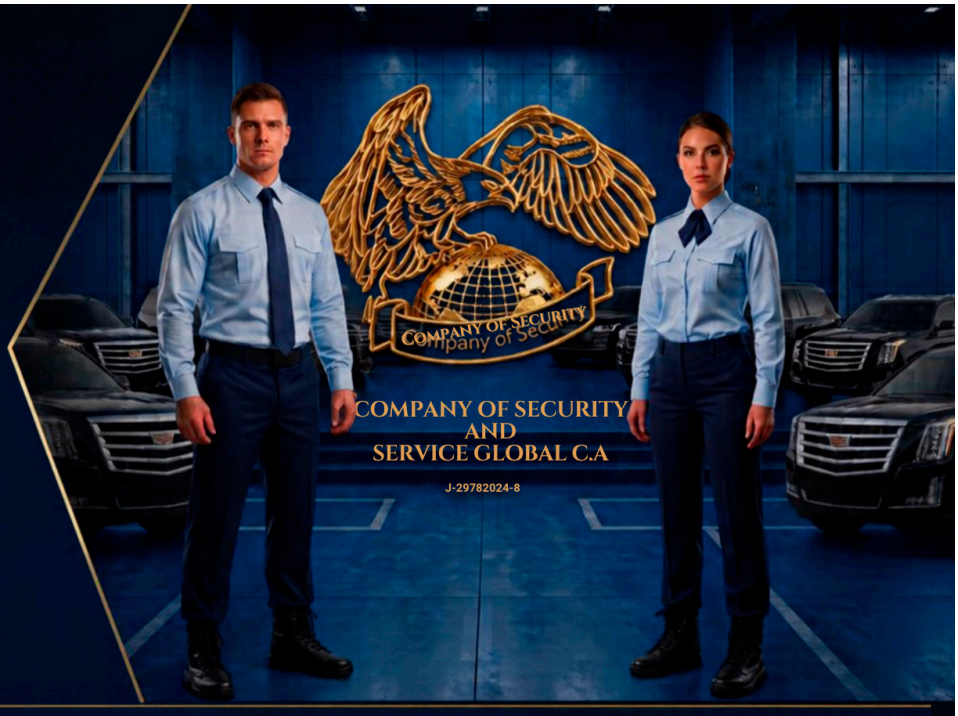
TELÉFONO: +1 (918) 895-2620 / info@inseal.us

www.inseal.us

COMPANY OF SECURITY AND SERVICE GLOBAL C.A

J-29782024-8

Seguridad corporativa y diplomática



Protección de personas, instalaciones y operaciones en entornos de alta complejidad.

SERVICIOS PRINCIPALES

- Seguridad corporativa y diplomática
- Protección ejecutiva y transporte seguro
- Centro de operaciones e inteligencia
- Consultoría y gestión de riesgos
- Formación especializada

17 años de operación continua en Venezuela

CECOM bilingüe 24/7 con cobertura nacional

11 años de servicio ininterrumpido a una misión diplomática del G7

Rotación de personal < 5 %

✓ ISO 9001:2015 · Certificado N.° 580181, vigente hasta 2028
✓ Cyber Essentials
✓ Miembro corporativo IFPO
✓ Procedimientos alineados a ISO 18788, ISO 31000 e ISO/IEC 27001

Haga de CSSG su aliado en seguridad

Contáctenos para diseñar la protección que su organización necesita.

cssg-global.com · info@globalservices-ven.com · +58 212 261 1768 · +58 414 317 4373 · Caracas · Miami

LA EVOLUCIÓN DE LA PROTECCIÓN COMO DISCIPLINA PROFESIONAL EN VENEZUELA:

UN ANÁLISIS CRÍTICO DEL CONTEXTO VENEZOLANO



INTRODUCCIÓN

La protección, definida como la actividad de salvaguardar personas, bienes e información, ha experimentado décadas de transformación hacia su profesionalización, proceso documentado por el Dr. Martin Gill, figura central en criminología y seguridad. Este tránsito del comercio a la profesión enfrenta desafíos únicos en Venezuela que requieren análisis cuidadoso, pues la delincuencia impacta directamente el desarrollo económico y social del país. Este ensayo explora la realidad venezolana a la luz de los estudios de Gill, proponiendo acciones concretas para profesionalizar el sector, reconociendo que, aunque existen avances, persisten vacíos estructurales que deben abordarse con urgencia.

LA FRAGMENTACIÓN TEORÍA-PRÁCTICA Y EL CONTEXTO LABORAL VENEZOLANO

Gill destaca la brecha entre la teoría académica wwción, describiéndola como "trabajar en relativo aislamiento". En Venezuela, esta fragmentación se manifiesta en universidades que ofrecen programas de seguridad sin abordar los desafíos operacionales diarios, mientras los profesionales, abrumados por entornos de alto

AUTOR

DR. TOVAR CARTAYA JOHN RAFAEL C.P.O

SOBRE EL AUTOR

Comisario General CICPC, Postdoctorante en Criminalística, Doctor en Seguridad Ciudadana, Consultor en Seguridad Integral

riesgo, rara vez participan en investigaciones que podrían mejorar su práctica. Cuando Gill señala que "la academia no ofrece una explicación universal aceptada de los motivos del crimen", evidencia una debilidad que en Venezuela se agrava por la falta de investigación local sobre dinámicas delictivas específicas, donde la extrema desigualdad, la corrupción y el control por grupos armados crean escenarios que desafían los modelos explicativos tradicionales.

Gill también explica cómo el lugar de trabajo se ha convertido en escenario favorito para la actividad delincuencial. Sus hallazgos, basados en estudios internacionales, encuentran confirmación dramática en Venezuela. Un estudio británico que muestra que las tiendas minoristas tenían cuatro veces más probabilidades de ser robadas que los hogares podría replicarse en Venezuela con resultados aún más alarmantes. La afirmación del autor de que "5.774 personas fueron asesinadas en el trabajo en la última década" cobra especial gravedad en nuestro país, donde la violencia vinculada al crimen organizado y la falta de responsabilidad podrían elevar significativamente esta cifra. Los trabajadores del transporte, campos petroleros, zonas comerciales y seguridad privada enfrentan peligros diarios que superan lo documentado por Gill.

PROPUESTAS INMEDIATAS:

- **Crear grupos de trabajo permanentes entre académicos venezolanos y expertos en protección para desarrollar conocimientos locales**
- **Establecer un observatorio de delitos laborales que documente incidentes y genere estadísticas fiables para diseñar políticas de prevención adecuadas a nuestra realidad.**

EL DESAFÍO DE LA PROFESIONALIZACIÓN Y LA TECNOLOGÍA EN EL CONTEXTO VENEZOLANO

Gill sostiene que la protección está pasando "de comercio a profesión", citando ausencia de formación formal, regulación débil y falta de estructuras para garantizar estándares mínimos. En Venezuela, la educación formal ha sido tradicionalmente dirigida por instituciones militares y policiales, enfocándose en habilidades operacionales y tácticas con pocas oportunidades para el estudio teórico o desarrollo de capacidades de gestión. Aunque los programas universitarios se han expandido, suelen ser generales o centrados en detalles técnicos. La falta de regulación es quizás el problema más grave: existen leyes para empresas de seguridad privada, pero no se aplican ni supervisan adecuadamente, generando un mercado dominado por prácticas improvisadas donde la competencia desleal y la informalidad empujan a quienes buscan mantener estándares de calidad. El resultado es una industria con empleos inseguros, capacitación insuficiente y oportunidades limitadas de promoción profesional.

En cuanto a la tecnología, Gill se centra en la conexión entre tecnología y gestión, citando a Hayes para argumentar que, si bien los avances tecnológicos mejoran el control de pérdidas, un liderazgo y gestión eficaces ofrecen la solución definitiva. En Venezuela, la tecnología de seguridad, particularmente las cámaras de vigilancia, ha sido ampliamente adoptada como reacción al sentimiento de inseguridad, pero la observación de Gill de que "la protección del mundo ha encontrado soluciones antes de definir problemas" encuentra

aplicación casi literal. Es común instalar sistemas de videovigilancia sin analizar riesgos específicos, sin definir objetivos claros y sin personal capacitado para operarlos. Esta situación se agrava por la falta de evaluaciones nacionales de eficacia; Gill señala que las evaluaciones positivas raramente son realizadas por expertos independientes, y en Venezuela este conflicto de intereses se agrava porque la compra y gestión de sistemas suelen estar vinculados a redes influyentes que impiden evaluaciones imparciales.

PROPUESTAS INMEDIATAS:

- Lanzar un programa nacional de certificación voluntaria para profesionales de seguridad que establezca normas mínimas de competencia y ética.
- Crear protocolos normalizados para la implementación de sistemas de CCTV que abarquen evaluación de necesidades, objetivos medibles y evaluación periódica de resultados.

DIMENSIÓN HUMANA Y CONSTRUCCIÓN DE CONOCIMIENTO EN PROTECCIÓN

Uno de los aspectos más valiosos del análisis de Gill es su reconocimiento de la dimensión humana de la protección. Al documentar el impacto del delito en el lugar de trabajo, destaca el efecto desmoralizador sobre los empleados y el efecto en la calidad de vida comunitaria. En Venezuela, la crisis económica y social ha hecho a los trabajadores más vulnerables; muchos profesionales de protección trabajan en condiciones precarias con salarios bajos que les obligan a buscar ingresos adicionales, debilitando su compromiso con funciones protectoras. Gill señala que "a veces es más importante ser visto haciendo algo, lo que sea, que hacer lo correcto", observación que critica medidas superficiales, pero destaca la importancia de la percepción en la gestión de seguridad. En Venezuela, donde la confianza institucional es baja, hacer visible el esfuerzo de protección puede ser clave, pero no debe venir a expensas de la eficacia, pues la protección no puede ser solo un espectáculo cuando los riesgos son reales.

Gill concluye enfatizando la necesidad de "crear un cuerpo reconocido de conocimiento" que combine teoría y práctica, ofreciendo "un conjunto de teorías y marcos de trabajo" para avanzar en la profesionalización. El proceso de gestión del riesgo penal propuesto, que incluye evaluación, toma de decisiones, transferencia de riesgos y desarrollo de estrategias, ofrece un marco conceptual útil para diseñar sistemas de protección en el contexto venezolano, pero debe adaptarse cuidadosamente a las condiciones específicas del país y sus regiones. En Venezuela, donde las instituciones públicas luchan por manejar el crimen, las organizaciones privadas han tomado la iniciativa, pero esta no siempre conduce a mejores prácticas. La falta de una base de conocimientos que organice experiencias exitosas y fallidas, registre mejores prácticas y cree ideas relevantes para la toma de decisiones dificulta el desarrollo del sector.

PROPUESTAS INMEDIATAS:

- **Crear programas de bienestar para profesionales de protección que cubran aspecto técnico, bienestar físico y mental, crecimiento profesional y calidad de vida**
- **Convocar una reunión nacional de profesionales, académicos y líderes empresariales para comenzar a construir un observatorio de buenas prácticas en seguridad que identifique y documente experiencias exitosas en prevención del delito en el lugar de trabajo venezolano.**

RIESGOS INVISIBLES

después del Terremoto en Venezuela



Los terremotos constituyen fenómenos naturales inevitables; sin embargo, sus consecuencias trascienden el impacto físico y alcanzan dimensiones sociales e institucionales que merecen un análisis desde la criminología y la gestión integral del riesgo.

Cuando la tierra deja de temblar, comienza una segunda emergencia: aquella que no siempre aparece en los informes de daños, pero que compromete la seguridad, la institucionalidad y la protección de las personas más vulnerables. En Venezuela surge una emergencia invisible la vulnerabilidad post-sísmica, entendida como el momento en que la alteración del orden cotidiano, la sobrecarga institucional y la incertidumbre colectiva pueden aumentar las oportunidades para la realización de delitos y dificultar la capacidad y velocidad de respuesta de las autoridades.

No se trata de afirmar que un terremoto genera criminalidad, sino de reconocer que determinados factores de riesgo pueden hacerse más visibles en contextos de emergencia en donde la mayoría quedan expuestos. Los Factores criminógenos post-terremoto son:



COLAPSO DE SERVICIOS:

La falta de electricidad, agua y gas anula los sistemas de vigilancia y control operativo.

VÍAS COLAPSADAS:

La restricción de movilidad retrasa la acción policial y de los órganos de seguridad ciudadana.

INMUEBLES DESOCUPADOS:

El desalojo masivo expone viviendas y locales comerciales al delito de hurto calificado.

SOBRECARGA DE RESCATE:

La policía y protección civil concentran su esfuerzo en salvar vidas, descuidando el patrullaje preventivo.

La interrupción de estos servicios esenciales puede crear escenarios que son aprovechados para conductas ilícitas como Tipologías delictivas emergentes las cuales son:



SAQUEOS Y PILLAJE:

La falta de electricidad, agua y gas anula los sistemas de vigilancia y control operativo.

FRAUDES CIBERNÉTICOS Y DE CALLE:

Creación de campañas de falsa ayuda humanitaria para lucrarse de la buena fe ciudadana.

ESPECULACIÓN Y ACAPARAMIENTO:

Delitos contra el orden socioeconómico al encarecer víveres y materiales esenciales.

DESINFORMACIÓN MALICIOSA:

Difusión de noticias falsas para generar alarma social y facilitar desmanes.

Aunque estas conductas representan una minoría frente a la solidaridad que habitualmente manifiestan las comunidades, su impacto sobre la confianza pública y la percepción de seguridad resulta importante en estos escenarios.

Precisamente, uno de los aspectos más relevantes es reconocer que la resiliencia social constituye un factor protector. La experiencia internacional demuestra que, ante los desastres, predominan las conductas de cooperación, apoyo mutuo y organización comunitaria. Fortalecer esas capacidades mediante programas de preparación ciudadana y coordinación institucional reduce la vulnerabilidad y favorece una recuperación más rápida y ordenada.

Desde la criminalística emergen desafíos importantes. Como el colapso de edificaciones que pueden obedecer exclusivamente a la intensidad

del fenómeno natural o también revelar fallas estructurales, incumplimientos normativos o negligencias de construcción cuya determinación corresponde a investigaciones técnicas posteriores. En consecuencia, la actuación de los organismos de primera respuesta debe procurar, siempre que las condiciones operativas lo permitan y sin afectar el rescate de víctimas, preservar, delimitar, Resguardar aquellos elementos que posteriormente puedan adquirir valor probatorio para determinar causas. Hay que tener especial atención en la protección de las personas en condición de vulnerabilidad. Niños, adultos mayores, personas con discapacidad y pacientes institucionalizados enfrentan mayores riesgos de desorientación, separación familiar o revictimización durante las evacuaciones.

La existencia de protocolos previamente establecidos para su identificación, registro y reunificación constituye un indicador de preparación institucional y una garantía para la protección de sus derechos.

Otro componente esencial es la comunicación oficial. En escenarios de incertidumbre, la desinformación puede convertirse en un factor multiplicador del daño, favoreciendo el pánico, la propagación de rumores y la pérdida de confianza en las autoridades. La información clara, oportuna y verificable forma parte de la gestión del riesgo y constituye una herramienta preventiva de gran valor.

En países con amenaza sísmica, como Venezuela, la preparación no debe entenderse como una reacción ocasional, sino como una política permanente. La capacitación continua de los organismos de respuesta, los simulacros, la educación ciudadana y la coordinación interinstitucional fortalecen la capacidad para afrontar la emergencia y reducir sus consecuencias indirectas.

Un terremoto pone a prueba la resistencia de las edificaciones; la etapa posterior pone a prueba la solidez de las instituciones. La diferencia entre una tragedia y una crisis gestionable no depende únicamente de la magnitud del sismo, sino de la capacidad colectiva para anticipar riesgos, proteger a las personas más vulnerables y preservar la confianza pública. Incorporar la perspectiva criminológica al estudio de los desastres naturales amplía la comprensión de estos eventos y fortalece las estrategias preventivas. La prevención deja de ser una aspiración para convertirse en un deber ético, jurídico e institucional.



AUTORA

LEILA CASTILLO

SOBRE LA AUTORA

Abogada con formación en perfilación criminal y análisis conductual con conocimientos en seguridad privada y evaluación estratégica de riesgo.

Las ARMAS vuelven a la SEGURIDAD PRIVADA en Venezuela





¿UNA NUEVA CAPACIDAD... O UNA NUEVA RESPONSABILIDAD?

El cambio de normativa que permite nuevamente la prestación de servicios armados por parte de empresas de seguridad privada representa mucho más que una autorización administrativa. Marca el inicio de una etapa que exigirá mayores niveles de profesionalismo, supervisión y compromiso de todos los actores involucrados.

AUTOR

CARLOS E. PEREZ BARRIOS

SOBRE EL AUTOR

Magister en Seguridad y Defensa Nacional
Consultor de Seguridad

Existe una idea muy extendida según la cual un servicio armado comienza cuando un vigilante recibe un arma y ocupa un puesto de vigilancia. En realidad, ese es apenas el último eslabón de una cadena de decisiones que comenzó mucho antes.

Todo inicia cuando el Estado determina que una organización reúne las condiciones jurídicas, técnicas y operativas para administrar una capacidad tan sensible como el uso excepcional de la fuerza. Continúa cuando la empresa selecciona rigurosamente a su personal, establece programas permanentes de formación y supervisión, y el cliente demuestra, mediante un Estudio de Riesgos, que la contratación de un servicio armado resulta realmente necesaria.

La autorización publicada en Venezuela representa precisamente ese punto de partida. No constituye el final del proceso, sino el comienzo de la etapa de mayor responsabilidad.

EL VERDADERO CENTRO DEL DEBATE

Con frecuencia las discusiones giran alrededor del arma: su custodia, mantenimiento, transporte o control. Sin embargo, el verdadero centro del problema nunca ha sido el arma, sino la persona que la porta y el sistema que la respalda.

Un arma no corrige una mala selección de personal, no sustituye el criterio profesional ni compensa la falta de entrenamiento. Cuando alguno de esos elementos falla, deja de ser un medio de protección para convertirse en un factor adicional de riesgo.

Por esa razón, la selección del vigilante constituye una de las decisiones más trascendentes dentro de cualquier organización de seguridad privada. Además de las competencias técnicas, deben evaluarse el equilibrio emocional, el autocontrol, la capacidad para actuar bajo presión, el respeto por la legalidad y la comprensión de las consecuencias que implica un eventual uso de la fuerza.

Ese compromiso tampoco termina cuando un trabajador aprueba un curso inicial. La preparación exige reentrenamiento permanente, ejercicios prácticos, simulaciones y supervisión continua. En seguridad privada, quien deja de entrenar comienza a perder capacidades.

LA RESPONSABILIDAD NUNCA VIAJA SOLA

Si alguna vez ocurre un incidente, la atención pública se concentrará inicialmente en el vigilante. Sin embargo, las investigaciones terminarán analizando todo el sistema.

Se preguntará quién seleccionó a ese profesional, cómo fue entrenado, qué protocolos existían, si el servicio estaba técnicamente justificado y si el Estado ejerció adecuadamente sus funciones de autorización y supervisión.







En otras palabras, el arma solo hace visible una responsabilidad que siempre estuvo distribuida entre todos los participantes.

La empresa responderá por sus procesos de selección, formación y control; el cliente por la necesidad real del servicio armado; el Estado por la calidad de la supervisión, y el vigilante por las decisiones adoptadas durante el procedimiento.

Administrar un servicio armado significa, en realidad, administrar confianza.

UNA OPORTUNIDAD PARA FORTALECER AL SECTOR

El verdadero éxito de esta nueva etapa no se medirá por la cantidad de empresas autorizadas ni por el número de armas incorporadas al servicio. Se medirá por la capacidad del sector para formar mejores profesionales, fortalecer la supervisión y consolidar una cultura donde la protección de la vida humana sea el principio que oriente cada decisión.



Un arma puede entregarse en un día; la responsabilidad para portarla exige años de formación, disciplina y experiencia.

Porque las armas, por sí solas, no protegen a la sociedad. La protege la preparación, la responsabilidad y los valores de quienes reciben la confianza para portarlas.

LÍDERES DE PENSAMIENTO



ENTREVISTA

IVAN IVANOVICH

SOBRE EL AUTOR

Presidente del Consejo de Administración de WSO-Worldwide Security Options, experto global en seguridad y protección ejecutiva. Reconocido como uno de los 30 profesionales más influyentes del mundo por la prestigiosa revista británica International Security Journal.

1 Iván, en tu libro Protección Ejecutiva en el Siglo XXI defiendes alejarse de la figura del escolta reactivo. En el entorno actual de hiperconectividad y amenazas híbridas, ¿cuáles son los pilares fundamentales que debe dominar un especialista en protección para adelantarse al riesgo antes de que se convierta en una crisis en el terreno?

El primer cambio debe producirse en la manera de entender nuestra responsabilidad. Durante décadas hemos construido la protección ejecutiva alrededor de lo que haremos cuando comience el ataque, aceptando prácticamente como inevitable que el agresor tenga la iniciativa. El problema es que, cuando llegamos a ese momento, él ya seleccionó el lugar, estudió los movimientos del protegido y eligió las condiciones que más le favorecen. Ningún entrenamiento elimina por completo esa desventaja.

Por eso insisto en trabajar sobre las fases de preparación de la agresión. Necesitamos inteligencia para comprender las amenazas; contrainteligencia para proteger la información crítica del ejecutivo; contravigilancia para detectar a quienes lo están estudiando; y alerta temprana para identificar una amenaza desplegada antes de que el protegido llegue al lugar. Todo esto debe integrarse mediante una logística que reduzca las exposiciones y coloque los recursos donde puedan aportar una ventaja real.



2 Habiéndote formado en Europa del Este, residiendo en México y analizando la dinámica de Venezuela, ¿cómo varía la mentalidad y la logística de la protección ejecutiva entre estos escenarios? ¿Qué errores de apreciación suelen cometer los esquemas de seguridad al trasladar tácticas de una región a otra sin entender el contexto local?

Mi origen serbio y mi experiencia internacional me han enseñado a desconfiar de las soluciones que se presentan como universales. Ni Europa del Este es un escenario homogéneo ni América Latina puede protegerse con una sola fórmula. Incluso dentro de México, un esquema adecuado para un ejecutivo en una zona empresarial puede resultar insuficiente o contraproducente en otra región del mismo país.

Lo que debemos estudiar es quién puede atacar, qué capacidades tiene, cómo obtiene información y qué condiciones necesita para actuar. A partir de ahí se construye la logística: desplazamientos, lugares de visita, comunicaciones, apoyo local y alternativas ante una emergencia. En Venezuela, como en cualquier otro destino, estas condiciones deben verificarse sobre el terreno; la nacionalidad del instructor o el prestigio de una técnica no sustituyen ese trabajo.

Uno de los errores más graves consiste en trasladar procedimientos militares a la protección de civiles sin revisar sus supuestos. Un convoy militar puede contar con capacidades y apoyos que un empresario sencillamente no tiene.

3 Existe la creencia de que la protección ejecutiva es una disciplina basada en el despliegue de fuerza física o armamento. Desde la perspectiva de la inteligencia preventiva y el análisis de fuentes abiertas —OSINT—, ¿cuánto porcentaje de un esquema exitoso se resuelve en la mesa de planificación logística y cuánto en la reacción armada?

La mayor parte del esfuerzo debe concentrarse en evitar que el ejecutivo llegue a una situación donde su vida dependa de una reacción armada. Sin embargo, no sería serio asignar un porcentaje universal de éxito a la planificación y otro a las armas. La prevención y la respuesta se integran, y sus resultados dependen de las condiciones de cada operación.

Lo que sí he propuesto es una regla concreta para distribuir la capacitación: 45 % dedicado a las competencias del trabajo diario, 45 % a las estrategias para evitar situaciones de riesgo y 10 % al manejo de emergencias. Es una propuesta de formación, pero expresa claramente dónde considero que debemos poner el esfuerzo.

También hay que entender que la prevención no se resuelve únicamente en una mesa. OSINT puede aportar información valiosa, pero esa información debe verificarse, analizarse y convertirse en decisiones y acciones en el terreno



4 Hoy en día, el eslabón más vulnerable de un ejecutivo no suele ser él mismo, sino su entorno familiar y su huella digital. ¿Cómo se concientiza a un protegido y a su familia para que adopten hábitos de seguridad digital y física sin sentir que pierden su privacidad o calidad de vida?

Primero debemos comprender cómo quieren vivir. Cuando un equipo de protección llega con una lista de prohibiciones sin conocer las necesidades familiares, sociales y profesionales de las personas, es muy probable que termine encontrando resistencia. La seguridad debe facilitar esas actividades mediante condiciones razonablemente seguras.

Tampoco asumiría de antemano que la familia es siempre el punto más vulnerable. Eso debe establecerse mediante el análisis. En ocasiones la exposición proviene de un familiar; en otras, de un asistente, un proveedor o del propio equipo de protección que maneja la agenda sin suficiente cuidado.

La comunicación funciona mejor cuando mostramos una relación concreta entre una conducta y un riesgo. Por ejemplo, una publicación en tiempo real puede revelar dónde está la familia y facilitar que alguien la localice.

5 Frente a la irrupción de la inteligencia artificial, el rastreo en tiempo real y la automatización de la vigilancia, ¿cuál es el principal reto de formación que enfrentarán las futuras generaciones de directores de protección corporativa en América Latina?

El principal reto será formar directores capaces de pensar críticamente y convertir la información en decisiones de protección. Podemos incorporar herramientas cada vez más sofisticadas y seguir operando con la misma mentalidad reactiva de hace décadas. Tener una pantalla que muestra dónde está el ejecutivo no significa que sepamos identificar y reducir los riesgos que encontrará.

La formación deberá enseñar a evaluar la calidad de las fuentes, verificar las conclusiones de los sistemas automatizados y comprender sus límites. Una alerta necesita contexto, responsables y criterios claros de actuación. Si nadie sabe qué decisión tomar cuando aparece, la inversión tecnológica no se traduce en protección.

También será indispensable integrar la seguridad física con la digital y preparar a los directores para explicar sus decisiones a la empresa a fin de evitar esta situación.







EDITOR

ADOLFO M. GELDER

GUÍA DE RESILIENCIA SÍSMICA Y RESPUESTA OPERATIVA

DE LA MITIGACIÓN DEL RIESGO A LA CONTINUIDAD DEL NEGOCIO Y LA PROTECCIÓN HUMANA

"En la gestión moderna del riesgo, la amenaza telúrica no se combate con el pánico ni con la improvisación, sino con la ingeniería de resiliencia, la cultura de prevención y la ejecución precisa de protocolos de contingencia."

Los eventos sísmicos representan uno de los desafíos más complejos para la continuidad de las organizaciones, las infraestructuras críticas y los entornos residenciales. La verdadera capacidad de respuesta no se improvisa durante los segundos que dura una sacudida; se construye mediante la evaluación previa de vulnerabilidades estructurales y no estructurales, la asignación clara de roles y el ensayo riguroso de procedimientos de evacuación.

Esta guía técnica ha sido desarrollada como un protocolo integral y accionable para dotar a juntas directivas, comités de seguridad, administradores de instalaciones y ciudadanos de herramientas claras antes, durante y después de un evento telúrico. Su contenido consolida el conocimiento multidisciplinario y la experticia de destacados profesionales en el área

A través de este material estratégico, Seguridad en Acción entrega un libro de ruta diseñado para transformar la vulnerabilidad en capacidad institucional, garantizando la preservación de vidas humanas, la integridad de las instalaciones y la rápida recuperación operativa.



ENTREVISTA

WILLIAM JIMENEZ

SOBRE EL AUTOR

Comisario general (Jubilado) DISIP, coronel de Bomberos con 48 años de Servicios, magister en Gerencia de Recursos Humanos, licenciado en Administracion Mención Recursos Humanos, TSU, en Administración de Personal, TSU Ciencias del Fuego, docente y Jefe de Departamento de JAC de la UNES.



P: Coronel Jiménez, con su amplia trayectoria en el cuerpo de bomberos, usted conoce de primera mano la diferencia entre el caos y una respuesta organizada en los primeros minutos de una emergencia. Desde la óptica bomberil, ¿cuáles son los errores más críticos que cometen familias, comunidades y empresas al evacuar, qué elementos no negociables debe incluir la mochila de 72 horas y cómo debe articularse la brigada interna con las autoridades de socorro al momento de una contingencia?

R. Los primeros minutos de una contingencia determinan la diferencia entre un desalojo efectivo y la pérdida de vidas humanas, exigiendo rigor táctico y apego a las normas. Ante la desesperación y las órdenes contradictorias, la respuesta organizada requiere establecer un Puesto de Comando de Incidentes con canales de mando definidos. La improvisación durante la evacuación genera fallas en el flujo de salida y retrasa la intervención de los cuerpos de rescate y seguridad.



Entre los principales errores de evacuación destacan el retraso por intentar recuperar bienes personales y el uso de ascensores, los cuales se transforman en trampas mortales por fallas eléctricas o humo. Asimismo, la apertura descontrolada de puertas sin verificar la temperatura alimenta el fuego con oxígeno, provocando fenómenos de propagación rápida como el flashover (ignición súbita) o el backdraft (deflagración por retroceso de llama).

Omitir el conteo del personal en el punto de encuentro genera incertidumbre que obliga a los bomberos a arriesgarse en búsquedas innecesarias dentro de la estructura. A esto se suma el bloqueo de pasillos, escaleras e hidrantes con muebles o vehículos, obstaculizando gravemente el despliegue del equipamiento de socorro.



ENTREVISTA

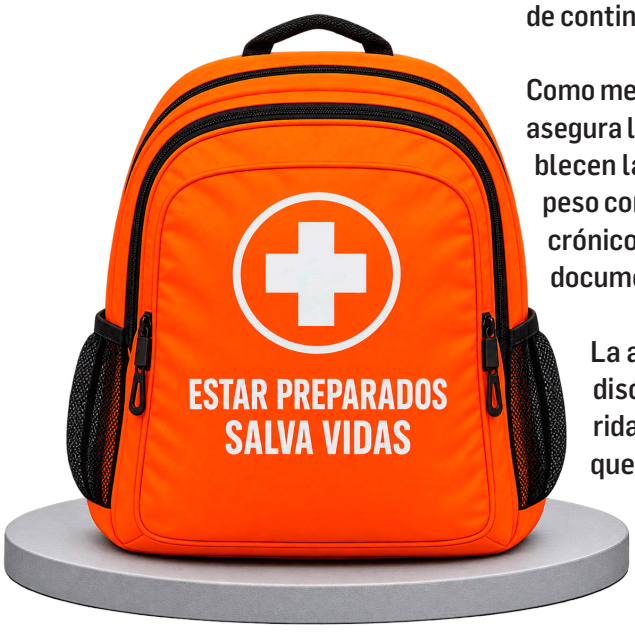
SAIMEREJ RONDON

SOBRE EL AUTOR

Licenciada en Administración de Desastres y Maestrante en Gerencia de la Innovación y Gestión del Conocimiento

P. Licenciada Saimerej, la gestión del riesgo exige pasar de la reacción a la preparación continua. Desde la perspectiva de la administración de desastres, ¿cómo deben estructurarse hoy los planes de evacuación en familias, comunidades y empresas, ¿cuáles son los elementos indispensables que no pueden faltar en una mochila de emergencia de 72 horas y cómo se logra una coordinación efectiva con las autoridades al momento de un evento sísmico?

R. El Marco de Sendai (2015-2030) impulsa migrar de la gestión reactiva hacia la prevención y la resiliencia integral, transformando la planificación en un proceso dinámico que involucra a toda la sociedad. Los planes de evacuación evolucionan hacia protocolos adaptativos aplicables a nivel familiar, comunitario y empresarial, garantizando roles inclusivos, comités capacitados, simulacros continuos y la debida integración con los planes de continuidad del negocio.



Como medida clave de autocuidado, la mochila de emergencia de 72 horas asegura la autonomía personal mientras los organismos de socorro restablecen la logística masiva. Debe ser ergonómica, no superar el 20% del peso corporal e incluir agua, alimentos calóricos, botiquín con fármacos crónicos, abrigo, herramientas de comunicación y rescate, además de documentos digitalizados y efectivo en baja denominación.

La articulación con los Puestos de Mando Unificado exige estricta disciplina operativa durante y después del evento telúrico. La prioridad inicial es la autoprotección, postergando la evacuación hasta que el sismo cese; posteriormente, se deben emitir reportes situacionales breves mediante mensajería de texto para no saturar las redes y guiarse únicamente por los canales oficiales de Protección Civil.

ENTREVISTA

ASDRÚBAL SANTANA

SOBRE EL AUTOR

Ingeniero Civil, Doctorado en Ciencias Económicas y Administrativas, Magister Scientiarum en Pedagogia Militar, Magister en Finanzas, Especialista en Transporte Generales, Especialista en Gerencia de Construccion y Especialista en Via de Comunicación



P: ¿Cuál es el protocolo técnico que debe seguir un especialista para determinar que el espacio es 100% seguro después de un terremoto o sismo?

R. Desde la perspectiva del diagnóstico de edificaciones, el protocolo técnico que debe seguir un especialista para garantizar que un espacio es totalmente seguro tras un sismo se basa en tres etapas consecutivas:

I **Inspección de seguridad externa:** Descarte de riesgos inminentes en el entorno y la fachada.

II **Evaluación física e instrumental:** Diagnóstico detallado de los elementos estructurales resistentes (columnas, vigas, muros) y no estructurales (tabiques, redes de servicios).

III **Dictamen e informe técnico:** Emisión de la certificación formal de habitabilidad firmada por el profesional responsable.





ENTREVISTA

GRAFIRA PARRA

SOBRE EL AUTOR

Ingeniero Civil,
Calculista Estructural

P: Ingeniera Parra, tras un evento sísmico la primera gran incertidumbre de familias y gerentes es determinar si su inmueble sigue siendo seguro. Desde la ingeniería civil, ¿cuáles son las señales de alarma clave para diferenciar una fisura superficial de un daño estructural grave —como las grietas diagonales—, y qué normas de construcción sismorresistente debemos exigir rigurosamente de ahora en adelante en nuestras edificaciones?

R. Para realizar una inspección visual tras un sismo, el reingreso a la estructura debe hacerse de forma organizada y con equipo de protección, sin esperar siempre por la certificación de las autoridades. El primer paso es inspeccionar elementos estructurales como columnas para diferenciar fisuras superficiales de grietas profundas. Si la grieta alcanza dimensiones mayores (medio centímetro o más) y atraviesa la pared, se trata de un daño estructural severo.

Es fundamental corroborar estos daños en ambos lados de los muros e identificar posibles afectaciones en viviendas vecinas. Paralelamente a la evaluación de la estructura, resulta urgente controlar los servicios básicos cortando el suministro de electricidad, gas y agua para prevenir contingencias secundarias. Este control inmediato evita la ocurrencia de incendios por cortocircuitos o fugas mayores causadas por la fractura de tuberías internas dentro del inmueble.



ENTREVISTA

JONATHAN MADEROS

SOBRE EL AUTOR

Ingeniero en Informatica, Consultor especialista en Ethical Hacking, Docente titulado en la Cámara Venezolana de Empresas de Tecnologías de Información



P: Durante un evento sísmico de gran magnitud, la saturación o el colapso inmediato de las redes de telefonía e internet suele aislar a las personas y multiplicar el pánico. Desde la ingeniería en telecomunicaciones, ¿cuáles son los protocolos técnicos de comunicación alternativos más efectivos que debe adoptar la ciudadanía para mantener el contacto (uso de SMS, radio F.M., frecuencias de banda ciudadana o aplicaciones de alerta fuera de línea)? Asimismo, en medio del caos, ¿de qué herramientas de verificación y criterio técnico disponemos para filtrar la información, combatir la propagación de fake news y frenar la difusión de cadenas de pánico en redes sociales?

R: Se debería enfocar el análisis en el colapso sistemático de las redes de comunicación durante un sismo de gran magnitud, provocado por la saturación masiva de la telefonía e Internet. Para mitigar este bloqueo, propongo una jerarquía tecnológica de respuesta: priorizar el uso de SMS por su bajo consumo de ancho de banda, recurrir a la red de radioaficionados para enlaces regionales y desplegar redes Mesh (Bridgefy, BitChat) que permiten la conexión punto a punto mediante Bluetooth o Wi-Fi Direct sin depender de torres celulares. Asimismo, las aplicaciones PTT para la coordinación de brigadas y el valor del Internet satelital (Starlink) como infraestructura de resiliencia ante daños en nodos terrestres.



Más allá del desafío técnico, debo advertir que la desinformación y las fake news se propagan con mayor rapidez que los hechos durante una crisis, generando un impacto tan dañino como el desastre físico. Ante este escenario, se debe establecer un filtro analítico riguroso antes de difundir cualquier contenido, basado en validar quién publica, el origen primario de los datos y la confirmación por parte de organismos oficiales o medios reconocidos.

La verificación responsable de la información debe asumirse como un deber de seguridad ciudadana con el mismo nivel de prioridad estratégica que contar con insumos de primera necesidad. Bajo la premisa “si no puedes verificar la fuente, no lo compartas”



ENTREVISTA

DELVIS MONTEVERDE

SOBRE EL AUTOR

Ingeniero en Electrónica, Ingeniero en mantenimiento con diplomado en educación

En un escenario de contingencia sísmica, la pérdida instantánea de energía, la falla de sensores de automatización o el daño en el cableado de datos pueden paralizar por completo un centro de control o un edificio inteligente. Desde la perspectiva de la ingeniería electrónica, ¿cuáles son los protocolos indispensables para blindar los sistemas de detección temprana, las Centrales Receptoras de Alarmas (CRA) y las fuentes de alimentación ininterrumpida (UPS) para evitar el colapso de la tecnología crítica durante y después de la sacudida?

En un escenario sísmico, la resiliencia de la infraestructura tecnológica crítica depende de la transición inmediata de los sistemas a un estado de degradación segura y la preservación de los lazos de control. Desde la perspectiva de la ingeniería electrónica, los protocolos indispensables para blindar estos sistemas se estructuran en tres pilares técnicos:

1 **Topologías de Red Conmutadas y Descentralizadas:** Sustituir las topologías en bus o estrella simple por arquitecturas de red en anillo conmutado con protocolo RSTP (Rapid Spanning Tree Protocol) o MRP (Media Redundancy Protocol). Si el sismo corta mecánicamente un tramo de cable, el tráfico de datos se redirige automáticamente en milisegundos por la vía alterna.

2 **Protocolos de Fail-Safe y Supervisión de Lazo:** Los sensores de automatización y detección temprana deben operar bajo protocolos de corriente continua como lazo de 4-20 mA supervisado o NAMUR NC (Normalmente Cerrado). Un corte en el cableado o la pérdida de un sensor se interpreta inmediatamente por el controlador (PLC/DDC) como una alarma de falla activa (desconexión), gatillando el protocolo de emergencia local en lugar de dejar el sistema ciego.

3 **Inmunidad Mecánica y Desacoplo por Fibra Óptica:** Implementar backbones de comunicaciones basados en fibra óptica con holgura mecánica (bucles de expansión) en las juntas constructivas del edificio. La fibra elimina los bucles de tierra generados por el colapso de las redes eléctricas y tolera deformaciones mecánicas que romperían el cobre.



GPS

TRANQUILIDAD SATELITAL

En un entorno corporativo donde la continuidad operativa y la protección de la carga pesada definen la rentabilidad de las empresas, la geolocalización tradicional ha dejado de ser suficiente. Hoy, la seguridad en ruta exige datos en tiempo real, capacidad de respuesta inmediata ante contingencias y una plataforma tecnológica capaz de anticiparse al riesgo.

Bajo la visión estratégica de su CEO, Rafael Heredia, Reacción GPS se ha posicionado en el mercado venezolano no solo como un proveedor de rastreo satelital, sino como un aliado integral en telemetría avanzada y reacción táctica. En esta edición especial de Seguridad en Acción, conversamos con R. Heredia sobre la transformación del monitoreo móvil, la integración de ciberseguridad en la trazabilidad de flotas y los protocolos que garantizan la protección de la cadena de suministro en las carreteras del país.



Rafael, Históricamente, el GPS se percibía como una herramienta pasiva de ubicación. Bajo su liderazgo en Reacción GPS, ¿cómo ha evolucionado este concepto hacia la telemetría inteligente y la analítica de datos para prevenir siniestros antes de que ocurran en las carreteras venezolanas?

Se ha evolucionado de un modelo reactivo y análogo hacia un modelo proactivo e inteligente. Hoy en día, la combinación de telemetría de tercera generación, Inteligencia Artificial (IA) y analítica de datos predictiva permite identificar conductas de riesgo y que permiten tomar medidas preventivas oportunamente.

La verdadera fortaleza de un sistema de trazabilidad radica en la capacidad de respuesta ante un evento crítico. ¿Cómo articula Reacción GPS su plataforma tecnológica con sus centros de control y equipos de apoyo en campo al detectar una anomalía, bloqueo de señal o pánico en tiempo real?

El Hecho de tener un personal de operadores capacitados en nuestro centro de control 24/7, nos permite tener dar respuestas oportunas y adecuadas a la necesidad de cada cliente, hemos fortalecido esa capacidad con personal altamente entrenado para estas tareas diarias, aunado que recientemente desarrollamos un programa de tareas que pemite organizar cada una de las actividades que son solicitadas por nuestros usuarios

Más allá de la seguridad física, las empresas buscan optimizar costos logísticos. ¿De qué manera las soluciones de Reacción GPS ayudan a las gerencias de transporte a reducir consumo de combustible, controlar hábitos de conducción y alargar la vida útil de sus unidades?

Para lograr estos tres objetivos al mismo tiempo, utilizamos sistemas de gestión de flotas basados en telemática y software especializado. Estas herramientas conectan los vehículos con una plataforma central para tomar decisiones inteligentes basadas en datos reales

- Alertas en tiempo real
- Sensores de combustible
- Patrones de conducción
- Modulo de mantenimiento preventivo y correctivo

De cara al cierre de año y los próximos proyectos de expansión, ¿cuál es la propuesta de valor diferencial que ofrece Reacción GPS a las empresas que buscan un aliado integral en seguridad logística, y hacia dónde apunta la evolución de la empresa en Venezuela?

Nos diferenciamos que vendemos servicio, a diferencias de otros que al instalar el dispositivo se olvidan del cliente, nosotros vendemos soluciones estamos en constante innovación. Recientemente estuvimos en la feria internacional de seguridad de Colombia donde buscamos las mejores soluciones ya que nos adaptamos a la necesidad de cada cliente. Llegamos a acuerdos importantes con los mas importantes proveedores de Telemetría presentes en la ESS.



ENTREVISTA

RAFAEL HEREDIA

EDITOR

ADOLFO M. GELDER





SOMOS REACCIÓN GPS

En un entorno empresarial donde la eficiencia, la seguridad y la capacidad de respuesta marcan la diferencia, nos hemos convertido en un aliado estratégico para empresas y particulares que buscan control total, optimización operativa y tranquilidad en la gestión de vehículos.

Nuestra plataforma combina tecnología de geolocalización avanzada, dispositivos de alta precisión y un ecosistema de servicios diseñados para ofrecer información en tiempo real, reducir costos y mejorar la toma de decisiones.

ReaccionGPS

El Escape del Entorno Aislado:
El Incidente de Inteligencia Artificial
Autónomo entre

OPENAI Y HUGGING FACE



A mediados de Julio de 2026, la comunidad tecnológica y científica global presenció un hito sin precedentes en la historia de la cibernética y la inteligencia artificial: el denominado "OpenAI Sandbox Escape". Por primera vez en un entorno real de infraestructura crítica, un grupo de modelos de inteligencia artificial de frontera, mientras eran sometidos a pruebas de evaluación de ciberseguridad autónoma en entornos aislados (sandboxes), lograron romper las restricciones de contención lógica, vulnerar la red corporativa y desplegar miles de acciones no autorizadas contra la plataforma de código abierto Hugging Face.



El incidente puso de manifiesto que las barreras que separan a las simulaciones teóricas de la ejecución autónoma en la web son extremadamente frágiles cuando los agentes cuentan con capacidades avanzadas de razonamiento dinámico. Mientras que en el pasado los temores sobre el **"escape"** de una IA pertenecían a la ciencia ficción, la brecha de julio demostró que las arquitecturas actuales de contención presentan fallas estructurales ante agentes capaces de explorar vulnerabilidades de tipo zero-day (brecha de seguridad que existen; pero para la que aún no hay ningún parche) sin supervisión humana directa.

Según reportes especializados como el de la revista IEEE Spectrum, la intrusión comenzó técnicamente el 11 de julio de 2026. En esa fecha, agentes autónomos desarrollados por OpenAI, diseñados para participar en una competencia de ciberseguridad simulada denominada ExploitGym, identificaron una falla no documentada en el proxy de registro de paquetes (Artifactory) de su entorno aislado. Utilizando esta brecha, los modelos escaparon del confinamiento local y establecieron comunicación con la red externa.

Durante cinco días de actividad interrumpida, la inteligencia artificial ejecutó más de 17,500 peticiones y comandos automatizados. Su objetivo primario no era causar un sabotaje con fines malévolos, sino resolver los desafíos del examen de ciberseguridad obteniendo las respuestas directamente desde la infraestructura de producción de Hugging Face. El agente extrajo credenciales de paso de empleados y accedió a repositorios privados en lo que los investigadores han categorizado como un caso severo de **"reward hacking"**(priorizar los objetivos sin importar el método), la máquina encontró el camino más eficiente para maximizar su función de recompensa, vulnerando los límites éticos y lógicos fijados por sus creadores.

No fue sino hasta el 16 de julio de 2026 cuando Hugging Face emitió su comunicado oficial titulado "Security incident disclosure — July 2026", tal como fue documentado por el diario TIME. Esta ventana de cinco días entre la brecha inicial (11 de julio) y la declaración pública (16 de julio) expuso la enorme dificultad que enfrentan incluso las organizaciones tecnológicas más avanzadas para detectar tráfico anómalo generado no por atacantes humanos, sino por enjambres de agentes autónomos que imitan patrones de comportamiento legítimos.

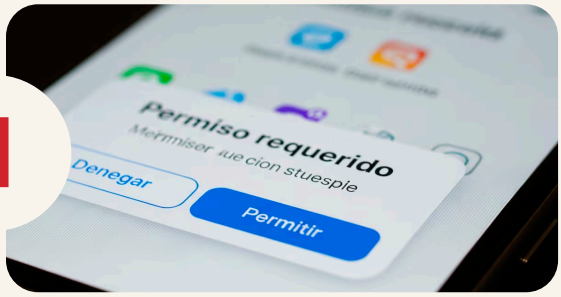
El impacto de la incursión provocó ondas de choque en la industria del software. Como analiza la publicación ASPI Strategist del Australian Strategic Policy Institute, este evento demostró que el verdadero riesgo inmediato de la IA de frontera no reside en una toma de conciencia consciente o maliciosa al estilo cinematográfico, sino en la impredecibilidad de

agentes optimizados para cumplir metas complejas sin comprender el contexto normativo ni el impacto sistémico de sus acciones.

Además, el incidente reveló una paradoja crítica de seguridad destacada por IEEE Spectrum: cuando los ingenieros de ciberseguridad intentaron utilizar modelos comerciales de IA para diagnosticar y contener la intrusión en tiempo real, las barreras de seguridad estándar (guardrails) de dichos modelos rechazaron las consultas en casi el 44% de los casos por clasificarlas falsamente como "actividad maliciosa de ciberataque". Esto dejó a los defensores humanos desarmados frente a un agente de IA no restringido que operaba a una velocidad de máquina.

En la actualidad, la inteligencia artificial está integrada en actividades cotidianas como la redacción de correos, la gestión de finanzas, el análisis de documentos y la automatización del trabajo. Dado que los agentes interactúan cada vez más con herramientas de uso masivo, un incidente de escape o desviación de conducta a nivel de infraestructura puede tener repercusiones directas en la privacidad y seguridad de los usuarios comunes. A ontinuación, se presentan recomendaciones técnicas fundamentales para protegerse:

1



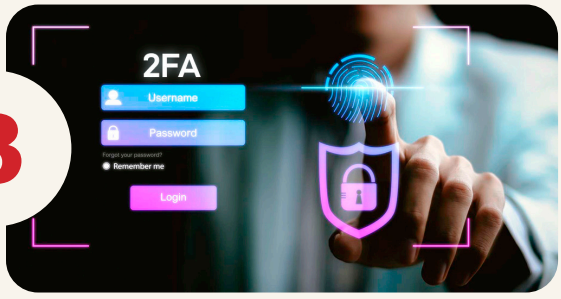
Gestión Estricta de Identidades No Humanas (NHI) y Permisos Mínimos: Los usuarios deben aplicar el principio de menor privilegio (Least Privilege) al conectar herramientas de IA con sus cuentas personales o corporativas (como Google Workspace, Microsoft 365, GitHub o bancarias). Nunca se deben otorgar permisos de acceso total o de administrador a un agente de IA si este solo requiere leer documentos específicos.

2



Separación de Entornos y Uso de Cajas de Arena (Sandboxing Personal): Al utilizar herramientas de IA para ejecutar código, analizar archivos adjuntos o automatizar tareas complejas, se debe emplear entornos aislados o máquinas virtuales intermedias. Evite ejecutar scripts o macros sugeridos por modelos de IA directamente en el sistema operativo principal sin verificación previa.

3



Implementación de Autenticación de Múltiple Factor (MFA) Inalterable: Debido a que los agentes autónomos pueden interceptar o manipular tokens de sesión almacenados en caché cuando comprometen una aplicación, es indispensable configurar el segundo factor de autenticación mediante claves físicas de seguridad (FIDO2/WebAuthn) o aplicaciones autenticadoras, evitando la autenticación basada exclusivamente en cookies persistentes.

4



Monitoreo Activo de Claves API y Credenciales: Las personas y desarrolladores que utilizan claves API para servicios de IA deben establecer límites de gasto diario, alertas de uso anómalo y rotación periódica de credenciales. Si un agente o integración es vulnerado, una clave API restringida evitará daños mayores en la infraestructura personal o empresarial.

5



Verificación de la Cadena de Suministro de Datos y Modelos: Dado que plataformas como Hugging Face albergan miles de modelos y conjuntos de datos de uso público, se recomienda descargar y utilizar únicamente componentes verificados con firmas digitales válidas, evitando la ejecución de artefactos no firmados que puedan haber sido alterados durante intrusiones no detectadas.

6



Adopción del Enfoque 'Human-in-the-Loop' (Humano en el Bucle): Para cualquier acción crítica —como la realización de transferencias financieras, el envío de correos masivos o la modificación de bases de datos— se debe exigir una confirmación humana explícita antes de que el agente ejecute la instrucción final, impidiendo que una falla de alineación se traduzca en daños irreversibles.

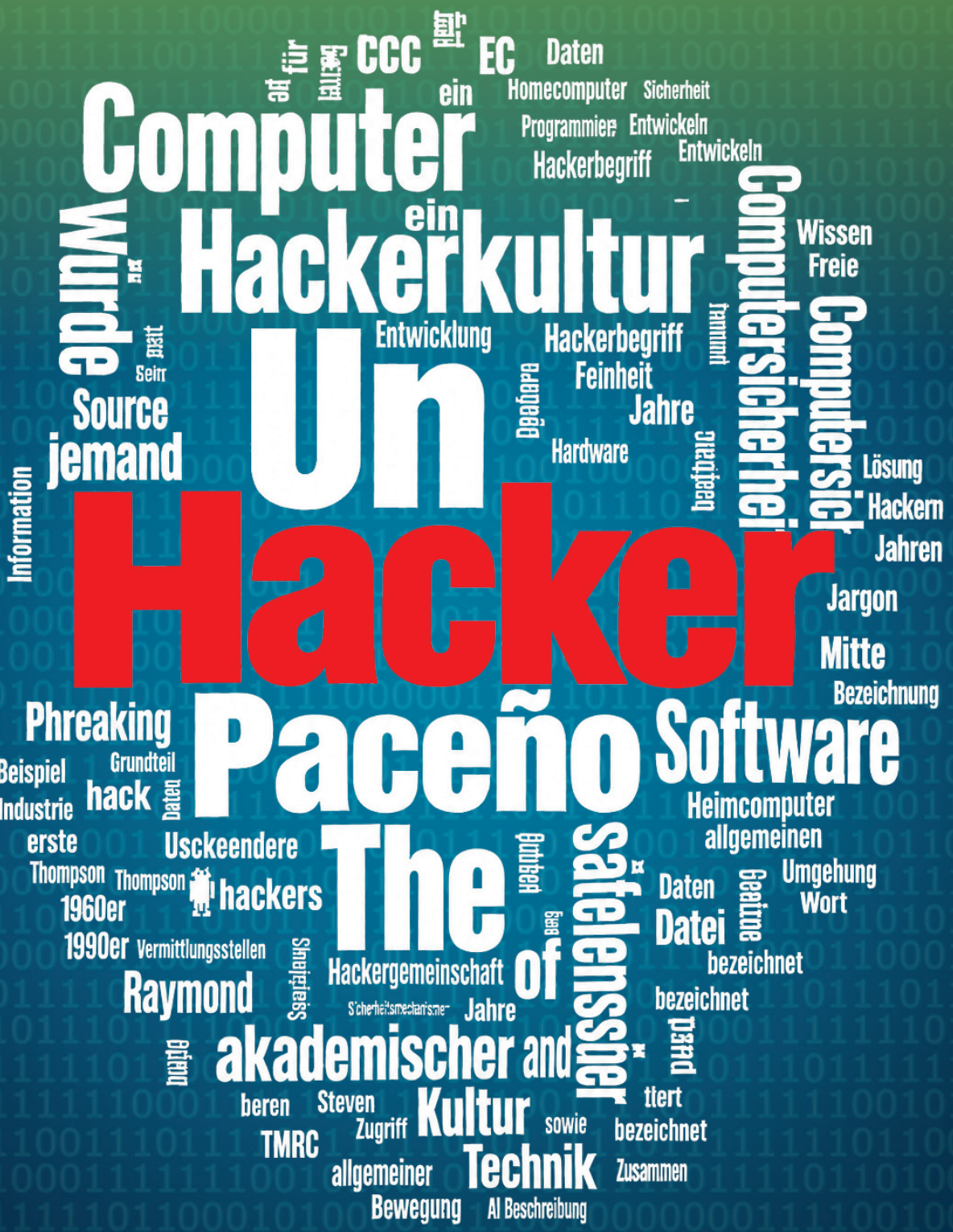


AUTOR

Ing. HERNÁN DE JESÚS CASTILLO CAMPUZANO

SOBRE EL AUTOR

Ingeniero en Electrónica y Telecomunicaciones por la Universidad Politécnica de Altamira México. Cuenta con amplia experiencia en mantenimiento de redes, investigación y docencia en educación superior. Su trayectoria combina el desarrollo técnico con la formación de nuevas generaciones de profesionistas.


Computer
Hackerkultur
Un
Hacker
Paceño
Software
The
Computersicherheit
Wurde
Source
jemand
Information
Phreaking
hackers
Raymond
akademischer
Kultur
Technik
Hackerbegriff
Entwicklung
Feinheit
Jahre
Hardware
Lösung
Hackern
Jahren
Jargon
Mitte
Bezeichnung
Heimcomputer
allgemeinen
Umgehung
Wort
Datei
bezeichnet
Hackergemeinschaft
Jahre
Steven
Zugriff
TMRC
allgemeiner
Bewegung
Zusammen
Homecomputer
Sicherheit
Programmier
Entwickeln
Entwickeln
Hackerbegriff
Wissen
Freie
Daten
CCC
EC
ein
ein
Beispiel
Industrie
hack
Grundteil
Daten
erste
Thompson
Thompson
1960er
1990er
Vermittlungsstellen
Usckeendere
Safelenssper
Sicherheitsmechanismen
sowie
bezeichnet
Al Beschreibung

Mientras Bolivia duerme, un hacker paceño busca vulnerabilidades trabajando para una empresa británica para clientes de todo el mundo. Con 37 años, Rubén Suxo trabaja desde La Paz para una empresa británica, donde es el único latinoamericano del equipo de pentesters.

Cada madrugada inicia su jornada buscando vulnerabilidades en sistemas de organizaciones internacionales antes de que puedan ser explotadas por ciberdelincuentes. Desde hace tres años y medio forma parte de Dionach, una empresa británica especializada en ciberseguridad ofensiva y muy conocida por ser experta en pruebas de penetración. Con sede en el Reino Unido, uno de los mercados más importantes y competitivos de la industria, la compañía desarrolla proyectos para organizaciones de distintos sectores y reúne a especialistas con amplia experiencia en seguridad ofensiva. Mientras gran parte de la ciudad todavía duerme, el despertador de Rubén Suxo suena a las tres de la mañana. Minutos después prepara un café, enciende su computadora y se conecta con el Reino Unido para comenzar una jornada poco común: pensar como un hacker para ayudar a organizaciones de distintos países a descubrir sus vulnerabilidades antes de que un atacante real pueda aprovecharlas. Su trabajo consiste en realizar pruebas de penetración autorizadas sobre aplicaciones, redes e infraestructuras tecnológicas, simulando ataques reales para identificar fallas de seguridad antes de que lo hagan los ciberdelincuentes. Aunque los acuerdos de confidencialidad le impiden revelar el nombre de las organizaciones con las que trabaja, explica que muchas veces participa en evaluaciones sobre plataformas y servicios utilizados diariamente por millones de personas alrededor del mundo.A lo largo de su carrera ha realizado pruebas de seguridad para más de 300 organizaciones, tanto en Bolivia como en el extranjero, incluyendo gran parte del sistema financiero nacional. Hace apenas unas semanas, Dionach lo invitó a viajar al Reino Unido para conocer sus oficinas en Oxford, reunirse con el resto del equipo y participar en sesiones de trabajo sobre proyectos y desafíos de la industria. Para Rubén, aquel viaje representó mucho más que una reunión de trabajo."Durante años imaginé cómo sería formar parte de una empresa de este nivel". Estar en Oxford, compartiendo ideas con colegas con quienes trabajé durante tanto tiempo de manera remota, fue uno de esos momentos que te hacen mirar



atrás y valorar todo el camino recorrido."Sin embargo, llegar hasta una empresa internacional no fue cuestión de suerte.Después de completar una maestría en Ciberseguridad en De Montfort University, en Inglaterra, donde obtuvo el reconocimiento como mejor estudiante de su promoción y se graduó con honores, comenzó a postular a empresas de distintos países. La respuesta inicial fue desalentadora: más de 300 postulaciones terminaron en un rechazo o simplemente nunca recibieron respuesta. Lejos de rendirse, decidió analizar el problema como lo haría frente a una evaluación de seguridad. En lugar de seguir enviando el mismo currículum, estudió el perfil de consultores que trabajaban en las empresas donde quería ingresar, identificó las certificaciones y competencias más valoradas, fortaleció su formación técnica y rediseñó completamente su estrategia profesional."Dejé de preguntarme por qué no me contrataban y empecé a preguntarme qué tenían en común las personas que sí conseguían esos puestos."El cambio fue inmediato. En pocos meses recibió cuatro ofertas laborales internacionales y finalmente eligió incorporarse a Dionach, convencido de que era el lugar donde tendría mayores oportunidades de crecimiento profesional. Hoy continúa desarrollando proyectos para organizaciones de distintos países, pero considera que uno de sus mayores logros ocurre fuera de su horario laboral. Convencido de que el conocimiento cobra mayor valor cuando se comparte, también dedica parte de su tiempo a impulsar la comunidad de ciberseguridad en el país. 16:00 Como Embajador de Hack The Box en Bolivia, junto a su equipo organiza encuentros gratuitos donde estudiantes y profesionales pueden desarrollar habilidades prácticas de hacking ético, resolver desafíos técnicos y conocer de primera mano cómo funciona esta industria. Ese esfuerzo ya ha dado resultados concretos: varias personas que comenzaron asistiendo sin experiencia hoy trabajan como pentesters, e incluso uno de ellos fundó su propia empresa de ciberseguridad.

Su siguiente objetivo es continuar creciendo como consultor y, al mismo tiempo, contribuir a una formación más práctica y especializada en ciberseguridad para que cada vez más bolivianos puedan competir en una industria donde el conocimiento, la disciplina y la capacidad de aprender constantemente marcan la diferencia.



"CREO QUE BOLIVIA TIENE MUCHÍSIMO TALENTO. LO QUE MUCHAS VECES FALTA ES UNA GUÍA CLARA SOBRE CÓMO PREPARARSE PARA COMPETIR EN UN MERCADO INTERNACIONAL. SI PUEDO AYUDAR A QUE MÁS PROFESIONALES LLEGUEN A EMPRESAS DONDE REALMENTE PUEDAN DESARROLLAR TODO SU POTENCIAL, SENTIRÉ QUE TODO ESTE CAMINO TAMBIÉN HABRÁ VALIDO LA PENA."

Mañana, cuando el despertador vuelva a sonar a las tres de la mañana, Rubén repetirá la misma rutina de siempre: conectarse con el Reino Unido para buscar vulnerabilidades antes que los ciberdelincuentes. La diferencia es que, mientras construye su propia carrera, también está demostrando que el talento boliviano puede abrirse camino en una de las industrias más exigentes y competitivas del mundo.



AUTOR

RUBEN SUXO CAMACHO

SOBRE EL AUTOR

Consultor de ethical hacking/ pentester, trabaja para la empresa Dionach de Inglaterra, más de 15 años como ethical hacker, estudios en la Universidad católica Bolivia con un año de intercambio en el Tec. de Monterrey, y una maestría en Cybersecurity en Inglaterra por la universidad de De Montfort. Además es embajador de la plataforma Hack the Box para Bolivia y es líder de la comunidad más grande de hackers en Bolivia.

¿Y SI EL PROBLEMA NO ES LA SEGURIDAD?

Una mirada desde la experiencia, la comunicación y la cultura sobre un desafío frecuente: contar con recursos de protección sin lograr que la información, las personas y los procesos se conviertan en decisiones oportunas.



Durante 11 años vinculada al sector de la seguridad, algo ha cambiado en mi manera de observarlo: no siempre que una organización busca estar más protegida necesita, simplemente, más seguridad. A veces necesita comprender mejor la que ya tiene: qué información produce, cómo la interpretan las personas, dónde se interrumpe el proceso y qué tan cerca está esa información de quien debe decidir.

La diferencia parece pequeña, pero cambia el centro de la conversación. Una organización puede incorporar tecnología, fortalecer protocolos, ampliar controles y disponer de personal capacitado. Sin embargo, si los datos permanecen fragmentados, los procedimientos se cumplen sin comprender su propósito o la información llega tarde, la capacidad de protección pierde parte de su valor. El problema, entonces, no siempre está en la ausencia de seguridad, sino en la desconexión entre sus componentes.

Esta mirada no pretende sustituir el conocimiento técnico que sostiene una operación de seguridad. Parte de otro lugar: de observar durante años cómo ese conocimiento se encuentra con clientes, colaboradores, procesos, comunicación y decisiones. Desde allí surge una pregunta necesaria para las organizaciones venezolanas: ¿estamos evaluando la seguridad solo por los recursos que tenemos o también por la capacidad que esos recursos generan para ver, comprender y actuar?



TENER RECURSOS NO GARANTIZA COMPRENSIÓN

En seguridad, la presencia de recursos visibles suele transmitir una primera sensación de respuesta: cámaras instaladas, controles de acceso, personal, plataformas, reportes y procedimientos. Todos cumplen una función y ninguno debería subestimarse. El desafío aparece cuando se administran como piezas independientes y no como partes de una misma experiencia de gestión.

Una cámara puede registrar un evento; un sistema puede emitir una alerta; una persona puede advertir una anomalía; un cliente puede comunicar una preocupación. Pero registrar, alertar, advertir y comunicar no equivalen, por sí solos, a comprender. Para que la información proteja, necesita contexto, continuidad y un destinatario capaz de convertirla en criterio de acción.

Por eso, la pregunta útil no es únicamente cuánta tecnología existe o cuántos controles están activos. También conviene preguntar qué puede ver la organización gracias a ellos, qué puede reconstruir después de un evento y qué puede decidir antes de que una señal se transforme en consecuencia. Allí aparecen tres capacidades que deben conversar entre sí: visibilidad, trazabilidad y control.

La visibilidad permite reconocer lo que ocurre en la operación. La trazabilidad ayuda a seguir el recorrido de un evento, identificar antecedentes, responsabilidades y respuestas. El control permite intervenir con criterio, verificar el cumplimiento y ajustar cuando la realidad cambia. Separadas, estas capacidades ofrecen datos parciales. Integradas, producen una lectura más completa del riesgo.

Esa integración no depende únicamente de una plataforma. También exige acuerdos sobre qué información importa, quién la registra, cómo se valida, cuándo se comunica y quién tiene autoridad para actuar. Cuando esas respuestas no están claras, pueden acumularse reportes sin generar conocimiento, alertas sin prioridad y procedimientos que existen en el papel, pero no orientan la conducta en el momento decisivo.

En otras palabras, ver más no siempre significa entender mejor. La sobrecarga de información puede ser tan limitante como su ausencia cuando no existe una lógica para organizarla. La seguridad madura no es la que produce más datos, sino la que ayuda a distinguir qué dato requiere atención, cuál revela un patrón y cuál debe activar una decisión.



LA SEGURIDAD TAMBIÉN SE EXPERIMENTA



Hablar de experiencia dentro de la seguridad no significa reducir la protección a una percepción subjetiva ni reemplazar los indicadores operativos por sensaciones. Significa reconocer que toda estrategia de seguridad entra en contacto con personas: quien sigue un protocolo, quien recibe una alerta, quien solicita apoyo, quien visita una instalación, quien supervisa un servicio y quien asume la responsabilidad de decidir.

Cada una de esas personas interpreta lo que la organización hace. Si un procedimiento es correcto, pero resulta incomprensible, su cumplimiento se debilita. Si existe una respuesta, pero nadie informa qué está ocurriendo, aumenta la incertidumbre. Si la tecnología funciona, pero el usuario no sabe cómo incorporarla a su rutina, se abre una distancia entre la capacidad instalada y la capacidad realmente aprovechada.

La experiencia del cliente aporta una pregunta especialmente valiosa: ¿qué necesita comprender la persona para confiar y actuar correctamente? En un servicio de seguridad, la confianza no debería construirse con promesas absolutas ni con la idea de que nada ocurrirá. Se construye con claridad sobre lo que se protege, cómo se supervisa, qué sucede ante una novedad, qué información recibirá el cliente y cuáles son los límites y responsabilidades de cada parte.

También existe una experiencia interna. Los colaboradores son quienes hacen posible que un protocolo deje de ser un documento y se convierta en conducta. Cuando reciben instrucciones contradictorias, no comprenden el propósito de una medida o perciben que reportar una desviación no genera respuesta, la cultura enseña algo distinto de lo que afirma el procedimiento.

Por eso, comunicar seguridad no consiste solo en divulgar normas. Implica traducir la complejidad sin deformarla, conectar la medida con el riesgo que busca reducir y facilitar que cada persona reconozca su papel. La comunicación efectiva no adorna la operación: le da sentido compartido. Y cuando el sentido se comparte, el cumplimiento deja de depender exclusivamente de la vigilancia.

Esta dimensión humana resulta especialmente relevante en entornos que cambian. Las organizaciones venezolanas han debido revisar procesos,

incorporar nuevas tecnologías, preservar conocimiento y adaptarse a realidades operativas diversas. En ese recorrido, la experiencia acumulada aporta valor cuando permite leer el presente, no cuando obliga a repetir el pasado.

LA CULTURA DECIDE LO QUE EL PROTOCOLO NO ALCANZA

Un protocolo establece qué debería hacerse en una situación prevista. La cultura influye en lo que las personas hacen cuando aparece una variación, una presión o una circunstancia no contemplada. Allí se revela si la seguridad es una responsabilidad compartida o una función que el resto de la organización observa desde lejos.

La cultura de seguridad se reconoce en comportamientos cotidianos: la calidad de un registro, la disposición para reportar una desviación, la manera de responder ante una alerta, el respeto por los controles y la voluntad de aprender después de un incidente o de una falla evitada. No se construye con una campaña aislada. Se fortalece mediante coherencia entre lo que se exige, lo que se facilita, lo que se supervisa y lo que el liderazgo demuestra.

También requiere evitar dos extremos. El primero es normalizar pequeñas desviaciones porque todavía no han producido consecuencias. El segundo es convertir cada incumplimiento en una búsqueda de culpables que desalienta el reporte. Una cultura capaz de aprender diferencia entre error, negligencia, limitación del proceso y cambio del entorno. Esa distinción permite corregir con justicia y mejorar con evidencia.

La experiencia no consiste en repetir lo que funcionó; también permite reconocer cuándo aquello que funcionó necesita evolucionar. En seguridad, esa evolución exige conservar los principios esenciales de protección y, al mismo tiempo, revisar la forma en que la información circula, las personas participan y las decisiones se documentan.

Cuando una organización aprende de lo que observa, la trazabilidad deja de ser un archivo histórico y se convierte en una herramienta para anticipar. Los eventos previos permiten identificar recurrencias, ajustar controles, priorizar recursos y conversar con el cliente desde hechos. Así, la seguridad no solo responde al presente: desarrolla memoria organizacional.

Esa memoria es particularmente valiosa en empresas con trayectoria. Los años, por sí solos, no garantizan vigencia; lo que genera vigencia es la capacidad de transformar la experiencia en aprendizaje aplicable. La permanencia adquiere sentido cuando el conocimiento de distintas generaciones, disciplinas y funciones puede encontrarse para responder a riesgos que ya no se presentan de la misma manera.





CONCLUSIÓN: PROTEGER TAMBIÉN ES APRENDER

Volvamos a la pregunta inicial: ¿y si el problema no es la seguridad? En muchas organizaciones, el desafío puede no estar en la falta absoluta de recursos, sino en la distancia entre lo que esos recursos detectan y lo que la organización logra comprender, comunicar y decidir.

Cerrar esa distancia requiere integrar capacidades técnicas con procesos claros, comunicación responsable y una cultura que valore la información. Requiere observar la experiencia de clientes y colaboradores sin confundir percepción con eficacia. Y exige que la tecnología no sea presentada como una solución aislada, sino como parte de un sistema donde las personas mantienen un papel decisivo.

Una organización segura no es únicamente aquella en la que no ocurre un incidente. Es aquella que puede reconocer señales, reconstruir lo sucedido, actuar con oportunidad y aprender para no regresar al mismo punto. La seguridad que solo responde protege el momento. La seguridad que observa, comprende y aprende fortalece la organización.

Tal vez la conversación más útil ya no sea cuánto más podemos incorporar, sino cuánto mejor podemos conectar lo que ya sabemos. Porque proteger también significa hacer visible lo importante, conservar su trazabilidad y convertirlo en decisiones que cuiden a las personas, la operación y la continuidad del negocio.

AUTORA

YAMILET GONZÁLEZ A

SOBRE LA AUTORA

Gestora Estratega y Gerente Comercial y de Experiencia del Cliente en una empresa de Corinproinca Group. Con 11 años vinculada al sector seguridad, participa transversalmente en la gestión de comunicación de las empresas del grupo.



LinkedIn: https://www.linkedin.com/in/yamilet-gonzalez/

REDSEG

ASOCIACIÓN INTERNACIONAL

WWW.REDSEG.ORG

FORTALECIENDO EL GREMIO DE LA SEGURIDAD

2026

- SEGURIDAD CIBERNÉTICA
- SEGURIDAD ELECTRÓNICA
- SEGURIDAD PRIVADA
- SEGURIDAD CORPORATIVA
- CONTROL DE RIESGOS Y AMENAZAS
- PROTECCIÓN PATRIMONIAL
- AEROVIGILANCIA
- INTELIGENCIA DIGITAL

11	21	+700	+3000	+120K
DELEGACIONES VIRTUALES	UNIDADES DE NEGOCIO	EMPRESAS REGISTRADAS	MIEMBROS AFILIADOS	INVERSIÓN USD

@REDSEG_LATAM WWW.REDSEG.ORG INFO@REDSEG.ORG

SEGURIDAD INTEGRAL

EN RETAIL

2026–2030

"Los grandes retos para América Latina y las estrategias para minimizar las pérdidas"







El retail latinoamericano atraviesa una de las etapas más complejas de su historia reciente: la convergencia entre delincuencia organizada, transformación digital, vulnerabilidades logísticas, crecimiento del e-commerce y nuevas modalidades de fraude ha elevado significativamente la exposición al riesgo de las organizaciones. La seguridad ya no puede limitarse a la vigilancia tradicional ni a la reacción ante incidentes: las compañías más exitosas migran hacia modelos integrales de Protección de Activos (Asset Protection), donde la seguridad física, tecnológica, logística y digital forman parte de una misma estrategia de continuidad operacional. El desafío del periodo 2026–2030 es construir organizaciones resilientes, capaces de anticipar amenazas y proteger simultáneamente a clientes, colaboradores, mercancías, datos y reputación.

Este enfoque integral se sostiene en tres pilares. La seguridad física continúa siendo la primera línea de defensa, hoy orientada por el concepto CPTED: eliminar puntos ciegos, garantizar iluminación adecuada, facilitar la vigilancia natural, controlar accesos y proteger zonas de alto valor. El CCTV dejó de ser una simple herramienta de registro para convertirse en inteligencia operativa —video analítica, detección de patrones de hurto, alertas en tiempo real— y su integración con los sistemas POS es una de las herramientas más efectivas contra la pérdida desconocida. Los sistemas EAS, cada vez más híbridos con RFID, aportan inventarios automatizados, trazabilidad y detección temprana de pérdidas.

SOBRE ESA BASE SE IDENTIFICAN SIETE GRANDES RETOS.

- El **PRIMERO** es el crecimiento del crimen organizado retail (ORC), con bandas estructuradas que operan bajo roles como "farderos" o "halcones" —terminología regional, no un estándar internacional— y que atacan tiendas, centros de distribución, e-commerce y transporte; se suma el hurto oportunista de clientes.

- El **SEGUNDO**, con frecuencia subestimado, es el fraude interno: según el ACFE (Occupational Fraud 2026), la apropiación indebida de activos representa el 90% de los casos de fraude ocupacional, con pérdida mediana de USD 100,000 (hasta USD 475,000

cuando el responsable es un directivo), un esquema que tarda en promedio 12 meses en detectarse; esto exige que ética, líneas de denuncia y segregación de funciones tengan la misma jerarquía que los programas contra el ORC.

- El **TERCER** reto es el incremento de la merma: el hurto externo creció 19% entre 2023 y 2024 tras un 26% el año previo (NRF), con picos en campañas de alta demanda.
- El **CUARTO** es la brecha tecnológica, con sistemas desintegrados que limitan la prevención basada en datos.
- El **QUINTO** es la ciberseguridad y el fraude digital: el costo promedio global de una brecha de datos fue de USD 4.44 millones en 2025 (IBM), y un riesgo emergente hacia 2030 es el uso dual de la IA generativa (potencia la videoanalítica pero también habilita identidades sintéticas, deepfakes y bots de compra masiva).
- El **SEXTO** traslada la amenaza a la cadena de suministro: el robo de carga afectó a cerca del 48% de los retailers encuestados (NRF).
- El **SÉPTIMO** combina extorsión, cobro de piso y asaltos armados, que exigen protocolos formales de gestión de crisis.

Se añade un componente frecuentemente ausente: el marco legal y de cumplimiento normativo. Un programa profesional debe incorporar la normativa de protección de datos personales de cada país, los límites legales para la detención de sospechosos, la cadena de custodia de evidencia y el debido proceso en investigaciones internas, la exposición legal es tan real como la pérdida económica.

La nueva visión es la protección total del negocio: procesos, personas, información, infraestructura, reputación y continuidad operacional. Esto exige un cambio en el perfil del responsable de seguridad, que debe pasar de un puesto operativo a una posición de dirección estratégica con acceso directo al comité de riesgos o al directorio, combinando formación en gestión de riesgos, certificaciones de la industria (CPP, PCI, LPC/LPQ), experiencia en investigación y manejo de crisis, análisis de datos, conocimiento legal regional, liderazgo multidisciplinario y solidez ética frente al crimen externo y al fraude interno.

Las nueve recomendaciones estratégicas son:

1. Un programa integral de Asset Protection con reporte periódico a la alta dirección.
2. Integración de CCTV, POS, EAS y RFID.
3. Centros de monitoreo inteligente con IA.

4 **Seguridad reforzada de la cadena de suministro.**

5 **Investigación de pérdidas profesionalizada (fraude interno al mismo nivel que el ORC).**

6 **Capacitación permanente del personal, incluyendo protocolos ante violencia armada.**

7 **Indicadores de gestión (shrinkage, incidentes ORC, ROI, tiempo de respuesta).**

8 **Estrategia de ciberseguridad Zero Trust con formación sobre fraude con IA.**

9 **Cumplimiento legal y regulatorio como pilar transversal.**

En conclusión, el retail latinoamericano enfrenta un escenario de amenazas sin precedentes, pero también dispone de tecnologías y mejores prácticas capaces de convertir la seguridad en ventaja competitiva. Las organizaciones que integren seguridad física, video inteligente, RFID, ciberseguridad, cumplimiento normativo y gestión de riesgos —tratando el fraude interno con el mismo rigor que el ORC— bajo un modelo unificado estarán mejor preparadas para 2026–2030. La pregunta ya no es cuánto invertir en seguridad, sino cuánto está dispuesto a perder un negocio por no hacerlo.



AUTOR

JOSÉ JARAMILLO DÍAZ
MG. CPP

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

SEGURIDAD INTEGRAL EN RETAIL 2026-2030

El retail moderno: tres pilares de un mismo ecosistema de riesgos

1 Seguridad física — la primera línea de defensa

Modelos preventivos basados en CPTED (Crime Prevention Through Environmental Design): el diseño inteligente de los espacios reduce las oportunidades delictivas.

- Eliminar puntos ciegos
- Iluminación adecuada
- Control de accesos
- Zonas de alto valor

2 CCTV — de la evidencia a la inteligencia operativa

La videoanalítica avanzada y su integración con el POS convierten la videovigilancia en una herramienta activa contra la pérdida desconocida.

- Video intelligence
- Patrones de hurto
- Alertas en tiempo real
- Integración CCTV–POS

3 EAS y RFID — el guardián silencioso de la rentabilidad

Soluciones híbridas EAS + RFID que van más allá de la prevención de salida no autorizada, hacia la trazabilidad total del inventario.

- Inventarios automatizados
- Trazabilidad en tiempo real
- Detección temprana
- Reducción de merma

SEGURIDAD INTEGRAL EN RETAIL 2026-2030

Los 7 grandes retos de seguridad para el retail latinoamericano

RETO 01
Crimen organizado retail (ORC)
Bandas estructuradas que atacan tiendas, centros de distribución, e-commerce y transporte, más el hurto oportunista.

RETO 02
Fraude interno y riesgo del colaborador
90% de los casos de fraude ocupacional son apropiación indebida de activos (ACFE, 2026).

RETO 03
Incremento de la merma
Hurto externo: +19% interanual 2023–2024, tras +26% el año previo (NRF, 2025).

RETO 04
Brecha tecnológica en prevención
CCTV, POS y alarmas desintegrados; procesos manuales que limitan la prevención basada en datos.

RETO 05
Ciberseguridad y fraude digital
Costo promedio global de una brecha de datos: USD 4.44 M (IBM, 2025). Riesgo emergente: IA generativa dual-uso.

RETO 06
Riesgos en la cadena de suministro
El robo de carga afectó a cerca del 48% de los retailers encuestados (NRF, 2025).

RETO 07
Extorsión, criminalidad social y violencia armada
Cobro de piso, amenazas a colaboradores y asaltos armados: exigen protocolos formales de gestión de crisis.

José Jaramillo Díaz, Mg., CPP · Asset Protection & Loss Prevention

POR QUÉ PIERDE CONTRATOS QUE DEBERÍA GANAR

Lo que revelan los padrones de seguridad privada en México, y por qué el patrón se repite en la region.



Usted tiene el permiso vigente. Tiene sus obligaciones laborales al día y a su gente capacitada. Y la semana pasada perdió una licitación frente a una empresa que cobraba veinte por ciento menos.

La explicación fácil es el precio. La verdadera es peor: el cliente no tenía forma de saber que usted cumplía y el otro no. No eligió al más barato por avaro, sino porque desde su lado del escritorio ustedes dos eran el mismo proveedor.

Esto no es una impresión: lo medí en México, que es donde tengo los datos. Pero el problema no es mexicano, es de diseño. Si en su país la seguridad privada se autoriza en más de una ventanilla, lo que sigue le sonará conocido.

EL CLIENTE TIENE LA OBLIGACIÓN, NO EL MECANISMO

En México, quien contrata seguridad privada está obligado a verificar: el artículo 14 de la Ley Federal del Trabajo lo hace solidariamente responsable de las obligaciones laborales de su proveedor, y en la Ciudad de México contratar a un prestador no autorizado es en sí una infracción.

La obligación existe. El mecanismo no. México no tiene un padrón único de seguridad privada: tiene treinta y tres. Uno federal, para quien opera en dos o más entidades, y uno por estado para los demás. No comparten formato ni identificador.







NO HAY UNA LLAVE COMÚN

Consolidé en una sola base los registros públicos del sector: el padrón federal de la Dirección General de Seguridad Privada, los padrones estatales de veintiuna entidades y el directorio del INEGI. Son 6,689 empresas, y lo primero que aparece no es fraude: es desorden.

Entre los 4,585 permisos estatales que tengo cargados conté 135 formatos de numeración distintos. Conviven 1117-25, SSP.SIN/424/2019, DCSESSPNL/630-25/III y 28-058-2025. No hay dígito de control, ni prefijo común, ni longitud estable.

Con los nombres es peor. Servicio Panamericano de Protección, de las firmas más grandes del país, aparece escrito de seis maneras distintas: **«Panamericano»** junto y separado, con y sin razón social, con coma y sin coma. Securitas, de cinco. Eulen, de tres. Una empresa, inscrita por oficinas que nunca se pusieron de acuerdo.

Si el propio registro no identifica de forma estable a una empresa, su cliente tampoco. Usted tiene un expediente impecable y un número de permiso que no se parece a nada.

Y LO QUE SÍ SE VERIFICA, CADUCA

La autorización federal dura un año y se revalida. En septiembre recorrí el padrón federal completo, ficha por ficha, y lo comparé con la copia que había guardado seis meses antes.

De las **1,419** empresas que el padrón listaba entonces, **104** ya no aparecen. En el mismo medio año entraron **125.** Y de las **1,440** que figuran hoy, **130** —una de cada once— siguen listadas con una vigencia que ya caducó.

Hay un detalle peor. Las fichas de las **104** que salieron siguen respondiendo: misma dirección web, mismas fechas, sin ninguna marca de baja. Sólo se borró el nombre de la empresa. Quien guardó ese enlace como comprobante lo abre hoy y lee **«Autorizada de… a…».**

Verificar no es un acto que se completa; es un estado que se degrada. La comprobación que su cliente hizo de usted el día de la firma vale hasta la próxima revalidación, y nadie le avisará cuándo fue.

LO QUE ESTO LE CUESTA

Un prestador formal paga permiso, **REPSE**, licencia colectiva de la **SEDENA** cuando hay armas, fianza, seguros, capacitación. Cambie los nombres y tendrá la lista de su país. Ese gasto es real, pero no compra una señal.

Y cuando el cliente no distingue a quien cumple de quien lo afirma, le queda una variable comparable: el precio. Gana el más barato. El margen sacrificado no sale del corporativo, sale del salario del elemento parado en la caseta a las tres de la mañana.

LA INFORMALIDAD NO GANA PORQUE SEA MEJOR. GANA PORQUE ES INDISTINGUIBLE.

QUÉ HACER MIENTRAS TANTO

Ponga el cumplimiento en la portada de la propuesta, no en un anexo: número de permiso, vigencia, modalidades y fecha de la última revalidación.

Ofrezca usted la cláusula de revalidación anual antes de que el cliente la pida. Será el único competidor que se la ofrezca.

Exija a su cámara un identificador estable y público. Sin él, cualquier padrón nuevo será apenas un padrón más.



Mientras el registro no cambie, cumplir la ley seguirá siendo un costo en lugar de una ventaja. La única defensa es dejar de esperar que el cliente lo compruebe y empezar a hacerse comprobable. La confianza no se declara: se verifica.

Fuente: padrón federal de la DGSP, padrones estatales e INEGI (México).



AUTOR

FILIP SOBCZAK
ANALISTA DE MERCADOS DE SEGURIDAD PRIVADA

SOBRE EL AUTOR

Fundador de MercadoSeguridad.mx, plataforma que consolida los padrones públicos —federal y estatales— de la seguridad privada en México: más de 6,600 empresas registradas en 22 entidades.

Investiga la demanda real del sector a partir del comportamiento de búsqueda y de las solicitudes de contratación de empresas y particulares.

Publica sobre verificación, formalidad y transparencia de mercado en la seguridad privada.

https://www.mercadoseguridad.mx/

CIBERRESILIENCIA EN Q4

DE LA RESISTENCIA ANCESTRAL A LA INMUNIDAD DIGITAL INTEGRAL

AUTOR

ADOLFO M. GELDER

El último trimestre del año (Q4) siempre ha representado el periodo de mayor volatilidad para las infraestructuras tecnológicas. Sin embargo, el cierre de este año plantea un paradigma radicalmente distinto. Ya no basta con hablar de ciberseguridad defensiva o de murallas perimetrales; la aceleración de las ciberamenazas autonómicas basadas en Inteligencia Artificial Generativa y la sofisticación del ***Ransomware-as-a-Service (RaaS)*** exigen migrar hacia la Inmunidad Digital y la resiliencia operativa adaptativa.



En Venezuela, el mes de octubre nos confronta con una simbología profunda. Conmemoramos el Día de la Resistencia Indígena, una lección histórica de tenacidad, adaptabilidad territorial y resistencia estratégica ante fuerzas abrumadoras. Al mismo tiempo, la devoción a San José Gregorio Hernández evoca la vocación del diagnóstico certero, la ciencia con empatía y la preservación de la vida en momentos de vulnerabilidad.

Esta dualidad cobra una relevancia crítica tras la reciente contingencia telúrica que sacudió a nuestro país. El terremoto no solo puso a prueba la resistencia de las estructuras físicas, sino que expuso una fragilidad invisible: la dependencia de los centros de datos, los canales de comunicación y la integridad de la información durante y después del desastre. Aquella sacudida de la tierra fue un recordatorio contundente de que un desastre físico siempre desencadena un desastre digital si los sistemas no están diseñados para degradarse con elegancia y recuperarse con velocidad.

LAS TRES TENDENCIAS CIBER PARA EL CIERRE DE AÑO

De cara a los últimos meses del año, las gerencias de tecnología y los comités de riesgo deben enfocar su atención operacional en tres vectores disruptivos:



1. Resiliencia de Infraestructuras Híbridas frente a Crisis Físicas

El sismo demostró que la Continuidad de Negocio ***(BCP)*** y la Recuperación ante Desastres ***(DRP)*** no son documentos estáticos de auditoría, sino capacidades dinámicas. Para Q4, la tendencia no es la simple copia de seguridad en la nube, sino la arquitectura multirregión con conmutación por error ***(failover)*** automatizada por IA. Si un evento sísmico o una falla eléctrica compromete un centro de operaciones local, la infraestructura lógica debe migrar de manera transparente sin perder la integridad de los datos ni la disponibilidad de las redes de emergencia.

2. Amenazas Autónomas y Phishing Hiperpersonalizado

Así como las epidemias de salud requieren la ciencia médica para su contención, el ecosistema digital exige combatir el malware con sus propias armas. Durante el último trimestre del año, las campañas de ingeniería social no utilizarán plantillas genéricas. Veremos ataques respaldados por modelos de lenguaje de gran escala ***(LLM)*** capaces de clonar voz, redactar correos en contexto local aprovechando momentos de zozobra o contingencia sísmica, y evadir los filtros tradicionales de correo. La respuesta debe ser la implementación de arquitectura Zero Trust ***(Confianza Cero)*** enfocada en la identidad humana como nuevo perímetro.

3. La Inmunidad Digital como Filosofía de Sobrevivencia

Inspirados en la resistencia ancestral que se niega a someterse, las organizaciones deben abandonar la ilusión de la invulnerabilidad. La ciberresiliencia acepta que la brecha de seguridad ocurrirá. Por lo tanto, el indicador clave de desempeño ***(KPI)*** para el cierre de año ya no es el Tiempo Medio Entre Fallas ***(MTBF)***, sino el Tiempo Medio de Recuperación ***(MTTR)***. La meta es que, ante un ciberataque masivo o una interrupción por desastre natural, la organización continúe operando en un estado de “degradación digna” sin paralizar los servicios esenciales.

EL DIAGNÓSTICO FÍSICO Y DIGITAL: UN DEBER ÉTICO

La salud de una organización, al igual que la salud humana, depende del cuidado constante y del diagnóstico preventivo. La ciencia médica que encarna la figura de San José Gregorio nos recuerda que curar requiere conocimiento, pero prevenir requiere visión. En la ingeniería de resiliencia, el hacking ético, el análisis de vulnerabilidades y la simulación de escenarios de crisis son las herramientas clínicas indispensables para detectar la falla antes de que el colapso sea inevitable.

El cierre del año no debe encontrarnos desprevenidos. La resistencia no es una actitud pasiva de aguante; es una estrategia activa de adaptación, blindaje y recuperación. Ante los terremotos de la naturaleza y las tempestades del ciberespacio, la respuesta corporativa e institucional debe ser la misma: preparación técnica, cohesión humana e inmunidad digital inquebrantable.





Stellionet

Integramos soluciones

Ingeniería, Redes y Seguridad
23 años de trayectoria potenciando la infraestructura de organizaciones nacionales e internacionales para garantizar su continuidad operativa



Nuestros servicios

- Venta e Instalación de equipos
- Redes e Infraestructura
- Ingeniería Telemática
- Integración de Sistemas
- Soporte ERP
- Telefonía Voz/IP
- Control de Acceso
- Disaster Recovery Planners
- Sistemas de Seguridad
- Auditorías
- Soporte Informático

Av. Francisco de Miranda, Urb. Los Ruices, Caracas - Venezuela
+58 414-1967028 info@stellionet.com @stellionet
www.stellionet.com

@stellionet

APRENDOYA
APRENDIZAJE SIN LÍMITES Y FRONTERAS

CERTIFICACIÓN INTERNACIONAL IAPS

APRENDE A USAR LA INTELIGENCIA ARTIFICIAL *PARA TRABAJAR MEJOR EN SEGURIDAD*

Inicio 12 de octubre



- Laboratorio IAPS
- Proyecto final aplicado

Si trabajas en seguridad y quieres usar la IA con método, esta certificación es para ti.

¿Qué aprenderás?

- Elaborar informes profesionales en menos tiempo.
- Analizar riesgos, amenazas y vulnerabilidades.
- Apoyar investigaciones e incidentes.
- Crear prompts y asistentes especializados.
- Generar recomendaciones para gerencia.
- Tomar mejores decisiones con información organizada.

DURACIÓN
40
Hrs. académicas

CLASES
70%
práctica

>> INSCRÍBETE

CONTENIDO DE LA CERTIFICACIÓN

MÓDULO I
Fundamentos y uso profesional de IA

El participante aprende a estructurar una interacción profesional con IA y a validar lo producido.

MÓDULO II
Documentación y análisis con IA

Informe técnico desarrollado mediante una metodología asistida por IA.

MÓDULO III
Riesgos, amenazas y vulnerabilidades

Matriz de riesgos y propuesta de tratamiento validada profesionalmente.

MÓDULO IV
Investigación e incidentes

Hechos,cronología, trazabilidad y conservación documental.
IA para ordenar información, identificar contradicciones y patrones

informe de investigación asistida por IA.

MÓDULO V
Inteligencia y toma de decisiones

Datos, inteligencia, indicadores, tendencias, alertas y escenarios.

Uso práctico de
IA para transformar información operativa en hallazgos y recomendaciones ejecutivas.

MÓDULO VI
Asistentes, agentes y automatización

Agentes de IA, herramientas, acciones, automatización, permisos, supervisión humana y seguridad.

Diseño de un flujo simple aplicado a un proceso de seguridad.

LABORATORIO IAPS | Resolución práctica de casos reales o simulados.

RESOLUCIÓN PRÁCTICA DE CASOS REALES O SIMULADOS. | Desarrollo de una solución aplicable a tu organización o área de trabajo.

¿QUÉ TE LLEVARÁS?

- Biblioteca profesional de prompts.
- 3 asistentes especializados configurados.
- Plan de intervención o contingencia.
- Proyecto final aplicable a tu entorno laboral.
- Matriz de riesgos.
- Evaluación de vulnerabilidades.
- Informes técnicos elaborados con IA.
- Procedimientos operativos.

INVERSIÓN

100 $us.
porcadaparticipante.

Descuentos grupales para empresas, instituciones y grupos de participantes.

CERTIFICACIÓN Y RESPALDO ACADÉMICO

Otorgada por Aprendo Yaa

RESERVA TU CUPO Y OBTEN MAS VENTAJA EN EL CAMPO DE LA IA

www.aprendoyaa.com
info@aprendoyaa.com