VENEZUELA, DICIEMBRE DE 2025 - AÑO 1 - NÚMERO 1

CON EL RESPALDO DE CORPROJO BOLIVIA

SEGURIDAD EN ACCION VENEZUELA

BAJO LA AMENAZA DE LOS ATAQUES DE HACKERS

Hoy, ninguna empresa es demasiado pequeña para ser objetivo de un ciberataque.

PAG. 10-13

USO Y MANEJO DE LA SELVA DIGITAL

Linkedin, el Elefante de la Selva Digital

PAG. 14-18

VENEZUELA, POSIBLE LABORATORIO PARA NUEVA DOCTRINA GLOBAL?...

PAG. 41-46

INFORMACIÓN PERSONAL - RRHH

¿Cómo mantener estos datos seguros de tu empresa ante amenazas digitales?

PAG. 32-34

Adolfo M. Gelder

PRÓLOGO DEL EDITOR

Con profunda gratitud y sentido de responsabilidad, asumo el honor de ser el editor de la edición venezolana de Seguridad en Acción. Esta publicación, que ya ha echado raíces en otras latitudes como México, llega ahora a nuestro país con la firme intención de convertirse en una herramienta útil, cercana y reflexiva para todos los ciudadanos que enfrentan, día a día, los desafíos de vivir y trabajar en un entorno donde la seguridad —en todas sus formas— se ha vuelto una necesidad urgente y transversal.

En esta edición, nos proponemos abordar los problemas de seguridad que afectan al venezolano desde una mirada integral: desde la seguridad física en espacios públicos y privados, hasta la seguridad laboral en entornos de riesgo, pasando por la cada vez más crítica seguridad informática en un mundo digitalizado. No nos limitaremos a describir los problemas: queremos identificar causas, visibilizar consecuencias y, sobre todo, proponer soluciones prácticas, accesibles y contextualizadas.

Además, incluiremos tópicos de interés que permitan al lector comprender cómo prevenir, anticipar o mitigar situaciones de riesgo. Porque en un país donde muchas veces la información salva vidas, aspiramos a que esta revista sea una guía que ayude a no ser víctima... y a no morir en el intento.

Gracias por acompañarnos en este esfuerzo. Que esta edición sea el inicio de una conversación nacional sobre la seguridad que merecemos.

STAFF

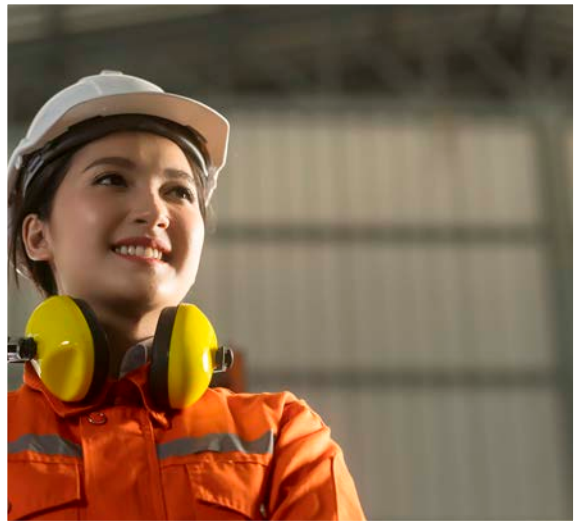
HUMBERTO COPA G.
DIRECTOR GENERAL

LUCIEL RIOS CAMACHO,
COORDINADORA ACADÉMICA Y OPERATIVA

DAVID CORONEL CLAURE
EDICIÓN Y PRENSA

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

CONTENIDO



Cuando la norma también protege:

EL PODER DE LAS COVENIN EN LA SEGURIDAD FÍSICA

POR SAIMEREJ RONDÓN MENDOZA

¿Qué pasaría si la seguridad de tu edificio, tu escuela o tu lugar de trabajo dependiera de decisiones improvisadas? ¿Y si no existiera un marco claro para prevenir robos, sabotajes o actos violentos en espacios públicos y privados? ¿Quién garantiza que las medidas de seguridad que vemos a diario realmente funcionan? ¿Y cómo sabemos si están alineadas con estándares que protegen vidas y no solo infraestructuras?

En Venezuela, esa realidad está cambiando gracias a un esfuerzo técnico y humano que merece ser visibilizado: la construcción de normas COVENIN en materia de seguridad física.

¿Qué está pasando actualmente en el acervo normativo en Venezuela?

Las Normas Venezolanas COVENIN son documentos técnicos elaborados por comités especializados bajo la coordinación de SENCAMER. Establecen requisitos, definiciones y procedimientos que permiten estandarizar prácticas en distintos sectores. En el campo de la seguridad, estas normas son esenciales para garantizar que las medidas implementadas sean eficaces, verificables y sostenibles.

En este contexto, el Subcomité Técnico SC6 – Seguridad Física, reactivado hace dos años, asumió el compromiso de crear y actualizar el acervo normativo venezolano en materia de seguridad física. Su enfoque combina estándares internacionales con una adaptación consciente a la realidad venezolana. Esto permite que los profesionales de seguridad cuenten con herramientas normativas que respondan a los desafíos concretos que enfrentan día a día.

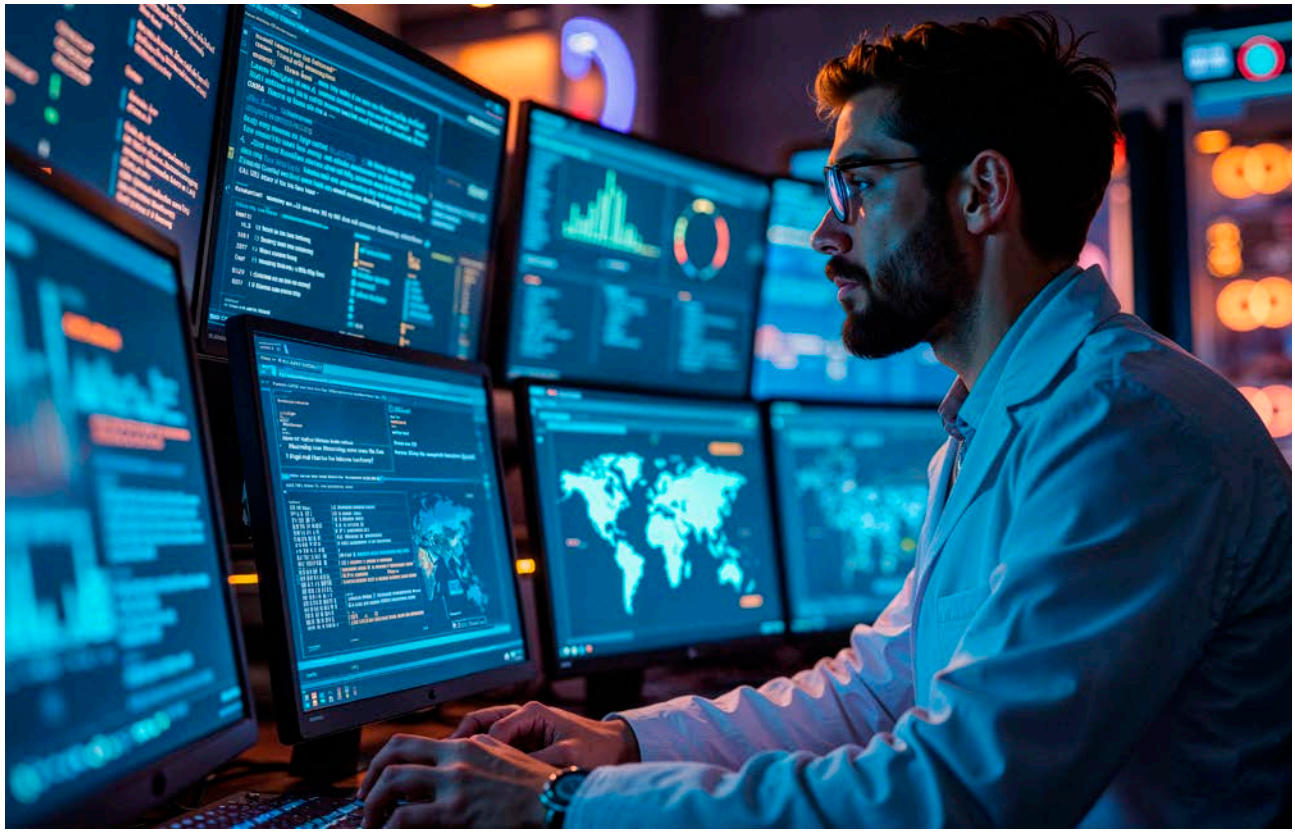
El proceso de reactivación del SC6 comenzó con la elaboración de la Noma Venezolana COVENIN 5043:2025 Planificación de seguridad física en edificaciones e infraestructuras. Requisitos.; una norma que marca el reinicio del trabajo normativo del subcomité, cuya última publicación databa de 1999 (COVENIN 3185:1999 sobre transacciones bancarias). Esta nueva norma, actualmente en fase previa a consulta pública, representa un hito técnico y simbólico para el país.

Desde el Subcomité Técnico de Normalización SC6 – Seguridad Física, un equipo multidisciplinario de más de 30 profesionales ha trabajado intensamente en la elaboración de la Noma Venezolana COVENIN 5043:2025, una norma que establece los requisitos para la planificación de la seguridad física en edificaciones e infraestructuras. Este documento representa un hito para el país: por primera vez se propone un marco normativo nacional que articula prevención, gestión de riesgos y protección de activos en el entorno construido.

La norma se inspira en estándares internacionales como la ISO 31000 (gestión del riesgo), la ISO 18788 (operaciones de seguridad privada) y la ISO 23234 (seguridad en edificaciones), pero con un enfoque adaptado a la realidad venezolana. Su desarrollo ha seguido el ciclo de mejora continua (Ciclo Deming), priorizando la fase de planificación como base para decisiones estratégicas.

Aplica a edificaciones, plantas industriales, infraestructuras públicas y privadas, así como a proyectos en construcción o remodelación.

La Noma Venezolana COVENIN 5043:2025 está estructurada en seis apartados: objeto, alcance, referencias normativas, términos y definiciones, requisitos y bibliografía. Su objeto es establecer los requisitos para la planificación de la seguridad en edificaciones e infraestructuras, orientada a la gestión integral de riesgos y la protección física de los activos en el entorno construido.



¿Por qué importa la COVENIN 5043:2025?

Porque la seguridad no puede depender solo de la intuición o la reacción. Necesitamos reglas claras, procesos verificables y criterios compartidos que orienten tanto a empresas como a instituciones públicas. Las normas Venezolanas COVENIN permiten eso: traducen principios técnicos en acciones concretas, medibles y replicables.

Además, el trabajo del SC6 no es solo técnico: es profundamente humano. Implica escuchar a expertos, víctimas, autoridades y ciudadanos para construir una norma que no sea letra muerta, sino herramienta viva. En un país donde la inseguridad ha sido una constante, contar con una norma como la COVENIN 5043:2025 es un paso hacia la resiliencia.

Porque esta norma no solo organiza procesos técnicos: transforma entornos, empodera comunidades y mejora vidas. Sus beneficios abarcan múltiples dimensiones:

* Sociales: fortalece el tejido comunitario, reduce el miedo al delito, promueve la inclusión y fomenta la participación ciudadana.
* Económicos: aumenta el valor de las propiedades, impulsa inversiones, reduce costos asociados al crimen y estimula el comercio local.
* Ambientales: promueve espacios verdes, reduce la contaminación y mejora la sostenibilidad urbana.
* Tecnológicos: integra sistemas inteligentes de vigilancia, iluminación y gestión urbana.
* Operativos: reduce la incidencia delictiva, mejora la vigilancia natural, optimiza recursos públicos y fortalece la resiliencia ante emergencias.

Además, la norma promueve la participación de todos los actores involucrados en el diseño y gestión de espacios: ciudadanos, autoridades, profesionales del urbanismo y la seguridad. Su enfoque preventivo, basado en los principios de CPTED (Prevención del Delito mediante el Diseño Ambiental), permite anticiparse a los riesgos en lugar de reaccionar ante ellos.

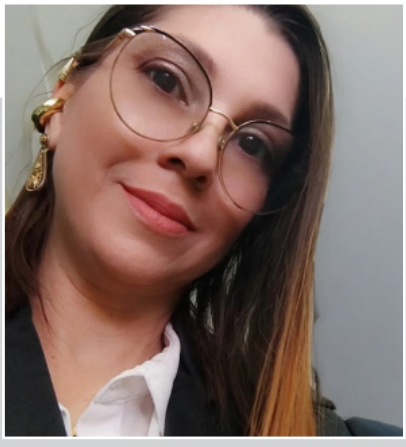
¿QUÉ APORTA ESTA NORMA?

* **Claridad estructural: define requisitos organizativos, técnicos y operativos para planificar la seguridad física.**
* **Aplicabilidad amplia: se adapta a edificaciones, plantas industriales, infraestructuras públicas, proyectos en construcción y más.**
* **Enfoque integral: combina medidas activas (como vigilancia) y pasivas (como diseño ambiental) para prevenir y mitigar riesgos.**
* **Evaluación continua: promueve el uso de indicadores para medir la efectividad de las medidas implementadas.**
* **Adaptabilidad: permite a las organizaciones responder a nuevas amenazas y vulnerabilidades con base en evidencia.**

RECOMENDACIONES

* Acompañar la consulta pública revisando el documento y aportando con la experiencia y conocimiento del profesional de seguridad
* Apoyar el trabajo normativo divulgando la norma una vez publicada, a través de espacios de formación ciudadana.
* Promover su adopción en proyectos públicos y privados como requisito de calidad.
* Fortalecer la articulación entre normas técnicas y políticas públicas de seguridad.

En un país donde muchas veces la seguridad parece un privilegio, esta norma nos recuerda que también puede ser un derecho. Y que detrás de cada artículo técnico, hay un compromiso colectivo por construir entornos más seguros, humanos y sostenibles. Porque cuando la norma protege, también dignifica.



Saimerej Rondón M. es experta en Salud y Seguridad en el Trabajo con formación en Administración de Desastres, Seguridad Integral y estudios de posgrado en Gerencia de la Innovación y Gestión del Conocimiento. Actualmente dirige FUNSEIN, además es docente, tutora e investigadora con múltiples publicaciones, y aporta en comités técnicos de normalización (SENCAMER).

Fraudes en Puntos de Venta

LA AMENAZA SILENCIOSA DEL COMERCIO MODERNO

En la era del comercio híbrido, donde conviven las transacciones físicas y digitales, los Puntos de Venta (POS) se han convertido en un blanco estratégico para los defraudadores.

Aunque muchas empresas han reforzado sus sistemas, los ataques se han sofisticado, mutando desde simples clonaciones de tarjetas hasta complejas redes de fraude digital.

Tipologías de fraude más comunes en POS

- Skimming: Instalación de dispositivos ilegales en terminales para clonar tarjetas. A menudo imperceptibles, estos aparatos capturan la banda magnética y el PIN del cliente.
- Phishing en terminales móviles: En entornos donde se usan POS móviles o tablets, los atacantes pueden suplantar interfaces legítimas para capturar datos.
- Manipulación interna: Empleados coludidos pueden alterar montos, duplicar cargos o registrar datos sensibles.
- Fraude por devolución: Clientes malintencionados simulan devoluciones para obtener dinero sin haber realizado una compra real.

Impacto en las organizaciones

- Pérdidas económicas directas: Desde reembolsos hasta multas por incumplimiento de normativas como PCI DSS.
- Daño reputacional: Un incidente de fraude puede erosionar la confianza del cliente de forma irreversible.
- Carga operativa: Investigar fraudes, revisar cámaras, auditar transacciones y responder a reclamos consume recursos valiosos.

CONCLUSIÓN:

Los fraudes en los Puntos de Venta no son solo un problema técnico, sino una amenaza transversal que involucra tecnología, procesos y personas. La seguridad debe ser proactiva, adaptativa y centrada en la experiencia del cliente. En un entorno donde cada transacción cuenta, proteger el POS es proteger la confianza.

BAJO LA AMENAZA DE LOS ATAQUES DE HACKERS

La opinión popular es la siguiente: ***los hackers y los extorsionistas en primer lugar se interesan por las grandes empresas porque es donde pueden aprovecharse de algo.*** Y las empresas más pequeñas, sobre todo, los usuarios ordinarios, supuestamente no le interesan a nadie.

Pero no siempre es así. En realidad, hoy día cualquier empresa, hasta la más pequeña, puede afrontar a los ciberdelincuentes y como resultado:

- Perder los datos de valor, lo cual puede paralizar todo el negocio,
- Permitir la filtración de los datos personales de clientes, lo cual puede ser un riesgo importante para su renombre,
- Pagar un rescate a los malintencionados por recuperar la información robada o cifrada,
- Perder el tiempo y el dinero para corregir los daños causados por las acciones de hackers.

Cualquier usuario puede ser víctima de un envío phishing masivo o una descarga importuna de software desde una fuente, al parecer, segura. Como, por ejemplo, la aparición del troyano Android.BankBot.Coper, destinado para los usuarios de Colombia. Este malware se difundía a través de Google Play camuflado por software oficial de la entidad de crédito Bancolombia – la aplicación Bancolombia Personas. Para mayor confianza, el icono de la aplicación fue diseñado con el mismo estilo que el software legal del banco. Como resultado, los usuarios que descargaron esta aplicación corrían el riego de introducir sus datos de pago en los formularios falsificados, y de esta forma permitir que los ciberdelincuentes controlen sus cuentas bancarias.

Asimismo, en un caso producido en octubre de 2024 con la filtración de datos de Interbank en Perú. Un ciberdelincuente afirmó haber utilizado credenciales internas para acceder a información sensible de más de tres millones de clientes del banco, que luego fue expuesta. El criminal intentó extorsionar a la entidad, exigiendo una alta suma de dinero para devolver la información extraída.

Para ganar mucho dinero, los hackers tienen que prepararse bastante, hacer investigaciones, gastar dinero para desarrollar troyanos que serán la "clave" para los "candados" especiales de la víctima en cuestión, etc. Pero nadie garantiza ningún resultado en este caso: las corporaciones importantes pueden permitirse no solamente usar los medios protección eficaces, sino también disponer de los departamentos serios de expertos en seguridad informática. Si pasa algo, los mismos saben qué hacer y afrontarán el ataque de forma eficaz.

De esta forma, a los delincuentes les surge una pregunta lógica: ***¿no es más fácil atacar a la presa más pequeña, no protegida de forma predeterminada, concentrándose en la cantidad y no en la calidad?*** Es que se puede infectar con el mismo cifrador 100 PYMES a la vez— o 10 000 usuarios — y demandar un rescate, aunque no sea muy importante, de cada uno de ellos.

Entonces, ¿qué ayudará a afrontar los ataques de hackers? Además de la atención y vigilancia por parte de usuarios durante la navegación en Internet, un antivirus seguro. La solución óptima del problema son los productos de la empresa rusa Doctor Web, cuya línea incluye los medios de protección tanto para el negocio como para el hogar.

Para los PCs Doctor Web ofrece un producto antivirus integral Dr.Web Security Space que protegerá contra cualquier tipo de amenazas en Internet.

¿Cuáles son sus ventajas?

- Impedirá cualquier intento de interceptar Sus datos de pago, no permitirá que se inicien los troyanos bancarios o los programas de extorsión, filtrará los mensajes phishing y no permitirá consultar los sitios web phishing.
- No permitirá a los malintencionados usar las vulnerabilidades en el software, analizará al vuelo el comportamiento de cada aplicación iniciada.
- Protegerá los datos contra la modificación y la eliminación, impedirá el inicio de los troyanos cifradores, detectará los intentos de robar información.
- No permitirá que los ciberdelincuentes conviertan Su equipo en una parte de la botnet, usen sus recursos para obtener la criptomoneda; bloqueará el acceso a la cámara y el micro para evitar supervisión.
- Asegurará Internet siempre limpio para niños, les impedirá consultar los sitios web de contenido peligroso o que puede dañarlos, les ayudará a gestionar su tiempo de uso del equipo de forma más eficaz.
- Protegerá los dispositivos en Android gratis.

Si se requiere proteger solo un dispositivo móvil, existe Dr.Web Security Space para Android. Servirá para la protección de tabletas, smartphones, consolas de juego y televisores "inteligentes" Android TV.

¿Cuáles son sus ventajas?

- Protegerá de forma segura contra todos los tipos de malware "móvil".
- Controlará la actividad en la red de las aplicaciones.
- Protegerá contra las llamadas y mensajes SMS no deseados.
- Restringirá el acceso a los recursos en Internet no deseados.

Hoy, ninguna empresa es demasiado pequeña para ser objetivo de un ciberataque. Los ciberdelincuentes ya no buscan solo grandes corporaciones: apuntan a PYMES y usuarios comunes, menos protegidos, para robar datos, extorsionar, paralizar operaciones y multiplicar sus ganancias atacando en masa. La seguridad tecnológica dejó de ser opcional y se convirtió en una necesidad estratégica para todos.

Para ganar mucho dinero, los hackers tienen que prepararse bastante, hacer investigaciones, gastar dinero para desarrollar troyanos que serán la "clave" para los "candados" especiales de la víctima en cuestión, etc.

- Ayudará a localizar el dispositivo móvil en caso de pérdida o robo del mismo y, en caso necesario, borrar la información privada del mismo de forma remota.
- Realizará un diagnóstico, detectará problemas y ofrecerá soluciones para resolverlos.
- No permitirá a los niños consultar las páginas de Internet no deseadas, bloqueará el acceso a las aplicaciones no requeridas desde el punto de vista de los padres y no permitirá iniciarlas, impedirá cambiar la configuración de restricción establecida.

Y para los usuarios de negocios sirve un conjunto entero de productos — Dr.Web Enterprise Security Suite.

Es una solución única destinada para la protección de todos los nodos de la red corporativa. Además de las posibilidades ya mencionadas, incluidas en los productos de hogar, sus ventajas importantes son las siguientes:

- Administración centralizada y medios de protección de todos los nodos de la red: estaciones de trabajo, servidores, Gateways Internet y dispositivos móviles.
- El perímetro de protección puede incluir no solamente los dispositivos de oficina, sino también los equipos y dispositivos usados por los empleados en casa.
- El Control Parental en el mismo se convierte en el Control de oficina que permite restringir el acceso a los sitios web no deseados para el personal, así como a los datos locales críticos.

Para la información más detallada sobre los productos, consulte el sitio web https://www.drweb.com

Un debido uso y manejo de la

Selva digital

en la Gestión de la Seguridad

Hablemos de la red social Linkedin, el Elefante de la Selva Digital

Las redes sociales con más de 4 mil millones de usuarios activos en todo el mundo, son una herramienta poderosa para los profesionales de la seguridad. Estas permiten construir una marca personal, aumentar la visibilidad de seguidores, interactuar con la comunidad, monitorear actividades y comportamientos, realizar inteligencia y contrainteligencia y otras razones más que pueden contribuir en el desarrollo de una profesión que cada vez exige habilidades y destrezas en ese ámbito tan importante en la actualidad, como lo es el medio digital.

+4.000 millones de usuarios en el mundo

Espacio de interacción, información y riesgo

Herramienta clave para profesionales de seguridad

Los expertos en la materia, la llaman “LA SELVA DIGITAL” y hasta han relacionado a cada una de las redes sociales con importantes protagonistas del reino animal como El Elefante, El Gorila, La Cebra, El Leopardo, El Buho, El Mono y otros más. Basaré este artículo solamente en la plataforma Linkedin, por considerarla una de las más útiles para los profesionales de la seguridad según mi apreciación y exploraremos cómo éstas pueden ser aliadas estratégicas en la gestión de la seguridad, permitiendo una comunicación más rápida y eficaz en los momentos que las necesitemos, ya que existen casos exitosos donde algunas instituciones de seguridad publica privada en el mundo, han utilizado éstas herramientas para mejorar la prevención del delito, gestionando emergencias y fomentando la colaboración entre las comunidades y las autoridades. Además, abordaremos los desafíos asociados, como la desinformación y la privacidad, resaltando la importancia de establecer un enfoque ético en su uso.

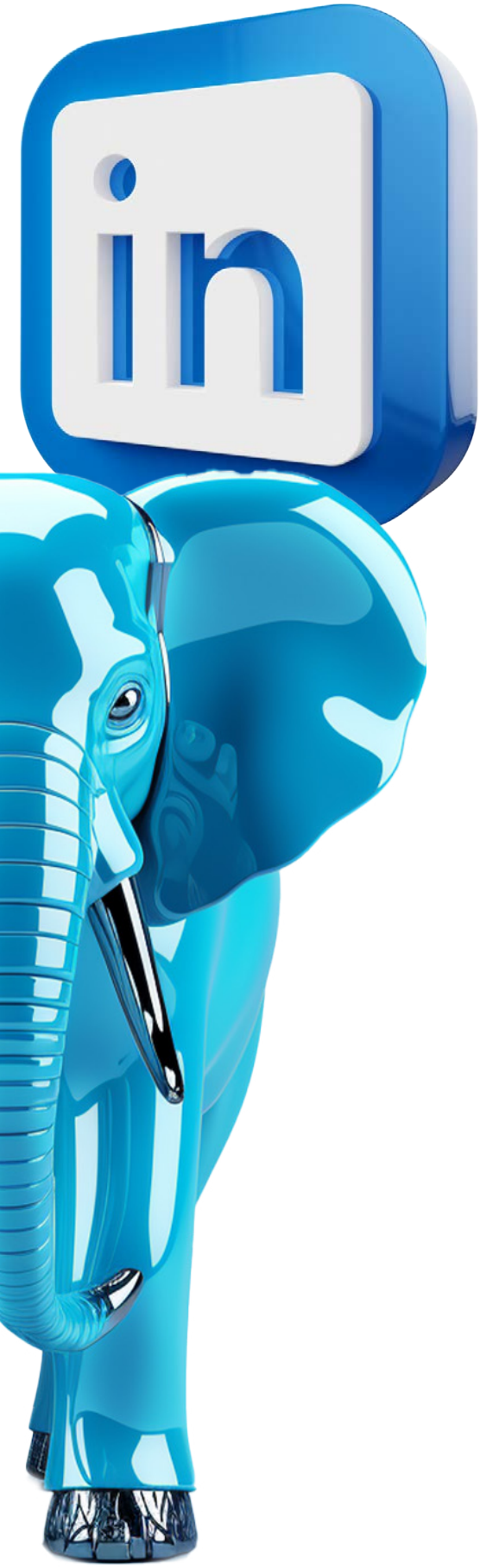
La Selva Digital en Seguridad:

Los expertos en tecnología comparan las redes sociales con una selva de complejo ecosistema, donde cada una de ellas necesitan sobrevivir y destacar y eso resulta ser tan desafiante como navegar por una selva salvaje. Al igual que en una selva natural donde encontramos una multitud de fauna, en las redes sociales tenemos una variedad de formatos de contenido: publicaciones, artículos, infografías, videos, lives, etc. Cada formato tiene su propia forma de captar la atención y de interactuar con los usuarios para destacar y lograr sus objetivos, por eso adaptarte y utilizar estrategias que te permitan sobrevivir y sobresalir, pueden marcar la diferencia entre el éxito y el fracaso, tal como sucede en la selva con los animales que siempre están luchando entre la vida y la muerte. En la selva, cada animal tiene su comportamiento único; algunos cazan en manada, otros son solitarios. De manera similar, los usuarios en las redes sociales pueden ser colaborativos, líderes de opinión, o buscadores de oportunidades discretas y eso dependerá del propósito que cada quien tenga para su uso, de manera que, en la selva digital, cada plataforma es como un hábitat diferente, lleno de diversas especies y comportamientos.

La vegetación = volumen de información

Los animales = plataformas, usuarios y comportamientos

Los caminos = estrategias digitales



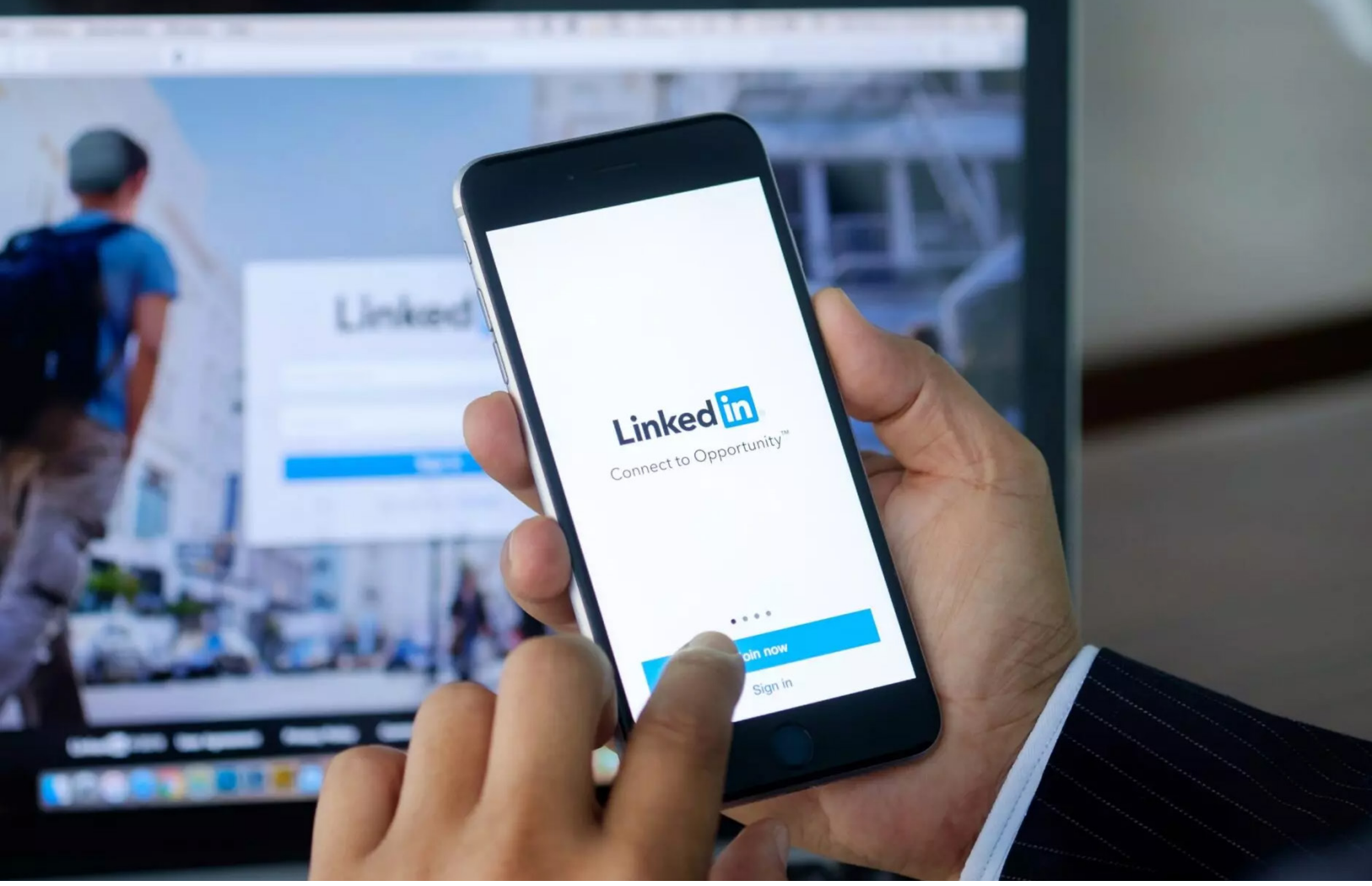
El Elefante de la selva digital y su comparación en características

Linkedin se posiciona como la red social líder donde convergen los líderes empresariales del mundo contemporáneo, similar a la majestuosa figura del elefante, que simboliza atributos esenciales para la excelencia en liderazgo. Una de las características más sorprendentes de las madres elefantes, son fortaleza y resiliencia, especialmente en condiciones adversas como la sequía.

Durante ese periodo crítico, las matriarcales se hacen aún más evidentes, destacando su liderazgo y capacidad de adaptación. Ellas con su extraordinaria memoria utilizan su conocimiento acumulado para guiar a su manada hacia fuentes de agua y alimentos. Su capacidad para recordar lugares de antiguas migraciones y recursos vitales no solo asegura la supervivencia de sus crías, sino que también fortalece la cohesión del grupo, lo que es fundamental en situaciones de escasez. Su fortaleza y resiliencia son realmente inspiradoras para líderes en Seguridad que usan la red social Linkedin como puntas de lanza para promover sus proyectos y empresas.

“La memoria y sabiduría” de un líder son fundamentales; así como los elefantes aprenden del pasado, los profesionales en LinkedIn utilizan la plataforma para recoger y compartir experiencias valiosas, aplicando ese conocimiento para enfrentar desafíos actuales.

Este aprendizaje continuo promueve una visión estratégica que impulsa el crecimiento empresarial. “La fortaleza y resiliencia” son también pilares del liderazgo eficaz. En LinkedIn, los líderes comparten historias de superación, mostrando su capacidad para enfrentar y superar adversidades.



Esta resiliencia infunde confianza en sus equipos, creando un entorno donde cada miembro se siente respaldado y motivado ante las dificultades, además, “la empatía y la sociabilidad” reflejan el espíritu colaborativo de LinkedIn. Al igual que los elefantes, que cuidan y apoyan a su grupo, los profesionales en esta red construyen relaciones sólidas y significativas, fomentando un networking enriquecedor que potencia la colaboración y la innovación. También “la paciencia y estrategia” son cualidades que todo líder debe cultivar. LinkedIn se convierte en un espacio donde se desarrollan y comparten estrategias a largo plazo, permitiendo a los líderes trazar caminos claros hacia sus objetivos, asegurando el uso eficiente de recursos y talentos.

En el caso de la Seguridad con esta red social, podemos darle un uso adecuado en el plano corporativo actual, por ser una red considerada como una herramienta invaluable para la gestión del talento y la seguridad organizacional. Su capacidad para conectar a profesionales de diversos sectores permite a las empresas no solo reclutar talento calificado, sino también identificar y mitigar riesgos asociados a la seguridad interna.

Linkedin se erige como la red donde no solo se vinculan talentos, sino donde se forjan líderes que, como los elefantes, poseen una sólida memoria, resiliencia, empatía, paciencia y autoridad, cualidades que les permiten afrontar el complejo panorama empresarial con éxito y sabiduría.

Para maximizar el uso de LinkedIn en materia de seguridad, las organizaciones pueden implementar estrategias como identificación de Perfiles Relevantes utilizando las funciones avanzadas de búsqueda y allí se pueden filtrar los candidatos según habilidades específicas, experiencia en seguridad y formación académica. Esto facilita la detección de perfiles que no solo cumplen con los requisitos del puesto, sino que también aportan una visión crítica hacia la gestión de riesgos.

Asimismo, para la verificación de Credenciales, LinkedIn ofrece la posibilidad de revisar las recomendaciones y las interacciones pasadas de un candidato. Este aspecto permite a los reclutadores evaluar la reputación profesional de los postulantes y validar sus experiencias, lo que es esencial para garantizar un entorno de trabajo seguro, además de facilitar la creación de redes profesionales, donde se pueden establecer conexiones con expertos en seguridad y otros sectores relevantes.

Las referencias cruzadas y las recomendaciones dentro de estas redes apoyan a las empresas en la toma de decisiones informadas sobre posibles contrataciones y realizarles un constante monitoreo de sus actividades, siguiendo el contenido compartido por profesionales clave en el campo de la seguridad, con el objeto de mantenernos actualizados sobre las mejores prácticas y alertarnos sobre nuevas amenazas o perfiles falsos cuando les realizamos el debido seguimiento.

Por último, considero que una presencia activa y transparente en esta red social, contribuye a fortalecer la marca empleadora de la organización, atrayendo a profesionales de alto calibre interesados en un entorno de trabajo que valore la seguridad y el desarrollo continuo.

Nuestra responsabilidad como profesionales de la seguridad, es contribuir con las autoridades competentes, cuando detectemos perfiles que luego de hacerles el debido trabajo de inteligencia en las redes sociales nos percatemos que se trata de perfiles falsos, para evitar estafas u otros delitos establecidos.

Amplia trayectoria profesional

International Security Alliance USA (INSEAL) Texas - Houston, USA

Autor:
Dicxon Ruiz Quintana

Director de Operaciones de INSEAL-USA, 14/11/2025

TSU en Seguridad Pública.

Especialidad en:

SGM (R) Guardia Nacional de Venezuela v Seguridad y Orden Público.

Seguridad en la Cadena de Suministros.

Seguridad Física e Integral. v Gestión de Liderazgo. y Seguridad en Centros Penitenciarios.

Desarrollo y Gestión Equipos de Seguridad.

Autor del libro titulado “HABLÓ EL SARGENTO MAYOR... Ante los antivalores de la humanidad”

BLINDA TU PYME:
MÁS SEGURIDAD, MEJORES FINANZAS OPERACIONES EFICIENTES

Transformamos tu riesgo en crecimiento
Estrategia, Ciberseguridad y Rentabilidad

Finanzas

Organización y control para tu tesorería

Ciberseguridad

Protección avanzada contra amenazas digitales

Organización y Métodos

Procesos eficientes y reducción de riesgos internos

S&S
Consultores Corporativos

S&S CONSULTORES CORPORATIVOS

Agenda tu auditoria de seguridad informática gratuita

DICIEMBRE

un mes de Prevención

Seguridad laboral, patrimonial y digital en fiestas

Por tradición las festividades navideñas son el concurso de variables importantes en el marco de la seguridad, por ello no debemos descuidar, intensificando medidas preventivas; la prevención es me mejor mecanismo de.minimizar eventos en esta época de disfrute

Prevención de Riesgos Laborales (PRL)

El aumento de la actividad, las distracciones por las fiestas y la presencia de decoración navideña incrementan el riesgo de accidentes.

Riesgo por Decoración y Electricidad

Verificar que las luces navideñas sean de bajo consumo (LED) y certificadas, sin cables rotos.

Evitar la sobrecarga de tomas y extensiones eléctricas.

Asegurarse de que el árbol y adornos no obstruyan pasillos, rutas de evacuación o señaléticas de seguridad.

Usar herramientas y escaleras adecuadas para la instalación de adornos en altura.

Riesgo por Distracción y Fatiga

Hacer charlas o dinámicas de 5 minutos para recordar la importancia de la concentración (“Mente y ojos en la tarea”).

Fomentar la gestión de la fatiga en empleados con jornadas extensas (Ej: logística, ventas).

Asegurar que los trabajadores eventuales o recién contratados reciban la capacitación de seguridad adecuada y el Equipo de Protección Individual (EPI).

Riesgo en Fiestas y Eventos

Hacer campañas de concientización sobre el consumo responsable de alcohol (evitar conducir bajo sus efectos).

Promover el consumo de alimentos saludables para prevenir intoxicaciones alimentarias en eventos corporativos.

Seguridad Patrimonial y Financiera

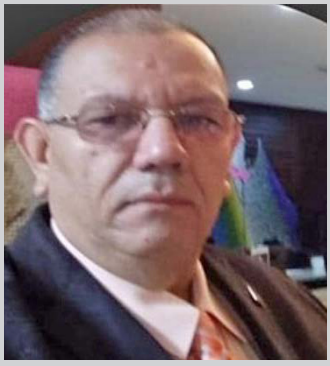
Diciembre es un mes de alto flujo de dinero (utilidades, bonos, aguinaldos), lo que atrae a los delincuentes.

Seguridad Física y Lógica

- Reforzar la vigilancia con personal adicional en puntos críticos.
- Revisar el funcionamiento de alarmas, cámaras y sistemas de acceso.
- Emitir comunicados a los empleados sobre seguridad personal al retirar dinero (preferir transferencias, evitar llevar grandes sumas).
- Prohibir o controlar el acceso a áreas críticas, especialmente durante horarios de baja actividad o vacaciones.

Ciberseguridad (Riesgo Festivo)

- Advertir sobre el phishing o correos electrónicos de fraude que se disfrazan de promociones, regalos o avisos de pago de utilidades.
- Reforzar las políticas de acceso remoto (uso de VPN y autenticación multifactor, MFA) si el personal se conecta desde casa o viajes.
- Asegurar que los sistemas y parches de seguridad estén actualizados antes del periodo de vacaciones del personal de TI.



David Jose Gonzalez Mendez

CONSULTOR DE SEGURIDAD INTEGRAL

Preparación Técnica
Curso para Formación Detective año 1987 (DISIP)
Curso en formación de análisis e inteligencia para Seguridad de Estado (DISIP) año 1988.
Curso de Instrucción sumarial en uso indebido de sustancias Psicotrópicas y Estupefacientes (PTJ División de Drogas).
Curso para formación de Sub/Inspector año 1989 (DISIP).
Diplomado en Gerencia de Seguridad
Asistencia a Conferencias, cursos de Criminologia y criminalística, Actas Policiales derecho penal en el Colegio de Abogados en el Estado Aragua Instituto de Estudios Jurídicos Carlos Taylhardat.
Curso de Contabilidad y auditoria documental (Banco Exterior División de Investigaciones Bancarias).
Taller Internacional de Riesgo Universidad Jose Antonio Páez
Diplomado Gerencia de Proteccion y Seguridad Integral Mención Consultor de Seguridad UCV.
CPO (IFPO) • ID 77038379
Auditor Interno Trinorma ISO Inter. 9001-14001 y 45001.
Seminario de Criminalística de Campo
Experticia Operativa
Dirección General de los Servicio de Inteligencia y Prevención (DISIP).
Policía Técnica Judicial (sumariador) División contra Drogas.
Gerencia de Investigación Banco Internacional, Banco Exterior y FONDOS FIVECA.
Gerencia de Investigaciones de PANAMCO COCACOLA.
Policía Municipal de Girardo Maracay Estado Aragua.
Gerencia de Proteccion Física Empresas Polar.
Gerencia de Seguridad Integral Centro Medico Maracay Estado Aragua.
INTERCON SECURITY SYSTEMS VENEZUELA.

Cuando la Inseguridad no Deja Dormir

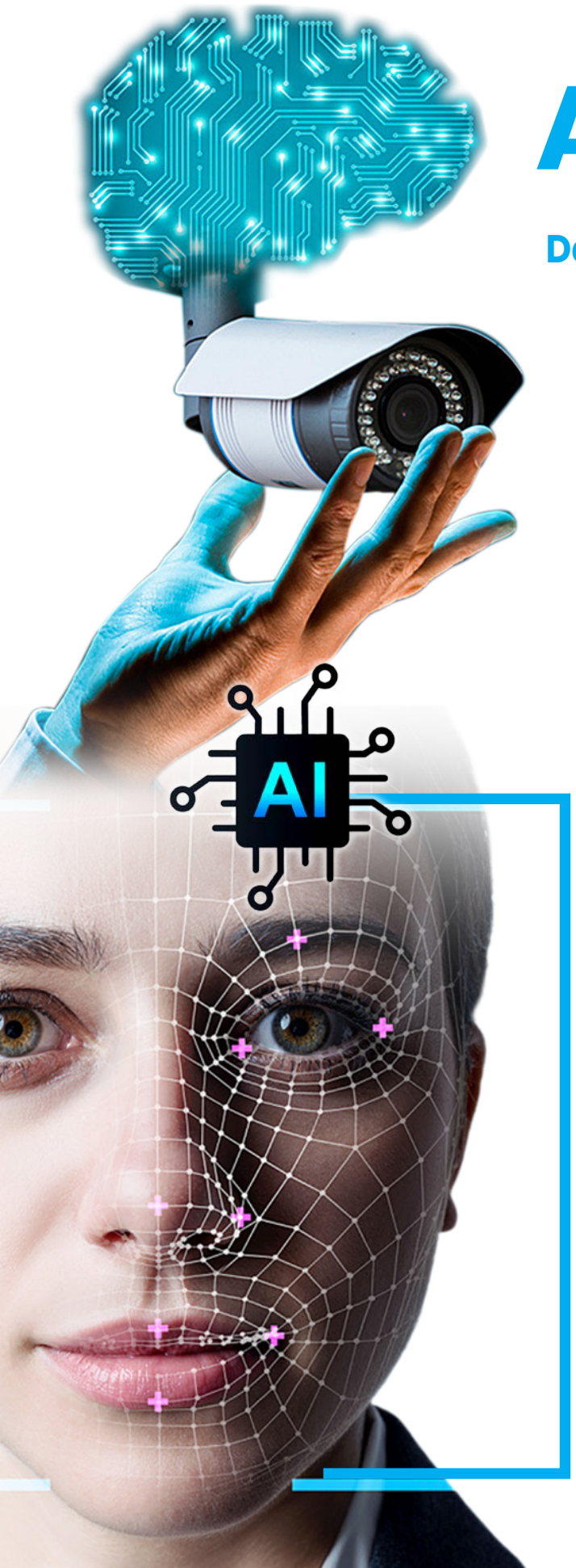
Autor: **Richard Parra.**

La Revolución Silenciosa de la Videovigilancia en las Comunidades Venezolanas

La noche cae sobre la comunidad de El Paraíso en Caracas. Ana, una madre de dos, se despierta sobresaltada por un ruido. No es la primera vez que la inseguridad golpea cerca de su hogar, y cada sombra en la oscuridad reaviva su miedo. Sin embargo, algo ha cambiado. En los postes de electricidad, discretas cámaras CCTV vigilan, y un sistema inteligente analiza los patrones, alertando sobre actividades sospechosas antes de que se conviertan en una amenaza. ¿Es esta la nueva cara de la seguridad en nuestras comunidades?

¿Qué está pasando? El Auge de la Videovigilancia Comunitaria

En los últimos años, ante el incremento de la percepción de inseguridad, numerosas comunidades en Venezuela han tomado la iniciativa de implementar sistemas de videovigilancia por CCTV. Desde condominios en el este de Caracas hasta urbanizaciones en Valencia o Maracaibo, los vecinos se organizan para adquirir e instalar cámaras en puntos estratégicos. Estos sistemas, aunque inicialmente básicos, buscan disuadir el delito y proporcionar evidencia en caso de incidentes. Los datos, aunque no siempre centralizados, sugieren un aumento exponencial en la adopción de estas tecnologías impulsadas por la autogestión y la necesidad de protección. La historia de los robos y la violencia ha llevado a muchos a buscar soluciones tecnológicas.



La Inteligencia Artificial
AL RESCATE

Dando Ojos y Cerebro a la Seguridad

La videovigilancia tradicional, si bien útil, requiere monitoreo humano constante, lo cual es costoso y propenso a errores. Aquí es donde la Inteligencia Artificial (IA) marca la diferencia. La inclusión de la IA en los sistemas CCTV comunitarios permite:

- **Detección de Movimiento Inteligente**: Diferenciar entre un animal callejero y una persona merodeando.
- **Reconocimiento Facial (con precaución y marco legal):** Identificar individuos conocidos o alertar sobre personas en listas de sospechosos (previa autorización legal).
- **Análisis de Comportamiento:** Detectar patrones anómalos, como personas corriendo en pánico, aglomeraciones inusuales o vehículos estacionados por tiempo prolongado en zonas prohibidas.
- **Detección de Objetos Abandonados o Removidos:** Alertar si un paquete es dejado en un lugar inusual o si un objeto de valor desaparece.
- **Alarmas Proactivas:** Generar alertas automáticas a grupos de seguridad vecinal o autoridades ante eventos críticos.

  Esto transforma un simple sistema de grabación en una herramienta de seguridad proactiva e inteligente, capaz de aprender y adaptarse.
- **El Futuro Cercano:** Actualizaciones y Potencial de la IA en Venezuela

Las posibles actualizaciones y mejoras de estos sistemas son vastas y prometedoras, adaptándose a las particularidades de nuestras comunidades:

Integración con otros sistemas: Conexión con alarmas, portones eléctricos e incluso sistemas de iluminación inteligente.

Análisis Predictivo: Basado en el historial de incidentes y patrones de delincuencia, la IA podría predecir zonas y horarios de mayor riesgo.

Cámaras con Visión Multiespectral: Para mejorar la visibilidad en condiciones de baja luz o niebla.

Acceso Remoto y Colaborativo: Plataformas donde los vecinos autorizados puedan acceder a las transmisiones y alertas desde sus dispositivos móviles.

Drones de Vigilancia (regulado): Para áreas más extensas o de difícil acceso, monitoreados y controlados por IA.

Audio Inteligente: Detección de disparos, gritos o rotura de cristales, complementando la vigilancia visual.

Estas innovaciones no solo mejorarán la respuesta ante incidentes, sino que podrían tener un efecto disuasorio mucho mayor. Aquí tienes una visualización de cómo se vería un sistema de videovigilancia inteligente en una comunidad venezolana

Mi Trayectoria en Seguridad Tecnológica

Perfil Profesional

Un profesional con 24 años de trayectoria en el sector de la seguridad tecnológica. Mi especialización principal se centra en el diseño, implementación y gestión de sistemas de CCTV (Circuito Cerrado de Televisión) de alta complejidad.

A lo largo de mi carrera, me he consolidado como un referente en la gestión de proyectos a gran escala con integración de Inteligencia Artificial (IA) y en la gestión de proyectos de seguridad complejos. Mi compromiso es inquebrantable en la optimización de la vigilancia y la protección de activos mediante la implementación de soluciones de vanguardia.

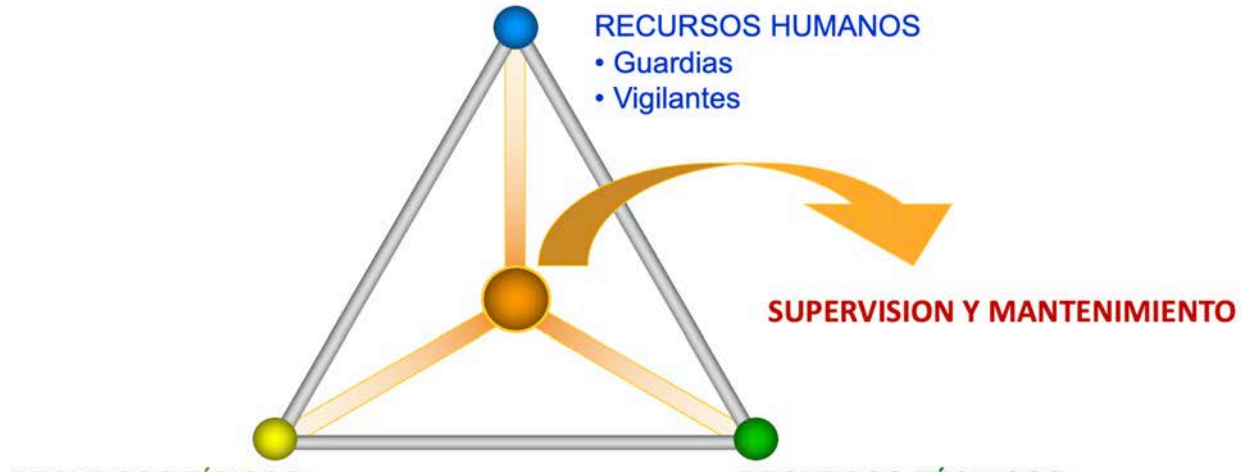
SISTEMATIZACIÓN DE LA SEGURIDAD

Presentado por: **Franklin Rafael Chaparro Rojas**
PRESIDENTE GRUPO SERSECO

Sistematización (Definición)
Es la interpretación crítica de una o varias experiencias que a partir de su ordenamiento y reconstrucción explica la lógica del proceso vivido, los factores que han intervenido y cómo se han relacionado entre sí.

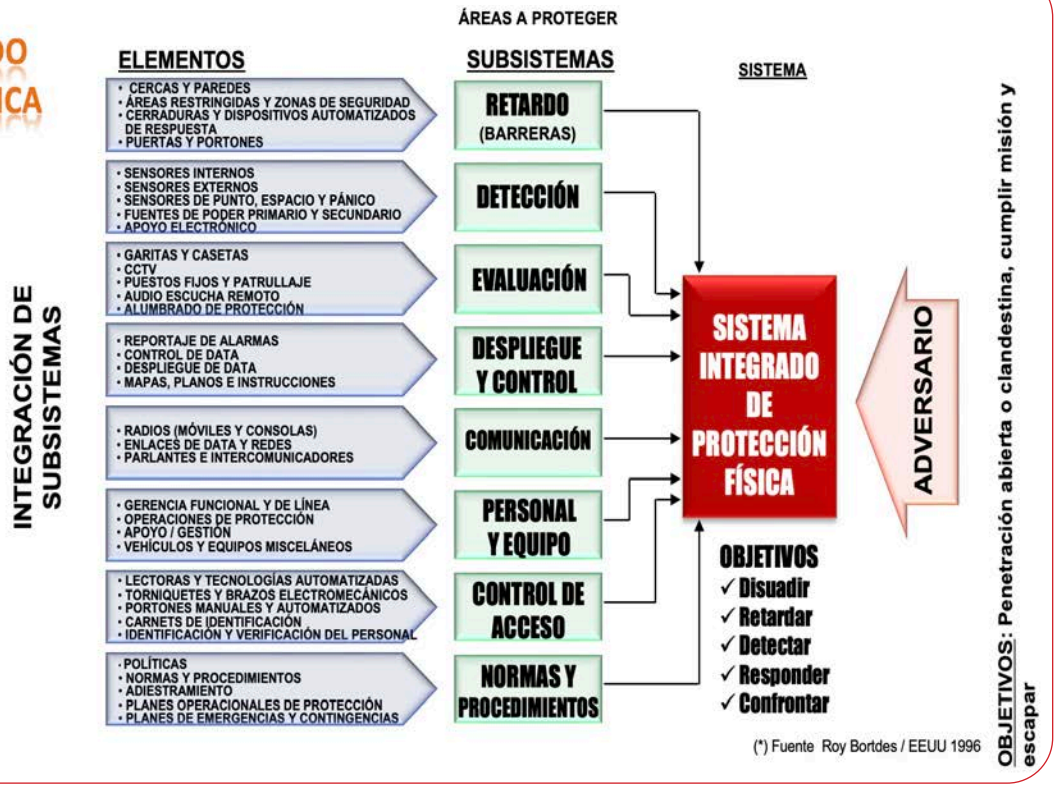
Con la sistematización se pretende ordenar una serie de elementos, pasos, etapas, etc., con el fin de otorgar jerarquías a los diferentes elementos

1. **Definición de los riesgos más relevantes: ¿Contra qué nos vamos a defender?**
2. **Objetivos de Protección: ¿Qué vamos a proteger?**
3. **Evaluar el nivel de tecnología y equipamiento de seguridad: ¿Cómo nos vamos a proteger?**
4. **Evaluar las políticas, planes y normas de seguridad.**
5. **Evaluar las auditorias y controles de seguridad.**
6. **Evaluar cultura y capacidad con temas de seguridad.**
7. **Información, inteligencia y comunicación.**

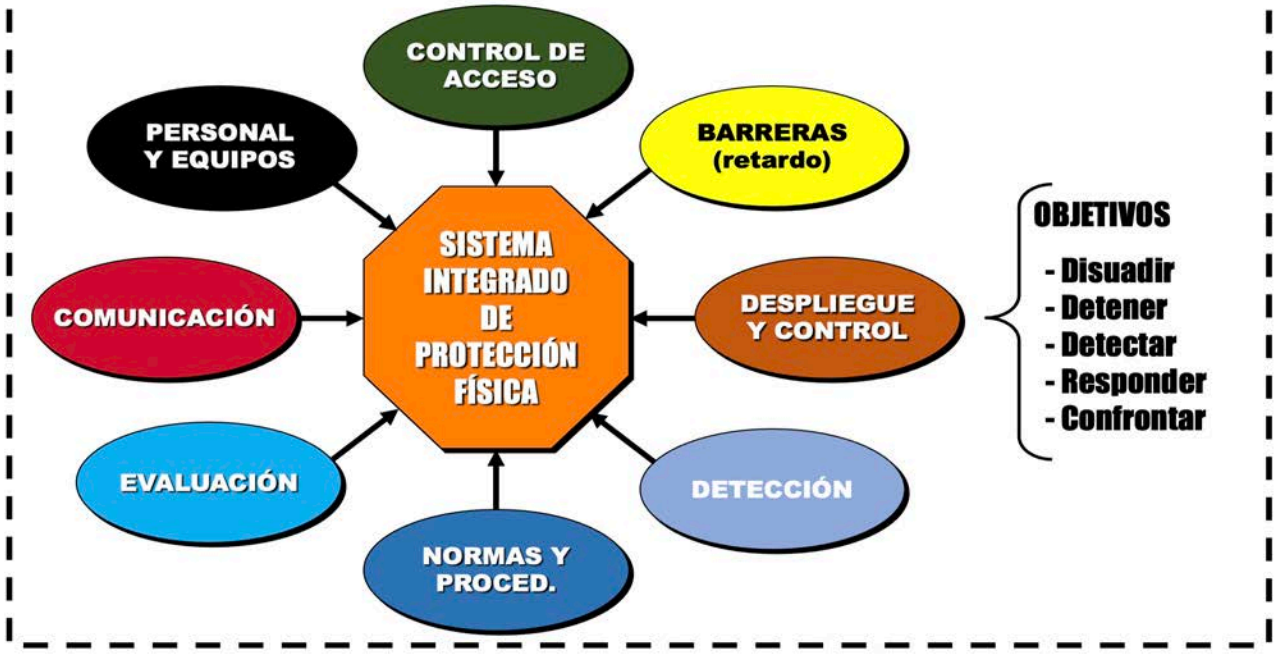

RECURSOS HUMANOS
• Guardias
• Vigilantes
SUPERVISION Y MANTENIMIENTO
RECURSOS FÍSICOS
• Candados
• Cerraduras
• Cercas o Muros
• Concertinas
RECURSOS TÉCNICOS
• Circuito Cerrado de TV
• Alarmas
• Comunicaciones
• Control de Acceso

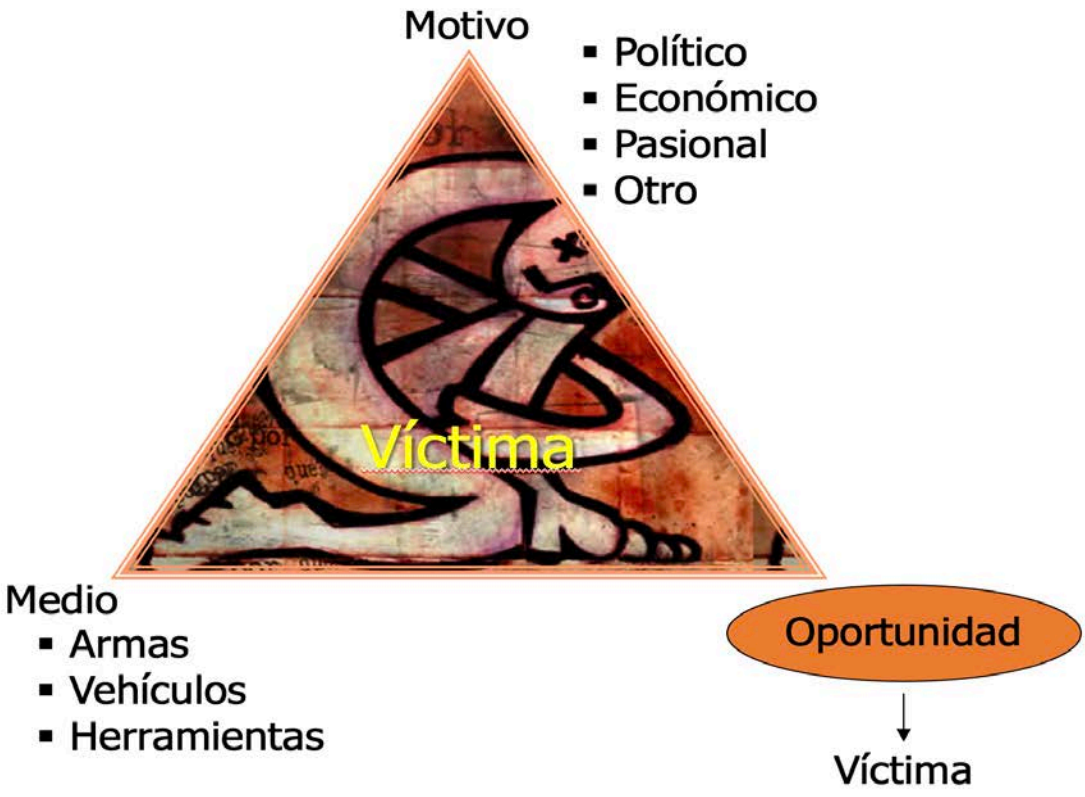

¿De qué nos vamos a proteger?
¿Qué vamos a proteger?
Análisis de Amenaza
Análisis de Vulnerabilidad
Evaluación de Riesgos
Evaluación de Costos
Nivel de Seguridad necesario
¿Cómo nos vamos a proteger?
Recursos Humanos
Recursos Técnicos
Recursos Físicos
Supervisión Adecuada
Perfil y Funcionamiento
Ingeniería de Sistemas
Cerraduras, Rejas y otros
Normas y Coordinación

SISTEMA INTEGRADO DE PROTECCIÓN FÍSICA

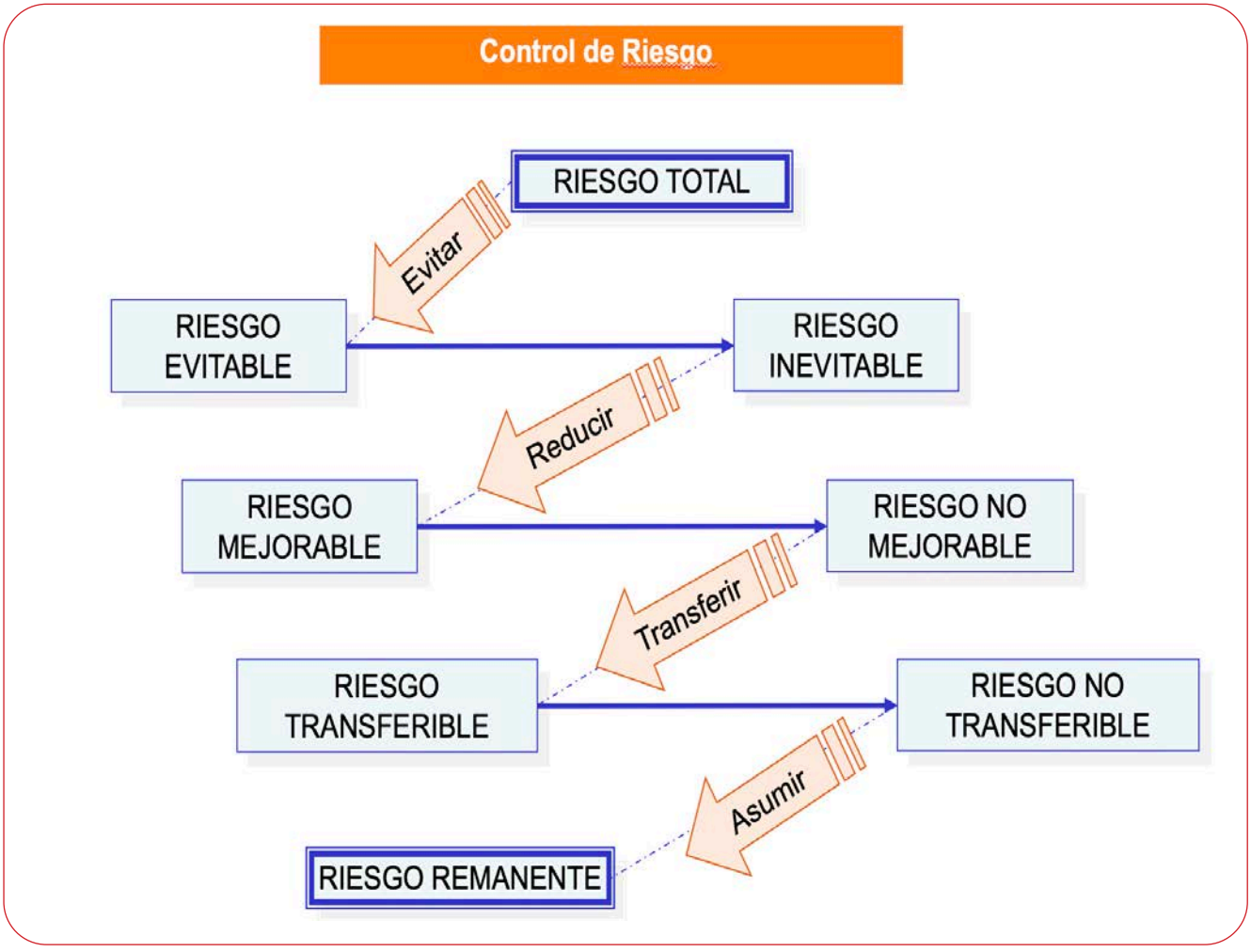


ADVERSARIO





FACTORES PRIMARIOS Estrategia de la delincuencia	FILOSOFÍA DE DEFENSA Medios a aplicar contra ella
El botín	Que el botín sea bajo
El riesgo	Que el riesgo sea mayor
El tiempo que se tarda en realizar el objetivo	Que el tiempo sea superior a las posibilidades
Las consecuencias	Que las consecuencias sean graves
Los medios técnicos y los medios humanos	Que los medios resulten costosos



Gracias!

Síganos en nuestras redes sociales

@sersecovenezuela
@sersecocolombia
@sersecointernational
@sersecopanama

Grupo Serseco
Serseco Colombia
Serseco International
Serseco Panamá

www.serseco.com

¿Desea ser contactado por un Asesor Comercial Grupo Serseco?

GRUPO serseco

Aprendizaje SIN LÍMITE

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

APRENDOYA
APRENDIZAJE SIN LÍMITES Y FRONTERAS

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

¡Es hora de crecer!

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

El momento de actuar es

AHORA

Haz que tu conocimiento brille y tus ventas despeguen.

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

CORPROJO
SERVICIOS INTEGRALES

PREPARACIÓN INTEGRAL EN SEGURIDAD PARA UN FUTURO MÁS PROTEGIDO

CON FORMACIÓN PRÁCTICA Y ESTRATEGIAS EFECTIVAS

www.corporacionrojo.com

BGMC Group
CAPACITACION PROFESIONAL EN SEGURIDAD

CONSULTORÍA Y CAPACITACIÓN ESTRATEGICA EN SEGURIDAD INTEGRAL

NUESTROS SERVICIOS

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

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

- Capacitación tecnica en Seguridad y protecccón ejecutiva

+58 424 398 6498
@ bgmc.group
bgmcgroup.director@gmail.com
+ 58 424 398 6498 / 426 218 2158

¿Mi informacion personal? ¿Está protegida en la empresa donde trabajo?

¿Seguridad y Recursos Humanos, como se relacionan?

Antes de poder relacionar dos áreas tan extensas como lo son la seguridad y el recurso humano de una empresa debemos entender cada concepto por separado, pero no de una manera conceptual, copiado de la red o de un libro necesitamos entenderlo con nuestras propias palabras.

¿Qué es la seguridad?

Es la ausencia de peligro, esa oración es lo primero que aparece en nuestro subconsciente al momento de escuchar esa palabra, pero actualmente va más allá de eso y todos por mas pequeño hemos notado el cambio y cuando vemos las siglas RRHH lo que pensamos es las personas que trabajan allí que hacen vida dentro de la empresa además del área en las nos remuneran por nuestros servicios, estos dos áreas se relacionan de una manera cada vez mas estrecha gracias a la tecnología que cada día nos arropa de una manera abismal.

Gracias a la tecnología hemos podido desarrollar diversas maneras de expandir nuestros conocimientos de dar a conocer nuestras ideas, proyectos y hacerlos realidad de una manera que antes era imposible de soñar, la manera de gestionar al personal en una empresa ha cambiado de una manera radical hemos pasado de tratar con los futuros candidatos para una puesto personalmente, citarlos e interactuar con ellos a realizar una entrevista online llenando un cuestionario, realizando entrevistas por las plataforma zoom, Google met que nos permite optimizar nuestro tiempo, recibir cientos de curriculum y poder seleccionar los más adecuados de manera rápida , generar una base de datos de posibles talentos con todos sus datos algo que debería ser privado se ha vuelto público, como estar seguro de que esos datos están seguros dentro de esa empresa, porque no solo se encuentran en riesgo quien busca empleo y va dispersando su información por todos los medios, también se encuentra en riesgo las personas que hacen vida dentro de una empresa en donde los archivos se han vuelto digitales almacenados en una nube.

La información del talento humano es hoy uno de los activos más vulnerables

En épocas de alto movimiento económico, el riesgo se multiplica

La planificación y la educación lo es todo sin ello estamos perdidos

En este momento es que debemos pensar

¿Cómo mantener esos datos seguros?

Como alejarlos de los delincuentes ahora denominados ciberdelincuentes que se han educado, estudiado y encontrado la manera de acceder a lo más imprescindible que es los datos del personal que maneja un departamento de RRHH que dependiendo del tamaño de la empresa podemos hablar de cien personas hasta catorce mil en una sola empresa o entidad pública.

A que nos enfrentamos en este momento, a la época decembrina que nos trae felicidad y reencuentro, pero también significa económicamente hablando donde se realizan mayores compras, se mueve el dinero, y en el departamento de recursos humanos específicamente en el área de nómina empieza la planificación de los pagos y de los beneficios que van a percibir los empleados de esa organización, nuestro primer punto es la confidencialidad, se debe mantener las directrices dadas al personal de nómina como las fechas de pago y los montos o beneficios que se otorgaran solo dentro de ese departamento para evitar la fuga de la información.

Para el proceso de pago se debe contar con un sistema ya sea profit, galac , infocent, y esperemos que no sea así data en Excel que es la manera más vulnerable de resguardar la información, pero todo esto que se menciona no se puede obtener de manera optima si no educas y mantienes motivado a tu personal, enseñándoles que es la seguridad a los riesgos que se enfrentan en la actualidad y la importancia de la privacidad, de que la información se puede usar de manera maligna para sacar provecho de cada uno de nosotros.

Si en la empresa donde trabajas no aplican la seguridad como un tema serio y de gran importancia se el pionero, se la persona que se interesa no te dejes pasar por alto esas inquietudes.

Desiree Da Silva

Biografía:

TSU EN ADMINISTRACIÓN
TECNICO CONTABLE
Especialista en legislación laboral
Cuenta con más de dos décadas de experiencia laboral en el area de recursos humanos privada y pública
Actualmente se encuentra estudiando en la UNEXCA
Venezolana, emprendedora y madre de familia

ASESORES Y CONSULTORES, C.A.

SEPREVYPRO

Rif. J-40474851-8

Seguridad, Prevención y Protección

La Agenda Ejecutiva de Seguridad Integral

Es mi Herramienta para Rendir mi Gestión

UTILIDAD DE LA AGENDA

Produce un esquema de trabajo organizado con fundamentos técnicos.

Es tener la organización a la mano para analizar, evaluar y dar la debida respuesta administrativa y operativa en cada caso.

BENEFICIOS ASOCIADOS

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

VALORES

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

INFORMACIÓN

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

Cuando el Ransomware Toca a tu Puerta en la Época Decembrina

Diciembre en Venezuela es una mezcla de nostalgia, esperanza y movimiento. Las calles se llenan de luces, los hogares se preparan para recibir a los que vienen de lejos, y las empresas cierran ciclos mientras proyectan el año que viene. Pero en medio de tanta emoción, hay una amenaza silenciosa que también se prepara para hacer de las suyas: el ransomware

Sí, ese virus que "secuestra" tus archivos y te exige dinero para liberarlos. Pero no es cualquier virus. En 2025, el ransomware se ha vuelto más astuto, más agresivo y más personalizado. Ya no solo bloquea tus documentos, ahora roba información confidencial, amenaza con publicarla y exige pagos en criptomonedas. Y lo peor: lo hace justo cuando estás más distraído, más confiado y más ocupado.

En Venezuela, esta amenaza ha crecido de forma preocupante. Plataformas como RansomHub y Fog han comenzado a atacar instituciones públicas, empresas agroindustriales, comercios, residencias, colegios y hasta espacios pastorales. ¿Por qué? Porque saben que muchos sistemas están desactualizados, que la cultura de ciberseguridad aún no está arraigada, y que diciembre es el momento perfecto para entrar sin ser detectados.

Imagina esto: estás organizando una jornada comunitaria, preparando el cierre contable de tu empresa o enviando mensajes navideños a tu equipo. De repente, un correo con apariencia festiva llega a tu bandeja de entrada. Tiene luces, buenos deseos y un archivo adjunto que parece inofensivo. Lo abres... y sin saberlo, acabas de abrirle la puerta al ransomware.

Este tipo de ataque no discrimina. Puede afectar desde una pequeña tienda en Cúa hasta una red de seguridad privada en Caracas. Y cuando entra, no pide permiso. Cifra tus archivos, te bloquea el acceso, y te deja un mensaje: "Si quieres recuperar tu información, paga". Pero incluso si pagas, no hay garantía de que todo vuelva a la normalidad. A veces, los datos se pierden. O peor, se filtran.

Y no se trata solo de empresas. En los últimos meses, se han reportado ataques a juntas comunales, parroquias, escuelas y hasta grupos de vecinos organizados. ¿El motivo? Muchos de estos espacios manejan bases de datos, listas de contactos, archivos de gestión y hasta información financiera. Todo eso es valioso para un atacante. Y si no hay respaldo ni protocolos, el daño puede ser irreversible.

La realidad venezolana hace que este tipo de amenazas sea aún más delicada. Muchas organizaciones trabajan con recursos limitados, equipos viejos y conexiones inestables. La prioridad suele estar en lo operativo, en lo urgente, y la seguridad digital queda relegada. Pero hoy, más que nunca, es momento de cambiar esa mentalidad. Porque proteger nuestros datos es proteger nuestras historias, nuestros proyectos y nuestras comunidades.

¿Qué puedes hacer para blindarte en esta temporada?

1. Actualiza tus equipos y sistemas. No dejes para enero lo que puedes asegurar hoy. Muchos ataques ocurren por fallas que ya tienen solución, pero que no se han aplicado por descuido o falta de tiempo.

2. Haz respaldos offline. Guarda tus archivos importantes en discos externos y desconéctalos de la red. Así, si algo ocurre, tendrás una copia segura.

3. Evita contraseñas débiles. Nada de “123456” ni “navidad2025”. Usa combinaciones seguras, con letras, números y símbolos. Y si puedes, cambia tus claves cada cierto tiempo.

4. No abras correos sospechosos. Aunque tengan luces, ofertas o bendiciones. Si no conoces al remitente o el mensaje te parece extraño, mejor no lo abras.

5. Capacita a tu gente. Haz charlas, comparte tips, crea conciencia. La prevención empieza por casa, por tu equipo, por tu comunidad.

6. Usa plataformas de monitoreo. Existen herramientas que te alertan si algo raro pasa en tu sistema. Son como vigilantes digitales que nunca duermen.

7. Segmenta tus redes. No todo debe estar conectado. Divide tus sistemas por niveles de acceso y sensibilidad. Así, si hay un ataque, no se propaga tan fácilmente.

8. Ten un plan de respuesta. ¿Qué harías si mañana te atacan? ¿A quién llamarías? ¿Qué sistemas apagarías? Tener un protocolo claro puede marcar la diferencia entre el caos y el control.

9. Involucra a tu comunidad. Si lideras espacios educativos o empresariales, promueve campañas de concientización. Puedes usar boletines, dinámicas, infografías o incluso mensajes de prevención.

10 No subestimes el riesgo. El ransomware no es cosa de grandes corporaciones. Es una amenaza real, presente y activa en nuestro país. Y diciembre es su momento favorito.

¿Y si ya fuiste víctima?

Si ya sufriste un ataque, lo primero es no entrar en pánico. Desconecta los equipos afectados, evita propagar el daño y contacta a un especialista. No borres nada, no pagues de inmediato y documenta todo lo que puedas. En muchos casos, hay formas de recuperar la información o al menos contener el impacto. Pero lo más importante es aprender de la experiencia y reforzar tus defensas.

En tiempos donde todo parece acelerado, hablar de ciberseguridad puede sonar técnico, frío o lejano. Pero no lo es. Es una forma de cuidar lo que amamos. De proteger lo que hemos construido con esfuerzo. De garantizar que nuestras comunidades, nuestras familias y nuestros sueños no se vean interrumpidos por un clic mal dado.

La seguridad digital también es comunitaria, también es humana. Porque detrás de cada archivo hay una historia. Detrás de cada sistema, hay personas. Y detrás de cada ataque, hay una oportunidad para crecer, para aprender y para fortalecernos.

En tiempos de unión, proteger nuestros datos es también proteger nuestras familias, nuestras comunidades y nuestros sueños. Que esta Navidad nos encuentre blindados, vigilantes y resilientes. Porque cuando el ransomware toca a tu puerta, solo la prevención y la conciencia pueden evitar que entre.

Autor:
Adolfo M. Gelder

Oferta exclusiva para lectores Inteligentes...

¡OBTÉN UN 10% DE DESCUENTO INMEDIATO!

en la compra de tu licencia de Dr.Web Security Space (para 1 año / 1 PC).
Para reclamar tu descuento exclusivo, por favor contacta a la revista enviando un correo a:

agelder@seguridadenaccionlatam.com

No esperes a que ocurra un imprevisto. Asegura tu tranquilidad hoy mismo.

Dr. Web. Creado para proteger.
Diseñado para que vivas tranquilo.
www.drweb.com

¿BUSCAS ALQUILER DE CAMIONETAS BLINDADAS?

¡TRASLADOS A NIVEL NACIONAL!

UNIVERSAL ADVENTURE®

*Imagen Referencial

- Servicios de Escoltas VIP
- Traslados al Aeropuerto
- Transporte de Ejecutivos
- Servicios en toda Venezuela

VENEZUELA, POSIBLE LABORATORIO PARA NUEVA DOCTRINA GLOBAL?...

“Un viejo adagio reza; En el mundo de los ciegos, el tuerto es Rey...”

En los últimos meses, Estados Unidos ha intensificado su presencia militar en el Mar Caribe bajo la justificación de combatir el narcotráfico, desplegando más de 4.000 efectivos, principalmente infantes de marina, y reforzando su presencia con aviones, barcos y misiles.

Paralelamente, Estados Unidos ha designado al presidente venezolano Nicolás Maduro como “narco-traficante”, ofreciendo una recompensa de 50 millones de dólares por su captura. Esta acusación se basa en la supuesta vinculación de Maduro con el “Cartel de los Soles”, una organización dedicada al narcotráfico que, según informes, involucra a altos funcionarios venezolanos. Todo este panorama vislumbra unas posibles fiestas Decembrinas en Venezuela, llena de incertidumbre y un ambiente político y social muy volátil.

VENEZUELA COMO FOCO ESTRATÉGICO

La designación de Maduro como líder de una red de narcotráfico y la acusación del "Cartel de los Soles" refleja un interés explícito de EE.UU. en deslegitimar al gobierno venezolano y justificar presiones multilaterales y unilaterales. Venezuela, aunque reconocida principalmente como país de tránsito, fue presentada ante el mundo como una amenaza directa a la seguridad hemisférica y a la seguridad nacional de Estados unidos.

Es importante destacar nuevamente; que la comunidad internacional, incluyendo a la ONU y la OEA, ha considerado a Venezuela principalmente como un país de tránsito para la distribución de drogas, sin ser un productor significativo. Por lo tanto, cualquier acción militar en Venezuela bajo la justificación de la lucha contra el narcotráfico requeriría una base legal sólida y un consenso internacional para evitar violaciones al derecho internacional y la soberanía de los estados involucrados.

POSIBLE DESARROLLO DE UNA DOCTRINA

La combinación de acciones políticas, judiciales, económicas y militares podría interpretarse como la preparación o implementación de una doctrina que justifique intervenciones bajo el pretexto de la lucha contra el narcotráfico, similar a la "Guerra Global contra el Terrorismo". En este marco, Venezuela podría ser vista como un "laboratorio" o caso piloto para validar tácticas, alianzas y legitimaciones internacionales.

"MATAR DOS PÁJAROS DE UN TIRO"

Desde esta perspectiva estratégica, atacar al régimen venezolano bajo el argumento del narcotráfico permitiría, simultáneamente:

- Desestabilizar y buscar la salida de Maduro, objetivo político central para la administración Trump en la actualidad.
- Justificar la presencia militar y operaciones en la región que podrían extenderse a otros países productores tradicionales (Colombia, Ecuador, Bolivia), ampliando el alcance de la doctrina.

Si se llegara a establecer una doctrina de “Guerra Global contra el Narcotráfico”, sus bases conceptuales y estratégicas podrían estructurarse tomando como referencia elementos claves de doctrinas precedentes (como la Guerra Global contra el Terrorismo) y adaptándolos a la naturaleza y desafíos específicos del narcotráfico.

BASES DE UNA DOCTRINA DE GUERRA GLOBAL CONTRA EL NARCOTRÁFICO

1. Definición amplia y global del enemigo

- Considerar no solo a los carteles y organizaciones narcotraficantes, sino también a los Estados o gobiernos que, directa o indirectamente, facilitan o toleran esta actividad ilícita.
- Incluir en el concepto a actores financieros, redes de lavado de dinero y grupos criminales transnacionales vinculados al narcotráfico.

2. Enfoque multidimensional y multisectorial

- Integrar acciones militares, policiales, inteligencia, cooperación judicial y financiera.
- Incorporar campañas para combatir la demanda de drogas en mercados consumidores y programas de prevención social y desarrollo alternativo en regiones productoras.

3. Prevención y acción preventiva

- Disposición para intervenir anticipadamente,
- Uso de sanciones, bloqueo financiero y presiones diplomáticas para aislar a actores vinculados.

4. Cooperación internacional reforzada

- Fortalecer alianzas estratégicas con países clave en producción, tránsito y consumo, especialmente en regiones vulnerables como América Latina y el Caribe.
- Implementar intercambio de inteligencia, conjuntos operativos y apoyo logístico.

5. Legitimación jurídica y política

- Basar las acciones en mandatos internacionales, acuerdos bilaterales y multilaterales, respetando (o reinterpretando) normas de soberanía estatal y derecho internacional.
- Crear marcos legales para operaciones especiales, detenciones, incautaciones y procesos judiciales transnacionales.

6. Uso combinado de poder “duro” y “blando”

- Emplear fuerzas militares y policiales para acciones directas contra infraestructuras, narcotraficantes y rutas de tráfico.
- Complementar con diplomacia, desarrollo económico, campañas educativas y lucha contra la corrupción.

7. Orientación hacia la desarticulación de redes y capacidades.

- Foco en desmantelar las estructuras criminales, desde productores hasta distribuidores y financieros.
- Control del flujo de armas, dinero y logística que sustentan el narcotráfico.

8. Adaptación tecnológica y estratégica

- Uso de tecnologías avanzadas para vigilancia marítima, aérea y cibernética.
- Adaptación a nuevas formas de tráfico y evasión, incluyendo el uso de drones, criptomonedas y rutas alternativas.

Este marco conceptual serviría para justificar una política exterior y de seguridad activa y coordinada, con un énfasis marcado en la acción preventiva y la cooperación estratégica, que podría facilitar las intervenciones directas en países considerados vulnerables o vinculados al narcotráfico.

RIESGOS Y DESAFÍOS

Ahora a mi parecer, existen riesgos y desafíos a enfrentar para la ejecución de la doctrina de "Guerra global contra el narcotráfico" y considero que serían las siguientes:

Soberanía nacional y derechos internacionales

Intervenciones militares o acciones coercitivas en países soberanos podrían violar el derecho internacional y generar conflictos diplomáticos, especialmente si no cuentan con respaldo multilateral claro.

1. Escalada de violencia y militarización

La presencia militar intensiva puede exacerbar conflictos internos, provocar resistencias armadas y aumentar la violencia, afectando a poblaciones civiles.

2. Estigmatización y politización

La doctrina puede ser utilizada para justificar presiones políticas o intervenciones contra gobiernos consideradas incómodas, bajo pretextos de lucha contra el narcotráfico, como ha ocurrido con Venezuela.

3. Efectividad limitada y desplazamiento del problema

Las acciones militares y represivas suelen desplazar las rutas o actores del narcotráfico sin erradicar la demanda o las causas estructurales, generando efectos colaterales y ciclos de violencia.

4. Impacto social y derechos humanos

Operaciones militares o policiales pueden derivar en violaciones a derechos humanos, afectaciones a comunidades locales y aumento de desplazamientos forzados.

5. Resistencia y radicalización

La intervención externa puede alimentar sentimientos antiimperialistas y de resistencia, fortaleciendo movimientos armados o extremistas.

CRÍTICAS PRINCIPALES

Por supuesto y como es de esperarse, esta doctrina llegaría a obtener y acumular críticas y en mi opinión particular de acuerdo a lo que he podido apreciar, pues serían las siguientes:

1. Enfoque militarizado y simplista

Se critica que una doctrina basada en la "guerra" priorice soluciones militares sobre políticas de reducción de demanda, desarrollo social y reforma institucional.

2. Falta de enfoque en causas estructurales

El narcotráfico es un fenómeno social muy complejo vinculado a la pobreza, corrupción, desigualdad y falta de oportunidades; ignorar estas raíces limita la sostenibilidad de los resultados.

3. Riesgo de intervenciones selectivas y sesgadas

La doctrina puede ser aplicada de forma selectiva, afectando a unos países y no a otros con problemas similares, por intereses de tipo geopolíticos.

4. Posible erosión de la cooperación multilateral

El predominio de acciones unilaterales o coaliciones ad hoc(para un fin específico) puede debilitar los mecanismos multilaterales existentes, como la ONU o la OEA.

5. Desconfianza regional

América Latina y el Caribe pueden ver la doctrina como una forma de injerencia o neoimperialismo, dificultando la cooperación y generando tensiones diplomáticas.

IMPACTO GEOPOLÍTICO GLOBAL

En este punto y para no extenderme demasiado, voy a nombrar donde considero que impactaría la doctrina de "Guerra Global contra el narcotráfico" sin profundizar por ahora sino en un próximo escrito:

- **Reconfiguración del Poder y las Alianzas Internacionales**
- **Tensiones y Conflictos Regionales y Globales**
- **Cambios en la Soberanía y Normas Internacionales**
- **Influencia en la Política y Economía Global**
- **Potencial para un Nuevo Orden de Seguridad Global**

MI CONCLUSIÓN

La instauración de una doctrina de "Guerra Global contra el Narcotráfico" representaría un cambio paradigmático en la política internacional y la seguridad global, con amplias repercusiones geopolíticas. Esta doctrina podría servir para legitimar y expandir la intervención militar y estratégica de potencias, principalmente Estados Unidos, en regiones clave consideradas vulnerables al narcotráfico, como América Latina y el Caribe.

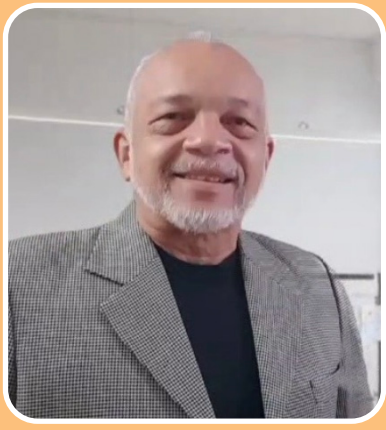
Si bien podría fortalecer la cooperación internacional y mejorar la capacidad operativa para enfrentar las redes criminales transnacionales, también implicaría riesgos importantes. Entre ellos, la erosión de la soberanía nacional, el aumento de tensiones diplomáticas y militares, y la potencial desestabilización regional debido a la militarización y posibles conflictos derivados de estas acciones.

Además, la doctrina podría exacerbar divisiones dentro de la comunidad internacional, alimentando percepciones de hegemonismo o intervencionismo selectivo. Esto podría impulsar alianzas alternativas y fortalecer actores políticos y armados contrarios a la influencia occidental, dificultando la gobernabilidad.

El éxito de esta nueva doctrina dependerá críticamente de su capacidad para equilibrar el uso legítimo de la fuerza con políticas integrales que aborden las causas profundas del narcotráfico, como la pobreza, la corrupción y la desigualdad. Asimismo, será esencial contar con un marco jurídico y político internacional sólido que garantice la legitimidad y el respeto a los derechos humanos y la soberanía de los estados.

Finalmente, considero que esta doctrina influiría en la redefinición del concepto de seguridad global, ampliándolo para incorporar de manera prioritaria al narcotráfico como amenaza transnacional, lo que podría llevar a la emergencia de nuevos modelos de cooperación y doctrina militar y política en el siglo XXI.

My. Marcos A. Carrillo C.
Consultor privado de Seguridad
Especialista en Gestión y análisis de riesgos
Miembro activo de la International Foudation Protection Officers (IFPO)



Perfil Profesional

El Mayor **Marcos Carrillo Castillo** es un oficial retirado del Ejército de Venezuela.

Su trayectoria profesional, incluye 22 años de servicio militar en unidades tácticas y administrativas del Ejército Venezolano y 16 años en el sector empresarial privado, lo cual le suma de 38 años de experiencia en el ámbito de la seguridad.

Es experto en operaciones de seguridad y protección corporativa, con experiencia en la implementación y supervisión de esquemas de seguridad en instalaciones críticas (públicas y privadas) en Venezuela.

También se desempeña como conferencista y ponente, dedicado a la capacitación de personal de seguridad desde el nivel operativo hasta el gerencial. Es consultor en seguridad Integral, con experiencia en análisis y gestión de riesgos, así como en control de pérdidas.

Actualmente, es miembro activo de la International Foudation Protection Officers (IFPO) y CEO de Carrillo & Consultores.

INVERTIR EN SEGURIDAD COMO GARANTIA DE SU INVERSION

Foto: Internet

Por Salvadort Romani

Los países desarrollados están convirtiendo la industria del turismo en su prioridad actual, para en un futuro, a mediano plazo y largo plazo, obtener mejores resultados de esos movimientos humanos.

Los inversionistas del turismo deben entender que esta es una de las áreas más vulnerables y que cualquier descuido en el ámbito de la seguridad puede ocasionar pérdidas económicas incalculables. En consecuencia, la seguridad en todo proyecto turístico debe verse como una inversión y no como un gasto; esto obliga a un cambio de visión de la seguridad en el entorno turístico, en donde el sector público y el privado compartan la misma mesa para diseñar estrategias conjuntas que permitan aunar esfuerzos en contra de las diversas amenazas a la que se ve enfrentado el

La industria del turismo ha constituido un emblema en un mundo ya globalizado, en donde las fronteras físicas del antiguo esquema del Estado Nación, prácticamente son inexistentes.En esta aldea global, el movimiento de personas cada día aumenta por lo que los beneficios del Estado como del sector privado dependerán en gran medida de la capacidad que estos tengan para manejar esos movimientos masivos de personas y capitalizarlos en beneficio de sus propios ciudadanos y empresas.

Hoy día se hace necesario un acercamiento entre los profesionales de la seguridad y los profesionales del turismo, la idea es integrar la seguridad dentro de las operaciones normales de un hotel. Los empresarios turísticos deben entender que la seguridad debe estar incluida en la etapa de planificación de un proyecto o evento. Al estar la actividad turística revestida de un matiz netamente comercial, los inversionistas buscan obtener ganancias a un menor costo.

sector, porque si bien es cierto, que la globalización ha traído beneficios, también ha arrastrado mayores riesgos que afecten directa o indirectamente el desarrollo de los destinos turísticos en la esfera mundial.

En ocasiones en busca de ese beneficio inmediato contratan agentes de seguridad sin la más mínima preparación; con frecuencia incurren en el error de no investigar, por considerarlo una pérdida de tiempo, los antecedentes personales es un tema importante de los profesionales de la seguridad, debido a que los que tiene acceso a las habitaciones de los huéspedes pueden haber tenido inconvenientes con los organismos policiales o judiciales. Con estas investigaciones, los empresarios evitarían la contratación de empleados deshonestos y propensos a cometer delitos.

La solución a un problema que afecte la seguridad en el ámbito turístico es diferente a la delincuencia común, en todo caso las campañas de información pública y las recomendaciones de los

países emisores, en muchos casos indiscriminadas en el tiempo, han generado históricamente un perjuicio mayor al sector, que el hecho en sí mismo, en donde el rescate de la buena imagen solo se lograra a travez de fuertes campañas publicitarias acompañadas de ofertas atractivas, lo que conllevaría a pérdidas económicas cuantiosas provocadas por la baja del turismo y los enormes costos publicitarios para su recuperación.

Sin duda alguna un atractivo turístico no depende únicamente de sus bellezas naturales o exóticas, en un mundo lleno de opciones; en esto juega un rol preponderante la seguridad, esto obligara al inversionista turístico a un cambio de mentalidad, a ver a la seguridad, no como un gasto sino como una inversión de garantía, en el crecimiento y desarrollo del destino turístico.

¿Cuánto estoy dispuesto a invertir para asegurar lo que recibo?, quizás no sea la pregunta; sino ¿Cuánto estoy dispuesto a invertir para evitar el no recibir nada?, es que un descuido en la seguridad y un incremento de la criminalidad en un destino turístico puede provocar no solo el desplome de ese destino, sino su desaparición. Cuando Cristóbal Colon y sus acompañantes, en tres frágiles embarcaciones, se aventuraron por el atlántico en 1492, se necesitaba de un valor más fuerte que el acero para iniciar esa aventura.

Hoy día es posible que los viajeros no tengan que enfrentar esas vicisitudes o amenazas mortales del pasado, pero en la actualidad hay una serie de amenazas modernas o emergentes y la industria del turismo tendrá que continuar analizando esos escenarios llenos de incertidumbres e invertir en la preparación, equipamiento, mantenimiento y actualización de la seguridad, para poder producir soluciones creativas si es que se desea continuar prosperando.

SALVADOR ROMANI ORUE

ASESOR DE SEGURIDAD

BOSQUEJO CURRICULAR.

Mi desarrollo laboral y profesional se ha basado en el campo de las actividades de seguridad física durante veinte años, estando en funciones en los servicios de inteligencia y prevención DISIP, laborando activamente en la Dirección de protección de personalidades, escolta civil presidencia, patrullaje vehicular y motorizado; asesorías en materia de seguridad a empresas del ramo hotelero, entidades financieras, empresas de transporte de carga y empresas de vigilancia y seguridad. Así mismo desempeñándome como instructor de cursos de preparación y formación de escoltas Vip, Gerente de protección integral del Instituto Postal Telegráfico de Venezuela IPOSTEL, además de ser miembro activo desde el año 2004 de la Asociación Venezolana de Ejecutivos de seguridad AVES siendo el miembro N° 110; además de poseer el Galardón de la Escuela de Inteligencia de las Fuerzas Armadas con el grado de Comisario y el reconocimiento mediante el otorgamiento del Botón Esinfa del Ministerio de la Defensa.

EXPERENCIA LABORAL

Gerente Corporativo de seguridad Hoteles Premier, MGH Protección Integral C.A, Gerente de de la unidad de escoltas de cargas, Gerente Corporativo de seguridad empresa Class Light C.A, Gerente de protección integral del Instituto Postal Telegráfico de Venezuela IPOSTEL, Jefe de seguridad presidenta de FEDECAMARAS Dra. Albis Muños, DISIP Ministerio de Interior y Justicia con el rango de: inspector.

FORMACIÓN ACADEMICA.

Bachiller en ciencias, Academia de Formación Policial DISIP.

OTRAS ACTIVIDADES.

Instructor de cursos de formación escoltas VIP, Consultorías de seguridad, Presidente de US MARSHAL SECURITY CA. Empresa dedicada al ramo de asesorías de seguridad y servicios de escoltas Vip.

INTERNATIONAL SEGURITY ALLIANCE

INSEAL

"Te conviertes en lo que entrenas"