

# SEGURIDAD EN ACCIÓN

## HAITÍ INSEGURIDAD TOTAL

Enfrenta su mayor crisis de orden público

PAG. 17-21

## LA CIBERSEGURIDAD Y SUS TEORÍAS

La prevención se vuelve clave  
para sobrevivir en línea

PAG. 13-15

## CUANDO LA MENTE IMPORTA

El desafío silencioso en el entorno laboral

PAG. 4-9



[www.seguridadenaccionlatam.com](http://www.seguridadenaccionlatam.com)

REVISTA DE REFERENCIA DEL SECTOR DE LA SEGURIDAD  
PRIVADA, CIBERSEGURIDAD, PROTECCIÓN DE DATOS.



# EDITORIAL

Hoy la seguridad integral es un pilar estratégico para el mundo corporativo y social. No solo implica prevenir riesgos, sino garantizar confianza, continuidad y desarrollo sostenible. En un entorno marcado por amenazas físicas, ciberneticas y sociales, la seguridad debe entenderse como una inversión y no como un gasto.

Esta revista busca ser un espacio de encuentro donde líderes, especialistas y organizaciones compartan experiencias, conocimientos y soluciones prácticas. Queremos promover una visión que abarque todos los frentes: protección de personas, gestión de crisis, resiliencia tecnológica y resguardo institucional.

Nuestro compromiso es brindar herramientas y contenidos que inspiren a empresas e instituciones a integrar la seguridad como parte de su identidad y estrategia. Solo a través del trabajo conjunto podremos transformar los desafíos en oportunidades y avanzar hacia un entorno más seguro y confiable para todos.

## STAFF



**HUMBERTO COPA G.**  
DIRECTOR GENERAL



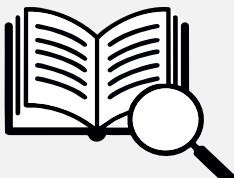
**LUCIEL RIOS CAMACHO,**  
COORDINADORA ACADÉMICA Y  
OPERATIVA



**DAVID CORONEL CLAU雷**  
EDICIÓN Y PRENSA

Seguridad en Acción es una revista especializada en seguridad integral, abordando temas de seguridad corporativa, industrial, electrónica, cibernetica 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



## Pag. 4-9 CUANDO LA MENTE IMPORTA

La importancia del cuidado de la salud mental de los colaboradores.



## Pag. 10-12 LA CRIMINALIDAD ORGANIZADA

El elefante está ahí, en la sala, entre memorandos y balances; pero nadie quiere verlo.

## Pag. 13-15 LA CIBERSEGURIDAD

Y la teoría de los sistemas complejos.



## HAITÍ, INSEGURIDAD TOTAL

Pag. 17-23 Rico en historia, fue la primera "República negra" del mundo.

## ATRACTIVO DEL RIESGO

Pag. 22-27 Y vulnerabilidad del activo desde la perspectiva del agresor



## Pag. 28+31 CRIMEN ORGANIZADO TRANSNACIONAL

Narcotráfico, corrupción y su impacto global

## Pag. 32-38 LA INTERNATIONAL POLICE ASSOCIATION (I.P.A.)

Punto de encuentro para todos los policías del mundo

## Pag. 40-42 RECLUTAMIENTO Y SELECCIÓN

El primer filtro de la seguridad





**CUANDO LA MENTE IMPORTA**

# El Desafío Silencioso

## en el entorno laboral

La importancia del cuidado de la salud mental de los colaboradores



**E**n América Latina, el riesgo psicosocial en el entorno laboral ha adquirido una relevancia creciente. A pesar de que varias naciones han adoptado normativas, protocolos y estrategias para mitigarlo, persisten notables brechas en regulación, diagnóstico y atención oportuna.

Aunque algunos países han avanzado normativamente como Colombia, con la Resolución 2646 de 2008, muchos aún carecen de marcos legales sólidos adaptados a las especificidades socio-laborales de la región. Las iniciativas de pre-

vención de accidentes y enfermedades laborales existentes son aún insuficientes cuando llega el momento de abordar de forma integral el bienestar psicosocial de los trabajadores.

A la complejidad se suman desafíos estructurales como la alta informalidad laboral, el acceso limitado a servicios de salud mental, la escasa formación de líderes en competencias emocionales, y culturas organizacionales que normalizan la presión excesiva, la violencia psicológica y estilos de gestión autoritarios.

**Promover ambientes donde no solo se prevengan riesgos físicos, sino también donde exista bienestar emocional, respeto, asertividad y cooperación.**



El contexto también enfrenta la urgencia de cumplir con los Objetivos de Desarrollo Sostenible (ODS), especialmente el ODS 3 (Salud y Bienestar) y el ODS 8 (Trabajo Decente y Crecimiento Económico). Para lograrlo, es fundamental fortalecer los sistemas de Seguridad y Salud en el Trabajo (SST), promoviendo ambientes donde no solo se prevengan riesgos físicos, sino también donde exista bienestar emocional, respeto, asertividad y cooperación.

Uno de los principales retos es la transformación cultural que muchas organizaciones requieren. Aún prevalecen estilos de liderazgo verticales, deshumanizantes y carentes de empatía. Se desconoce que el trabajador, más allá de su rol funcional, es un ser humano integral que necesita condiciones emocionales y sociales saludables para innovar, comprometerse y sentirse motivado.

**Por ello, los profesionales de SST deben adoptar una visión integradora:**

además de prevenir riesgos físicos, deben promover una cultura de bienestar emocional. Nuestro desafío consiste en “evangelizar” la importancia del bienestar psicosocial, generar entornos saludables y formar líderes conscientes que actúen desde el respeto, la empatía y el compromiso genuino con sus equipos.

# Por qué es esencial cuidar LA SALUD MENTAL EN EL TRABAJO?

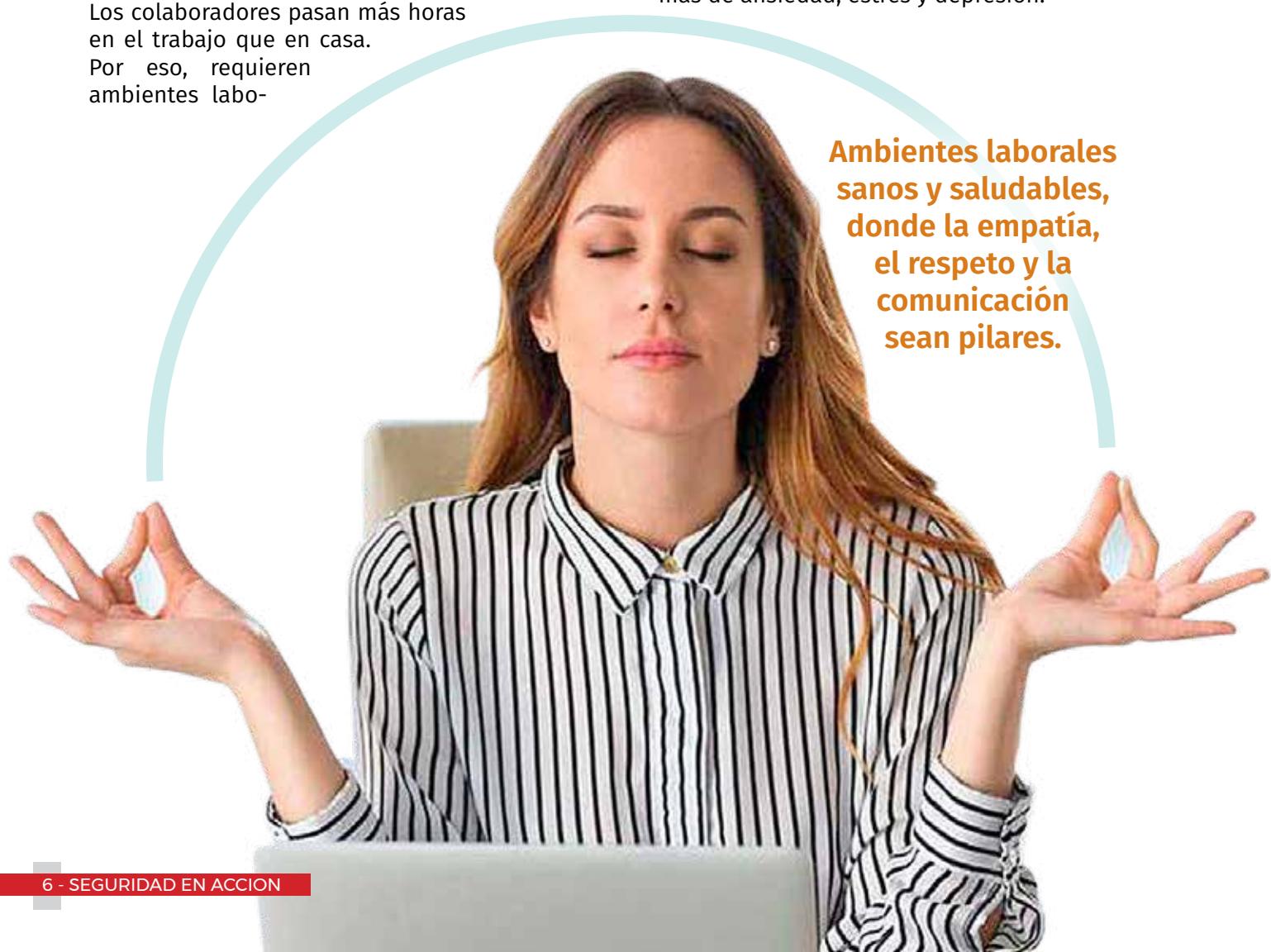
**L**a salud mental laboral se ha convertido en una prioridad, especialmente en escenarios postpandemia. Aunque tradicionalmente los departamentos de SST estuvieron centrados en prevenir daños físicos, hoy se evidencian altas tasas de ansiedad, depresión y estrés laboral.

En Colombia, según el Ministerio de Salud (2023), el 66,3 % de la población declaró haber enfrentado un problema de salud mental, siendo frecuentes las incapacidades asociadas a estrés y depresión. Esto evidencia la urgente necesidad de actuar en el entorno laboral.

Los colaboradores pasan más horas en el trabajo que en casa. Por eso, requieren ambientes labo-

rales sanos y saludables, donde la empatía, el respeto y la comunicación sean pilares. Es vital que los responsables de gestión humana comprendan su rol en el bienestar emocional de los colaboradores.

Lamentablemente, algunos departamentos se enfocan únicamente en funciones administrativas como selección y nómina, descuidando el bienestar emocional. En ciertos casos, la gestión humana se convierte en percibida como una barrera, ya que falta humanidad y empatía al abordar situaciones personales o laborales críticas, contribuyendo al aumento de síntomas de ansiedad, estrés y depresión.



**Ambientes laborales sanos y saludables, donde la empatía, el respeto y la comunicación sean pilares.**

# Normatividad y barreras en Colombia

**C**olombia cuenta con leyes y resoluciones como la Ley 1010 de 2006, la Resolución 2646 de 2008 y la Resolución 2404 de 2019, que definen protocolos de intervención psicosocial por sector (transporte, salud, educación, financiero, etc.). Sin embargo, la implementación real de estas normas aún es incierta.

Se reportan situaciones de acoso laboral, técnicas de gestión agresivas y jefaturas tóxicas que promueven el síndrome de burnout. La falta de instancias independientes para atender estas problemáticas y la capacitación limitada de los Comités de Convivencia —regulados por los Decretos 1356 y 652 de 2012— representan un obstáculo crítico para proteger la salud emocional de los trabajadores.

La desatención de este riesgo puede desencadenar enfermedades laborales relacionadas con el estrés e incluso casos extremos como ataques de pánico o suicidio. Por eso, es imprescindible que los líderes de gestión humana y SST apliquen protocolos oficiales, ofrezcan primeros auxilios psicológicos y sumen psicólogos con experiencia en vigilancia y promoción psicosocial.



**Colombia cuenta con leyes y resoluciones, que definen protocolos de intervención psicosocial por sector (transporte, salud, educación, financiero, etc.).**



## Causas comunes de riesgo psicosocial

- Falta de capacitación y entrenamiento constante.
- Falta de planificación organizacional y definición de funciones.
- Designación de perfiles inadecuados y falta de inducción.
- Gestión autoritaria o micromanagement.
- Objetivos poco claros y rumores internos.
- Bienestar y crecimiento laboral.
- Procesos internos claros.
- Resolución de conflictos
- Falta de un sistema de gestión en seguridad y salud en el trabajo.
- Evaluación del desempeño y feedback asertivo.
- Inclusión y equidad laboral.
- Plan carrera y bienestar organizacional.
- Indicadores de gestión
- Alineación de la estrategia organizacional con el propósito de vida de los colaboradores.
- Acciones sostenibles encaminadas a los colaboradores y responsabilidad social empresarial.
- Confusión entre liderazgo y jefatura.
- Ausencia de aprendizaje continuo y cultura colaborativa.

**Estas dinámicas crean entornos insanos y afectan directamente el bienestar del personal**



## Acciones recomendadas

- Promover espacios de comunicación abierta y establecer pausas laborales.
- Capacitar a líderes en detección de señales de estrés y conflicto.
- Implementar claridad en roles, funciones y objetivos.
- Diseñar mecanismos confidenciales de resolución de conflictos.
- Respetar la desconexión laboral y priorizar el bienestar emocional.
- Respetar la diferencia y la inclusión
- Diseño de estrategias de sostenibilidad.
- Auxilios psicológicos
- Relingaría en los procesos.
- Programas de bienestar y plan carrera.
- Aplicación de baterías de riesgo psicosocial, para evaluar factores internos y externos.
- Programas de salud mental liderados por psicólogos expertos en riesgo psicosocial.

**Ignorar estas señales no solo merma la salud de los empleados, sino que también perjudica la reputación de la organización y su capacidad de atraer y retener talento**

# Conclusión

Pese a contar con una normativa robusta, la implementación efectiva del cuidado psicosocial aún es pendiente en múltiples empresas. Priorizar la productividad por encima del bienestar crea entornos laborales tóxicos que, con frecuencia, llevan a la renuncia silenciosa.

La salud mental en el trabajo no puede relegarse: solo mediante un enfoque integral, estratégico y humano lograremos construir organizaciones sanas, sostenibles y resilientes.

Las empresas, departamento de gestión humana y los líderes en HSE tienen un reto a cambiar y repensar el propósito de la seguridad y salud en las compañías debe enfocarse al cuidado físico y mental de la organización.

## Fuentes:

- Ministerio de Trabajo de Colombia
- UNICEF – “Over US\$30 billion lost to economies in Latin America and the Caribbean each year due to youth mental health”
- Organización Panamericana de la Salud (OPS)  
– Salud Mental
- ODS – Naciones Unidas

Magíster en innovación

# Especialista en higiene, seguridad Industrial y gestión ambiental

Autora:  
**ELENA LARA FLORIAN**  
(Colombia)



## Liderazgo con visión transformadora en SST y sostenibilidad

Elena Lara Florian, es una reconocida profesional en el campo de la Seguridad y Salud en el Trabajo, con más de una década de experiencia liderando procesos de transformación organizacional en sectores de alto impacto, incluyendo Oil & Gas, industria y servicios. Administradora de Empresas, especialista en seguridad industrial, higiene ocupacional y gestión ambiental, gerencia de mercadeo, gestión de residuos sólidos.

Consultora Empresarial, speaker internacional, mentora, auditora y docente universitaria impulsando proyectos con triple impacto: económico, social y ambiental.

Autora y referente en programas de salud mental empresarial, sostenibilidad corporativa e innovación aplicada al contexto laboral, Elena promueve una visión más humana y consciente de la SST. Su misión es clara: construir organizaciones seguras, responsables y resilientes, donde el cuidado de las personas sea el eje de la productividad y el crecimiento sostenible.

elenalaraflorian@gmail.com

# El Elefante Criminal en la Sala de Juntas



## La amenaza que los CEO en América Latina **PREFIEREN NO NOMBRAR**

**E**n muchas empresas de América Latina se discute de crecimiento, innovación y sostenibilidad, pero hay un tema que permanece intangible, aunque se siente en el aire como un silencio espeso: la criminalidad organizada. El elefante está ahí, en la sala, entre memorandos y balances; pero nadie quiere verlo.

Mientras las estrategias corporativas se alinean con metas ESG (Ambientales, Sociales y de Go-

bernanza) como de transformación digital, el crimen organizado ha evolucionado en paralelo, mimetizándose con estructuras legales, penetrando cadenas de suministro y lavando capitales en operaciones legítimas. Ha dejado de ser un fenómeno ajeno para convertirse en actor económico regional, con métodos más sofisticados que muchos conglomerados y sin competencia.



Competen con redes criminales que juegan con otras reglas: sin impuestos, sin auditorías, sin códigos de ética. Estas organizaciones han aprendido que la corrupción es más rentable que la violencia. No necesitan disparar cuando pueden firmar convenios. No buscan notoriedad: buscan permanencia.

Y ahí está el problema. Los CEO, que no gestionan el riesgo criminal están simplemente financiándolo.

La informalidad, tan frecuente en la región, ya no es solo un escollo administrativo, es una trampa estructural. Empresas que toleran zonas grises —por conveniencia o por omisión— se vuelven vulnerables a extorsiones, infiltraciones y alianzas peligrosas. El crimen organizado no entra por la fuerza, entra por la puerta de proveedores sin verificar, licitaciones opacas y políticas de cumplimiento meramente decorativas.

### **Negar la amenaza no es neutralidad, es complicidad silenciosa.**

Los costos de esta ceguera son invisibles, hasta que se materializan, y cuando lo hacen, la caída es estrepitosa: pérdida de activos, daño reputacional, fuga de talento, sanciones legales y pér-

dida de confianza de los stakeholders. Todo por no asumir a tiempo que el crimen organizado no necesita asaltar una oficina: le basta con firmar un contrato.

En América Latina, las estructuras criminales no solo trafican drogas o personas. También manipulan precios, financian campañas políticas, controlan sectores extractivos y operan como holding empresarial paralelo. Usan a los Estados cuando conviene y los eluden cuando estorban. El resultado es un ecosistema híbrido donde legalidad e ilegalidad se confunden, y donde muchas empresas creen —erróneamente— que mantenerse al margen las mantiene a salvo.

**Pero el crimen organizado ya no pide permiso: participa.**

### **LOS DATOS LO CONFIRMAN**

**Países con estructuras institucionales débiles y baja cultura de legalidad exhiben los mayores niveles de penetración criminal. Y aunque el problema es regional, sus consecuencias son globales: mercados distorsionados, inversiones en riesgo y gobernanza empresarial contaminada. La globalización del delito no conoce fronteras; pero sí reconoce vacíos de liderazgo.**

Por eso, no se trata de colocar más rejas ni tercerizar funciones. Se trata de comprender que la seguridad debe pensarse como un eje estratégico transversal, comparto con ustedes mis recomendaciones mejor alineadas al contexto corporativo:

- Integrar mapas de criminalidad en los análisis de riesgo corporativo,
- Formar alianzas público-privadas que anticipen patrones delictivos,
- Fortalecer programas de integridad que no dependan de voluntades individuales,
- Alinear indicadores de seguridad con los de rentabilidad y reputación, pero sobre todo:

Preparar a la alta dirección en escenarios de crisis criminal donde la pasividad no es opción.

Porque la amenaza más peligrosa no es la que se desconoce, es la que se conoce y se decide ignorar.

### **Máster en Estrategia Marítima, triple certificado CPP, PSP y PCI por ASIS International**

**EJECUTIVO  
LUIS EMILIO  
GONZALES  
SAPONARA CPP,  
PCI, PSP (Perú)**



Ejecutivo senior en gestión de riesgos y protección de activos con más de 20 años de trayectoria estratégica en seguridad física, financiera y continuidad de negocio. Máster en Estrategia Marítima, triple certificado CPP, PSP y PCI por ASIS International. Generador de retornos de inversión de hasta 7:1 en proyectos de alta complejidad. Referente en optimización de programas de seguridad, formación de equipos de élite y prevención de pérdidas en sectores críticos.

# La CIBERSEGURIDAD

## Y LA TEORÍA DE LOS SISTEMAS COMPLEJOS

A woman with long brown hair is shown from the chest up. She is wearing a dark blue blazer over a light-colored top. Her right hand is touching a transparent screen or interface that displays various data visualizations: a bar chart with values like 50, 82, and 95, and some circular icons. A glowing blue brain-like pattern is visible behind her head. She has a serious expression.

**E**n la era digital actual, la ciberseguridad se ha convertido en una preocupación primordial para individuos, empresas y gobiernos. La creciente interconexión de dispositivos y sistemas ha dado lugar a una complejidad sin precedentes en la infraestructura tecnológica global. Para abordar eficazmente los desafíos que plantea esta complejidad, es esencial adoptar enfoques innovadores. Uno de estos enfoques es la Teoría de los Sistemas Complejos, que ofrece una perspectiva única y poderosa para comprender y gestionar la ciberseguridad.

**¿Qué es exactamente la Teoría de los Sistemas Complejos?** Es un campo de estudio que se centra en cómo interactúan los componentes de un sistema y cómo estas interacciones dan lugar a comportamientos emergentes. A diferencia de los sistemas simples, donde las relaciones entre los componentes son lineales y predecibles, los sistemas complejos presentan interacciones no lineales y adaptativas. Esto significa que el comportamiento del sistema en su conjunto no se puede predecir fácilmente a partir del comportamiento de sus partes individuales.

La teoría de los sistemas complejos nos enseña que el

**Un Enfoque Innovador para Proteger el Mundo Digital**





## Uno de estos enfoques es la Teoría de los Sistemas Complejos, que ofrece una perspectiva única y poderosa para comprender y gestionar la ciberseguridad.

ciberespacio no es simplemente una colección de dispositivos y redes individuales, sino un sistema interconectado y dinámico. Las interacciones entre sus componentes pueden generar comportamientos emergentes y difíciles de predecir, lo que dificulta la detección y prevención de ataques cibernéticos.

La infraestructura de ciberseguridad de una organización puede considerarse un sistema complejo debido a la multitud de componentes interconectados, incluidos hardware, software, redes y personas. Cada uno de estos componentes interactúa de manera dinámica, lo que puede dar lugar a vulnerabilidades imprevistas y amenazas emergentes. Por ejemplo, una actualización de software aparentemente inofensiva podría desencadenar una cadena de eventos que exponga nuevas debilidades en el sistema.

**Entonces, ¿cómo podemos aplicar la Teoría de los Sistemas Complejos en la ciberseguridad?** Fundamentalmente, implica un cambio en nuestra aproximación a la protección de la infraestructura digital. Algunas estrategias claves que podrían mencionarse son las siguientes:

**Análisis Holístico:** En lugar de centrarse en componentes individuales, es crucial analizar el sistema en su totalidad. Esto permite identificar interaccio-

nes y dependencias críticas que podrían pasar desapercibidas en un enfoque fragmentado.

**Resiliencia y Adaptabilidad:** Los sistemas complejos son inherentemente adaptativos. Implementar medidas que fortalezcan la resiliencia del sistema, como la diversificación de herramientas de seguridad y la capacitación continua del personal, puede ayudar a mitigar los efectos de las amenazas emergentes.

**Detección de Patrones Emergentes:** Utilizar técnicas avanzadas de análisis de datos y aprendizaje automático puede ayudar a detectar patrones y comportamientos inusuales en el sistema. Esto permite una respuesta más rápida y eficaz a las amenazas antes de que se conviertan en incidentes de seguridad.

Para ejemplificar aún más lo que quiero demostrar, voy a mencionar algunos ejemplos concretos de ciberataques y cómo se relacionan con dicha teoría.

**Ataques de ransomware a infraestructuras críticas:** El ataque de ransomware a Colonial Pipeline (2021) interrumpió el suministro de combustible en la costa este de Estados Unidos, y los ataques a hospitales y sistemas de salud que paralizan servicios vitales.

## **Relación con la teoría de los sistemas complejos:**

**Estos ataques demuestran cómo la interdependencia de los sistemas críticos puede tener consecuencias devastadoras.** Un ataque a un componente (en este caso, la red de Colonial Pipeline) puede generar efectos en cascada en otros componentes (el suministro de combustible, la economía, etc.). La complejidad de estas infraestructuras dificulta la protección y la respuesta a los ataques. Además, la vulnerabilidad de un solo punto de entrada puede afectar a todo el sistema.

## **Ataques a la cadena de suministro de software:**

El ataque a SolarWinds (2020), en el que los atacantes comprometieron una actualización de software legítima para acceder a las redes de miles de organizaciones.

## **Relación con la teoría de los sistemas complejos:**

Estos ataques explotan las interconexiones entre proveedores de software y sus clientes. La complejidad de las cadenas de suministro dificulta la detección de código malicioso. Un solo punto de compromiso puede tener un impacto masivo en todo el ecosistema, donde la confianza depositada en un software puede ser el punto de entrada para dañar a miles de usuarios.

## **Ataques DDoS (Denegación de Servicio Distribuido) a gran escala:**

Ataques que paralizan servicios en línea como redes sociales, plataformas de comercio electrónico o servicios bancarios.

## **Relación con la teoría de los sistemas complejos:**

Estos ataques demuestran cómo la coordinación de múltiples dispositivos (botnets) puede generar un comportamiento emergente que supera las defensas tradicionales. La complejidad de las redes de botnets dificulta la identificación y mitigación de los ataques. La reacción en cadena de peticiones a un servidor lo colapsa, mostrando el caos que se puede generar en un sistema complejo.

Esto demuestra que, de cierta manera, existe una sinergia entre la interdependencia de los sistemas y la vulnerabilidad de los mismos. Un ataque a un componente del sistema puede tener efectos en cascada en otros componentes, amplificando el impacto del ataque. Las vulnerabilidades en un área del sistema pueden ser explotadas para acceder a otras áreas, resaltando la importancia de una seguridad integral.

Podemos decir que existe un comportamiento emergente, ya que los ataques ciberneticos pueden evolucionar y adaptarse a las defensas, lo que requiere una vigilancia constante y una capacidad de respuesta ágil. La propagación de malware y la formación de botnets son ejemplos de comportamientos emergentes que pueden ser difíciles de controlar.

El análisis de redes complejas puede ayudar a identificar puntos críticos en la infraestructura digital y a predecir la propagación de ataques. Los modelos basados en la teoría de sistemas complejos pueden simular el comportamiento de los atacantes y evaluar la eficacia de las estrategias de defensa. La inteligencia artificial y el machine learning son herramientas que ayudan a analizar la gran cantidad de datos que se generan en un sistema complejo y, de esta manera, anticipar posibles ataques.



**Adolfo M. Gelder**

Auditor de Normas ISO de Seguridad, Consultor Técnico Criminalista, con Maestría en Gerencia de Protección y Seguridad Aplicada, Experto en Ciencias Forenses, Especialista en Ciberseguridad. (Venezuela)



**CORPROJO**  
SERVICIOS INTEGRALES

**CORPORACIÓN ROJO**

Innovación y Seguridad en Movimiento

## Servicios de **RASTREO SATELITAL** de Vehículos

- La seguridad, control y eficiencia que tu flota merece!

Con nuestro servicio de rastreo satelital, llevarás la gestión de tus vehículos al siguiente nivel



Asistencia 24/7 para resolver cualquier inconveniente técnico.

### Soporte Técnico Premium

- Actualizaciones constantes del software para garantizar la mejor experiencia.



- RASTREA
- MONITOREA
- CONTROLA



**NOSOTROS**  
te ayudamos a resolver  
esos problemas

Nos destacamos al brindar una solución integral que aborda las principales necesidades de las empresas modernas:



#### Control absoluto

Olvídate de rutas no autorizadas, excesos de velocidad o falta de información en tiempo real.



#### Seguridad preventiva

Minimiza riesgos y responde rápidamente a incidentes gracias a nuestras alertas inteligentes.



#### Optimización operativa

Mejora la eficiencia con herramientas que facilitan la gestión diaria y la planificación de tus viajes.

La seguridad no tiene precio, pero sí una solución confiable y accesible!



[info@corporacionrojo.com](mailto:info@corporacionrojo.com)

# HAITI, INSEGURIDAD TOTAL



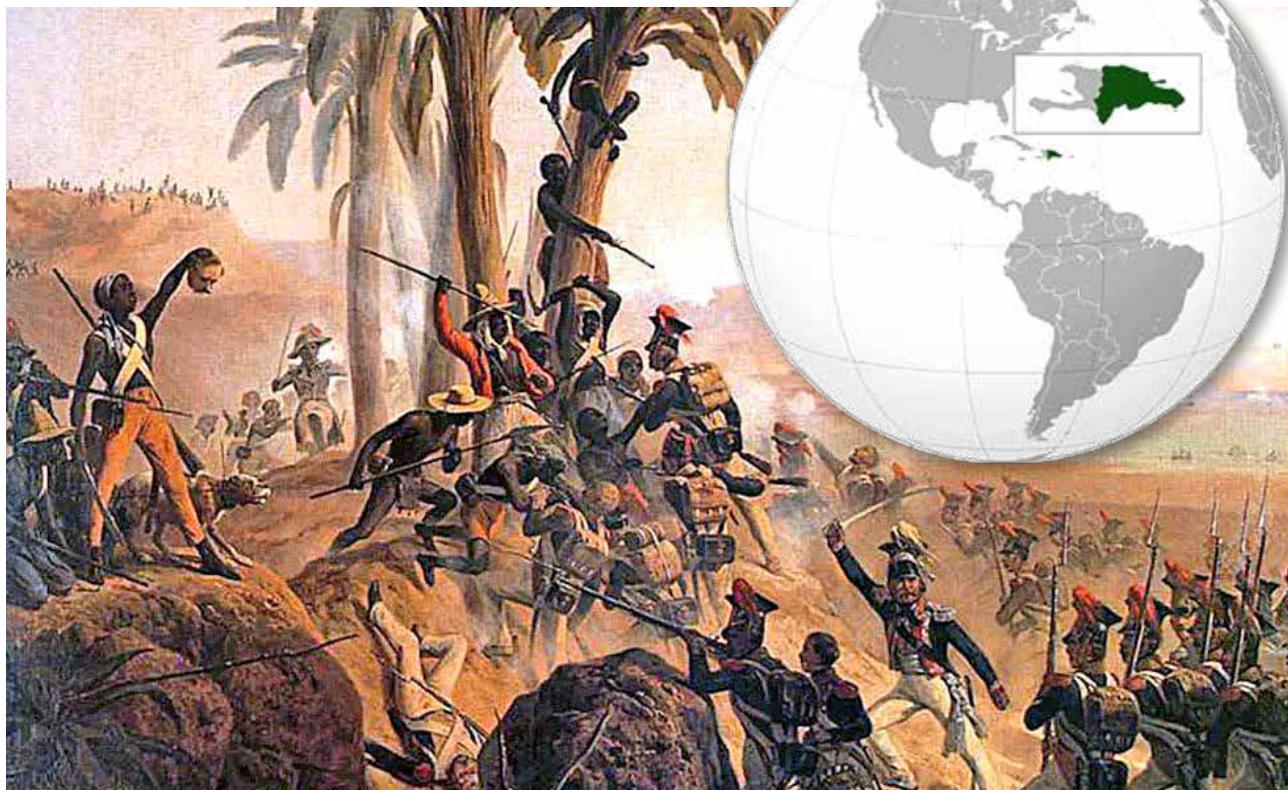
**U**na trágica noticia conmocionó el medio cultural e histórico del Caribe. Las pandillas que azotan actualmente Haití con su vandalismo, incendiaron el Hotel Oloffson, ícono de la arquitectura “gingerbread” y de la historia cultural caribeña. El Oloffson de Puerto Príncipe era mítico, con sus secretos, historias de amor, recuerdos de fiestas célebres y su anuario de visi-

tantes ilustres. En el hotel, Graham Greene escribió “Los Comediantes”, que se desarrolla en la época de Duvalier, siendo el escenario de la novela el Hotel Trianon, nombre que le puso al Oloffson. Truman Capote era asiduo visitante, igual que James Jones, Charles Addams, Sir John Gielgud, Jacqueline Kennedy Onassis y Mick Jagger. Sobre los Comediantes se hizo una película con Richard Burton , Elizabeth Taylor , Alec Guinness , Peter Ustinov.

# Haití, rico en historia

FUE LA PRIMERA “REPÚBLICA NEGRA”

DEL MUNDO



**A**l independizarse de Francia en el año 1804, después de vencer al ejército de Napoleón conducido por su cuñado, el general Leclerc. Su independencia fue fruto de una rebelión de esclavos liderada por Toussaint Louverture y fue, después de los Estados Unidos, el segundo país en lograr su independencia en América. Haití tuvo muchos gobernantes y hasta un rey, Christophe, conocido como Enrique I de Haití, quien construyó un suntuoso palacio en Cap Haitien y se rodeó con una nobleza local.

Más adelante, en 1816, el presidente Petion apoyó a Simón Bolívar con barcos, un ejército y dinero, para lograr la independencia de Venezuela y otros países sudamericanos. Después vinieron gobiernos nefastos y en 1957, una dictadura de casi 30 años con los Duvalier, Papa Doc y su hijo Baby Doc. Finalmente en 2016 Juvenel Moïse, asume la presi-

dencia hasta su asesinato por un sicario, ex militar colombiano en 2021, quien con otros dos esbirros entró a la habitación del presidente y su esposa. Desde entonces, el país, que quedó bajo el mandato del primer ministro, Ariel Henry, se encuentra sin presidente y sin celebrar elecciones libres. A partir de ese hecho, la situación, ya caótica, deviene insostenible y ahora son las pandillas unificadas en el grupo llamado Viv Ansanmb, nombre en creole que significa “vivir juntos”, del francés “vivre ensemble” que manejan el país.

Haití es el país más pobre del hemisferio occidental donde el 80% de la población vive en la pobreza y ahora se ha convertido en un estado en crisis, vandalizado por bandas de delincuentes, que se están uniendo, está casi sin gobierno y con carencia total de seguridad.



**El histórico hotel Oloffson**, fue completamente destruido por un incendio, en Puerto Príncipe, Haití, en un hecho que es atribuido a la coalición Viv Ansanm, encabezada por el temible Jimmy Chérizier, alias Barbecue.

Haití tiene una extensión de 27,755 Km<sup>2</sup>, ocupando el tercio occidental de la isla La Española, en el mar Caribe, que comparte con República Dominicana. Su población es de 11.5 millones de habitantes y sus idiomas son el francés y el creole. La organización social es singular, sin comparación con ningún país de América. En ella se superponen la estructura del gobierno oficial, con la organización popular que tiene a los "chefs de quartier ou de village", como los mandos absolutos en los barrios y pequeños pueblos. A esto se suma el poder de los Oungans, sacerdotes Vudú, quienes dominan el territorio de sus grupos religiosos.

Haití, sin embargo, es rico en cultura, la literatura, la pintura, la música, la arquitectura, la artesanía, el cine, son parte de la muy valiosa cultura de este país, sometido permanentemente a la violencia de los hombres y de la naturaleza. Los artesanos haitianos y su producción en madera, fibra, cerámica, metal es muy reputada y buscada por los turistas. Como referencia señalemos que en el 2009 los autores haitianos habían ganado 11 premios internacionales de literatura, y las películas de directores haitianos se pasaban en los

mejores auditorios cinéfilos. La artesanía que se vende en las islas caribeñas francesas, inglesas, holandesas y americanas, en su mayoría, son hechas en Haití. La música haitiana tiene su máxima representación en el ritmo Compas (en francés) y Kompas (en el creole haitiano), música, proveniente de ritmos africanos y el baile de salón europeo; pero, la "verdadera", es aquella salida de cuatro notas de las bandas "rá-rá" que aparecen en tiempo de cuaresma para celebrar ritos religiosos.





**Langosta “bucané” a la parrilla:** una fotografía apetecible que muestra langostas asadas sobre leña, evocando esas cenas frente al mar en el estilo rústico bucanero haitiano.



**Un terremoto de 7,2 grados de magnitud** se registra en Haití a 10 kilómetros de profundidad este 14 de agosto de 2021.

## La comida haitiana

La comida haitiana de sabor creole tiene igualmente sus encantos. La langosta “bucané”, asada en leña a las orillas de las playas, son una reminiscencia de las comidas de los bucaneros; el “lambi”, (caracol) en sopa o salteado, los pescados asados cubiertos de especias creoles, al igual que los crevettes creole (camarones) son delicia para el paladar más exquisito. La pintura en su estilo “naif”, es famosa y ha inspirado a pintores famosos en el mundo.

## Desastres

Haití es también rico en desastres, además de los constantes ciclones y tormentas tropicales que asolan su territorio, en enero del 2010, un terremoto de 7.0 grados destruyó casas, edificios, infraestructura, dejando más de 200 mil fallecidos y 1.5 millones de personas sin hogar y 10 millones de toneladas en escombros.

La remoción de escombros dejó al descubierto muchas fallas de construcción relacionadas con la inseguridad de la infraestructura. Se descubrió que las construcciones que más daños sufrieron fueron la construidas en concreto armado. Las columnas tenían tres fierros verticales en lugar de cuatro y los estribos, que deben colocarse cada 15 cm, estaban puestos cada 50 cm. Lo cual, por ahorro de material, debilitaba y daba inseguridad a las obras. Por otro lado, al revisar las mezclas utilizadas, la relación cemento arena no tenían las proporciones adecuada. Esto, entre otras fallas, dio una gran inseguridad a las construcciones que fueron presa fácil del sismo. Como anécdota, se cuenta que muchos ingenieros y constructores fueron amenazados por los propietarios de las construcciones derribadas y tuvieron que huir del país.

## Crisis políticas y económicas

El país lleva años sufriendo las crisis políticas y económicas, sin embargo, la crisis actual es peor que cualquier otra, 30 personas han muerto en las manifestaciones, hay escasez de combustible, los hospitales redujeron sus servicios, han cerrado las escuelas y las empresas han dejado sin trabajo a miles de trabajadores, el transporte público está interrumpido y la huida hacia República Dominicana-

na, Estados Unidos, Canadá, se ha intensificado, llegando ahora hasta Chile, donde existe una gran colonia haitiana.

Uno de los incidentes más alarmantes fue la toma de la ciudad de Mirebalais, donde más de 500 reclusos escaparon en el quinto motín carcelario en menos de un año. La violencia supera la capacidad policial incluso con el apoyo de las Fuerzas Armadas y la "Misión Multinacional de Apoyo a la Seguridad". Más de 1000 personas han sido asesinadas y al menos 60,000 debieron desplazarse huyendo de la violencia, lo que agravó una crisis humanitaria que ya afecta a más de un millón de personas.

## La inseguridad

Ante el terror generado es casi total, las fuerzas armadas y la policía no pueden controlar las acciones vandálicas de las pandillas, controladas, se dice, por el narcotráfico.

"Cuando todo cae queda la cultura", declaraba Dany Laferrière, escritor haitiano galardonado con el premio Médicis francés por «El enigma del regreso» («L'Énigme du retour»). Sin embargo, con los atentados a ésta, comienzo a dudarlo.

Por último, hace poco, se ha descubierto que Haití, en la costa sudeste, tiene la segunda mayor reserva de iridio del mundo, después de Sudáfrica, metal cuyo precio es tres veces más caro que el oro, alcanzando los 6.000 dólares por onza. Se estima que en suelo haitiano podrían estar enterrados metales preciosos por valor de 20,000 millones de dólares. Lo que nos recuerda la invasión norteamericana en Haití de 1915 a 1934, para salvaguardar los intereses norteamericanos y salvar al país de la violencia en que también vivía en esa época.



Autor:  
**JORGE  
CABRERA  
GOMEZ**



(Trujillo-Perú, 1940), Arquitecto urbanista, experto de NN UU con misiones en África, Suramérica, Centroamérica y el Caribe.

Autor de 7 novelas y una antología: EL BAO-BAB; CAMP CHARLIE-EL DESARRAIGO, finalista Premios COPE-2015; LA UTOPIA-PLAN DE FUGA; TRES INGENIEROS; EL PINTOR DE NATURALEZA MUERTA; EL OTOÑO DE GINA; FANTASIAS DE ARENA; PROSAS Y VERSOS RESCATADOS DEL OLVIDO. Ganador de microrrelatos en Concurso Literario COVID-19, Almandino Editores. Galardonado como "Los Rostros del Bicentenario", por la fundación Crea Bicentenario, 2021.

**En Haití, tomar el autobús es casi una experiencia artística.** El medio de transporte más común en Haití, el "tap tap" son pequeños autobuses pintados vistosamente y tallados en su totalidad con efigies religiosas y vudú o figuras públicas.



# Atractivo del riesgo

## Y VULNERABILIDAD DEL ACTIVO DESDE LA PERSPECTIVA DEL AGRESOR



**E**n el ámbito de la seguridad patrimonial, la protección de activos se enfoca tradicionalmente en la fortificación de defensas y la mitigación de debilidades internas. Sin embargo, para desarrollar estrategias verdaderamente resilientes, es imperativo adoptar una perspectiva contra intuitiva: la del agresor. Comprender cómo un potencial atacante evalúa el atractivo de riesgo y la vulnerabilidad de un activo es la clave para anticipar y neutralizar amenazas de manera proactiva.

# La Mente del Agresor:

## Un Análisis Costo-Beneficio

Desde el punto de vista del agresor, toda operación ilícita es un cálculo de riesgo-recompensa. No buscan la oportunidad más fácil, sino la que ofrece la relación más favorable entre el esfuerzo, el riesgo inherente y el beneficio esperado. Este análisis trasciende la mera detección de una vulnerabilidad obvia; implica una evaluación holística que pondera factores psicológicos, técnicos y logísticos.

### Factores de Atractivo del Activo (Recompensa)

El atractivo de un activo para un agresor no se limita a su valor monetario directo. Incluye una serie de dimensiones que lo hacen un objetivo deseable:

#### Valor Intrínseco y Extrínseco

Más allá del valor de mercado (dinero en efectivo, joyas, tecnología), el agresor considera el valor de uso (equipos críticos para la operación de la empresa), el valor estratégico (información confidencial, propiedad intelectual) e incluso el valor simbólico o de prestigio (obras de arte, objetos colecciónables). Para un delincuente organizado, el atractivo puede residir en la facilidad de reventa o en la utilidad del activo para otras actividades ilícitas.

#### Volumen y Concentración

Un gran volumen de activos en un solo lugar (un almacén con mercancía de alto valor, una bóveda bancaria, productos terminados en espera del registro de inventario) incrementa su atractivo. La concentración minimiza la logística necesaria para obtener una recompensa significativa.

#### Portabilidad y Disposición

La facilidad con la que el activo puede ser movido y posteriormente transformado en valor monetario o utilizado es crucial. El dinero en efectivo, joyas o productos electrónicos pequeños y de alto valor son intrínsecamente más atractivos que maquinaria pesada o estructuras fijas, a menos que el agresor tenga la capacidad logística para moverlos o la intención de desmantelarlos para la venta de partes.

#### Valor de la Información

En la era digital, la información es un activo primordial. Bases de datos de clientes, secretos comerciales, planos de proyectos o datos financieros pueden ser más valiosos que los bienes tangibles. El atractivo reside en su potencial de venta en el mercado negro, extorsión o uso para futuros ataques.



## Factores de Vulnerabilidad del Activo (Riesgo Percibido por el Agresor)

La vulnerabilidad, desde la perspectiva del atacante, se refiere a la facilidad percibida para superar las defensas y alcanzar el objetivo con un riesgo aceptable de detección o captura. No es solo la ausencia de una barrera, sino la debilidad explotable en un sistema integral:



### ■ Vulnerabilidades Físicas:

1. Perímetros Débiles: Cercas bajas, portones sin supervisión, muros sin reforzar, iluminación deficiente o ángulos ciegos para las cámaras.
2. Puntos de Acceso: Puertas o ventanas mal aseguradas, cerraduras de baja calidad, o la falta de sistemas de control de acceso robustos.
3. Sistemas de Alarma y CCTV: Equipos obsoletos, mal mantenidos, sin respaldo energético o con puntos ciegos. La ausencia de monitoreo 24/7 o la lentitud en la respuesta a las alertas son indicadores clave de vulnerabilidad.

### ■ Vulnerabilidades Humanas/Operacionales

1. Falta de Conciencia o Capacitación: Personal de seguridad desmotivado, sin formación adecuada en protocolos de emergencia o respuesta a incidentes.
2. Procedimientos Laxos: Controles de acceso de visitantes deficientes, falta de supervisión en áreas restringidas, o protocolos de manejo de llaves y códigos poco estrictos.
3. Colusión Interna: La presencia de un “topo” dentro de la organización reduce drásticamente el riesgo para el agresor, al proporcionar información privilegiada sobre horarios, rutinas, sistemas de seguridad y puntos débiles. Esta es una de las vulnerabilidades más críticas y difíciles de detectar.
4. Fatiga de Seguridad: La complacencia o el exceso de confianza por parte del personal, que lleva a ignorar procedimientos o a bajar la guardia.

### ■ Vulnerabilidades Tecnológicas/Cibernéticas

1. Sistemas Obsoletos: Software y hardware sin actualizar, lo que los hace susceptibles a exploits conocidos.
2. Configuración Incorrecta: Fallas en la implementación de medidas de seguridad (firewalls mal configurados, contraseñas débiles o por defecto).
3. Falta de Segmentación: Una red plana permite al agresor, una vez dentro, moverse lateralmente sin restricciones.
4. Ingeniería Social: La capacidad de manipular al personal para obtener información o acceso, explotando la confianza o el desconocimiento. Esto puede ser una “puerta de entrada” para ataques cibernéticos o físicos.

## La Sinergia entre Atractivo y Vulnerabilidad: El Eje de Decisión del Agresor

El agresor no evalúa el atractivo y la vulnerabilidad de forma aislada. Más bien, busca la intersección óptima entre un activo de alto valor y una vulnerabilidad explotable. Un activo de inmenso valor, pero con defensas impenetrables, es poco atractivo debido al riesgo. Por el contrario, un activo de bajo valor, aunque completamente desprotegido, tampoco justifica el esfuerzo.

**La fórmula mental del agresor podría resumirse en:**

<b>Atractivo del Objetivo=</b>	Valor Percibido del Activo
Riesgo Percibido de Detección o Captura	



**Donde el Riesgo Percibido es directamente proporcional a la robustez de las defensas y la eficiencia de los sistemas de respuesta, e inversamente proporcional a las vulnerabilidades existentes.**

## Implicaciones para el Profesional de la Seguridad Patrimonial

Para los profesionales de la seguridad patrimonial, esta perspectiva obliga a un cambio de paradigmas, por lo cual deben implementar:

- 1. Mapeo de Activos Críticos:** No solo en términos de valor monetario, sino de su impacto estratégico, operacional y reputacional. Identificar los “joyas de la corona” que, al ser comprometidas, causarían el mayor daño.
- 2. Análisis de Vulnerabilidades desde Afuera:** Realizar evaluaciones de seguridad (pen-tests, simulacros de intrusión, auditorías de seguridad física) con la mentalidad de un atacante. ¿Dónde buscaría el agresor? ¿Qué rutas tomaría? ¿Qué debilidades explotaría?
- 3. Inteligencia de Amenazas:** Entender las tácticas, técnicas y procedimientos (TTPs) de los agresores relevantes para su sector. Esto incluye desde la delincuencia común hasta grupos de crimen organizado o actores patrocinados por estados.

- 4. Integración de Seguridad Física y Lógica:** Reconocer que las vulnerabilidades ciberneticas pueden ser la puerta de entrada a ataques físicos, y viceversa. Una estrategia de seguridad holística debe abordar ambas dimensiones de forma interconectada.
- 5. Fomento de la Cultura de Seguridad:** El eslabón humano es a menudo el más débil. Capacitar constantemente al personal, fomentar la notificación de anomalías y promover una cultura de vigilancia y cumplimiento de protocolos.
- 6. Disuasión Activa y Pasiva:** Implementar medidas que no solo dificulten el acceso, sino que también eleven la percepción de riesgo para el agresor, haciéndolo desistir. Esto incluye desde la visibilidad de la seguridad (guardias, cámaras) hasta la velocidad de respuesta.



## Conclusión

La seguridad patrimonial no puede ser un ejercicio reactivo o meramente defensivo. Al adoptar la perspectiva del agresor y analizar meticulosamente el atractivo de riesgo y la vulnerabilidad de los activos, los profesionales de la seguridad pueden trascender las medidas superficiales.

Este enfoque proactivo permite identificar y mitigar los puntos ciegos, fortalecer las defensas donde más importa y, en última instancia, construir un entorno de seguridad más robusto y adaptativo, desincentivando al agresor antes de que el ataque se materialice.

La verdadera protección reside en pensar como el adversario, anticipar sus movimientos y hacer que el riesgo de la operación sea inaceptablemente alto para su objetivo de recompensa.

Recordemos una de las premisas contenidas en la obra El Arte de la Guerra de Sun Tzu, cito; ""cada batalla se gana antes de pelear"... fin de la cita. Esto implica que la planificación y la comprensión del enemigo son cruciales para el éxito, incluso antes de que comience la batalla.

Autor:  
**Marcos  
Carrillo  
Castillo**



### Perfil Profesional

El Mayor Marcos Carrillo Castillo es un oficial retirado del Ejército de Venezuela con más de 38 años de experiencia en seguridad. Su trayectoria incluye 22 años de servicio militar en unidades tácticas y administrativas del Ejército Venezolano y 16 años en el sector empresarial privado.

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 patrimonial, con experiencia en análisis y gestión de riesgos, así como en control de pérdidas.

Actualmente, es miembro activo de la International Foundation Protection Officers (IFPO) y Subdirector Ejecutivo de BGMC Group.

# Crimen Organizado Transnacional:

## Narcotráfico, Corrupción y su Impacto Global

El crimen organizado trasciende fronteras y afecta directamente la economía, la estabilidad social y la gobernabilidad de los países. Las redes criminales que controlan el narcotráfico, junto con la corrupción y la migración forzada, presentan un desafío monumental para los líderes empresariales y gubernamentales. En este artículo, exploramos los riesgos y las estrategias para enfrentar este fenómeno.

### El Crimen Organizado y el Narcotráfico: Una Amenaza Transnacional

Las redes criminales de alcance global han transformado el narcotráfico en un negocio multimillonario que cruza fronteras con facilidad. América Latina, al ser uno de los mayores productores y rutas de tránsito de drogas ilegales, se encuentra en el epicentro de esta problemática. Organizaciones como el Tren de Aragua y el PCC brasileño utilizan sus conexiones transnacionales para mover cocaína y otros narcóticos hacia mercados en Europa, Asia y Norteamérica. La debilidad institucional y la falta de cooperación internacional efectiva contribuyen a que estos grupos prosperen, perpetuando la violencia y la inseguridad en la región.





---

**La corrupción  
es el pilar que  
sostiene la  
expansión del  
crimen  
organizado**

---

## **Impacto: Económico y Social del Crimen Organizado**

El impacto económico del crimen organizado es devastador. La pérdida de inversión extranjera directa, el aumento de los costos de seguridad, y la desconfianza en las instituciones públicas son solo algunas de las consecuencias que enfrentan los países afectados. La violencia generada por estas organizaciones no solo destruye comunidades, sino que también limita las oportunidades de desarrollo y reduce la calidad de vida de millones de personas en América Latina. A nivel social, la criminalidad influye en la vida cotidiana, desde la extorsión de pequeños negocios hasta el control territorial en áreas urbanas, afectando a las poblaciones más vulnerables.

## **La Corrupción: El Aliado Silencioso del Crimen Organizado**

La corrupción es el pilar que sostiene la expansión del crimen organizado. A través de sobornos, amenazas y la infiltración en instituciones gubernamentales, estas organizaciones logran evadir la ley y expandir sus operaciones. Funcionarios públicos, fuerzas de seguridad y hasta el poder judicial son objetivos constantes de estas redes, que utilizan la corrupción como una herramienta estratégica para garantizar su impunidad. El narcotráfico, en particular, depende en gran medida de la corrupción para mover sus productos y lavar los ingresos obtenidos de manera ilícita.



## Vinculación con la Migración: Redes de explotación y trata de personas

La migración forzada y la falta de oportunidades en los países de origen son aprovechadas por el crimen organizado para expandir sus redes de trata de personas y tráfico de migrantes. Estas organizaciones criminales engañan a los migrantes, prometiéndoles un mejor futuro, solo para explotarlos y someterlos a condiciones inhumanas. La militarización de las fronteras y la falta de protección adecuada incrementan la vulnerabilidad de estas personas, creando un ciclo de abuso y explotación que va mucho más allá del tráfico de drogas.



## Desafíos: Riesgos para las empresas y el rol de los Líderes de Seguridad

Las empresas no están exentas de los riesgos asociados con el crimen organizado. Desde la extorsión hasta la infiltración de redes criminales en sus operaciones, los líderes de seguridad deben estar siempre alertas y preparados para enfrentar estos desafíos. Es esencial que las compañías implementen medidas de seguridad robustas y colaboren con las autoridades para proteger sus activos y a su personal. Los líderes de seguridad tienen un rol crucial en este escenario, actuando como la primera línea de defensa y asegurando la resiliencia corporativa frente a estas amenazas.

## Acciones efectivas: La importancia de denunciar y la respuesta de los Estados

La colaboración entre el sector privado y las fuerzas del orden es fundamental para desmantelar las redes criminales. Las denuncias por parte de empresas y ciudadanos son un componente clave para generar acciones efectivas contra el crimen organizado. Sin embargo, las respuestas estatales a menudo se centran en políticas de 'mano dura' que han demostrado ser ineficaces y a veces contraproducentes, agravando la violencia y la fragmentación de los grupos criminales. Es vital adoptar enfoques más integrales que incluyan prevención, sanción efectiva y la modernización de las instituciones encargadas de la seguridad.



## Aliados Clave: Consultorías en Seguridad Estratégica Corporativa

Las empresas de consultoría en seguridad, como BESAFE INTERNACIONAL, juegan un papel esencial al asesorar a empresas y gobiernos en la gestión de riesgos asociados con el crimen organizado. Su expertise en seguridad estratégica permite desarrollar políticas efectivas y proteger los intereses corporativos en un entorno cada vez más complejo y peligroso.

El crimen organizado transnacional es un problema de gran escala que requiere una respuesta coordinada y estratégica. Las empresas, los líderes de seguridad y las consultoras especializadas deben trabajar juntos para enfrentar estos desafíos y proteger tanto a las personas como a los activos corporativos. La lucha contra estas redes no solo es un imperativo de seguridad, sino también una responsabilidad colectiva para asegurar un futuro más seguro y estable.

## Referencias

BCN\_GF\_Caracterizacion\_del\_crimen\_organizado\_en\_Latinoamerica.pdf

Riesgo Político América Latina 2024

Valeska Troncoso, La Tercera, 2024.

Iniciativa Global contra el Crimen Organizado Transnacional (GI-TOC).

**Amplia trayectoria profesional  
Actualmente es  
miembro del Comité  
de Governance and  
Finance del Board  
Latinoamericano (LAB)**

Autor:  
**HUMBERTO  
SANTIBÁÑEZ,  
CPP**



**Su enfoque combina conocimiento  
técnico, visión estratégica y compromiso  
con la profesionalización del sector de la  
seguridad en América Latina.**

Es Director Estratégico de Negocios en BeSafe Internacional y posee más de 30 años de experiencia, con más de dos décadas dedicadas a la seguridad corporativa. Ha liderado proyectos estratégicos en empresas nacionales e internacionales, integrando estándares como ISO 31000 y TAPA. Licenciado Investigador Policial, Licenciado en Seguridad y Defensa, cuenta además con diplomados en alta dirección, seguridad privada, seguridad de la información e integración de sistemas de protección. Fue gerente general de Besafe y ha sido un destacado líder voluntario en ASIS International, participando activamente a nivel nacional y global.

LA INTERNATIONAL POLICE ASSOCIATION

# PUNTO DE ENCUENTRO PARA TODOS LOS POLICÍAS DEL MUNDO



**L**a Asociación Internacional de Policía (I.P.A.) es una organización de amistad para miembros de las fuerzas policiales, tanto en activo como jubilados, sin distinción de rango, puesto, género, raza, idioma o religión. Nuestro lema es 'Servo per Amikeco' - Servicio a través de la amistad.

Somos una organización no gubernamental y nuestros objetivos son crear y fortalecer lazos de amistad entre los miembros del servicio de policía, promover la cooperación internacional en los campos sociales, culturales y profesionales, fomentar la coexistencia pacífica entre los pueblos y la preservación de la paz mundial, mejorar la imagen pública del servicio de policía y mejorar el reconocimiento de la IPA por parte de los organismos internacionales.

La IPA está comprometida con los principios establecidos en la Declaración Universal de Derechos Humanos adoptada por las Naciones Unidas en 1948, y tiene estatus consultivo (especial) ante el Consejo Económico y Social de las Naciones Unidas, y también tiene estatus consultivo ante la Organización de los Estados Americanos y la UNESCO.

Contamos con unos 372.000 miembros en casi 100 países, de los cuales 68 son Secciones Nacionales afiliadas, y estamos representados en seis continentes.



# Un poco de historia



## Arthur Troop

Un Sargento de la Policía de Lincolnshire (Inglaterra) emprendió la enorme tarea de fundar una organización de amistad para policías de todo el mundo.



**A**rthur Troop fundó la IPA el 1 de enero de 1950 bajo el lema en esperanto «Servo per Amikeco» (Servicio a través de la amistad). Arthur Troop se convirtió en el primer Secretario General de la Sección Británica. Su idea de una asociación que fomentara vínculos sociales, culturales y profesionales entre sus miembros, en un entorno sin distinción de rango, género, raza, idioma ni religión, se hizo realidad.

Con la ayuda de pioneros, Arthur Troop trabajó incansablemente para impulsar la fundación de otras Secciones Nacionales. Desde sus modestos comienzos, el mensaje de la IPA se arraigó rápidamente y la formación de nuevas Secciones en todo el mundo se aceleró. Pronto hubo secciones en la mayor parte de Europa Occidental. En 1955, en la primera reunión del Comité Ejecutivo Internacional en París, Arthur Troop se convirtió en el primer Secretario General Internacional, cargo que ocupó hasta su dimisión en 1966 por motivos personales.

En 1986, debido al aumento de miembros de la Asociación, se identificó la necesidad de personal permanente. Se reconoció que sería cada vez más difícil trasladar la administración de una Sección a otra, como se había hecho hasta entonces. Por ello, en 1987 se estableció un centro permanente en el Reino Unido, en la sede de la Sección del Reino Unido.

Aquí también se alojan los archivos de la Asociación, con registros que se remontan al principio, cuando nuestro fundador Arthur Troop comenzó a establecer contactos.

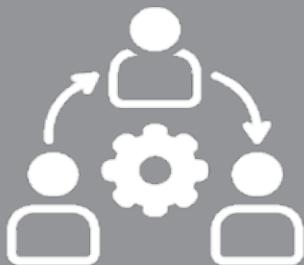
El Centro de Administración Internacional (IAC) es la oficina oficial de la IPA, mantenida por el Comité Ejecutivo Internacional y que emplea personal profesional.

Ubicado en Nottingham, Reino Unido, el IAC es el primer punto de contacto para cualquier pregunta de los miembros del IPA y del público en general.

En la actualidad la IPA cuenta con más de 372.000 miembros. Existen Secciones Nacionales en 70 países de todo el mundo, y hay más en proceso de afiliación. Hemos presenciado el crecimiento constante de la que se ha convertido, sin lugar a dudas, en la principal organización policial del mundo, tanto en número de miembros como en influencia.



# Organización de la IPA



**Junta Ejecutiva Internacional (IEB) es el órgano máximo de decisión de la IPA, está formado por policías de todo el mundo:**

Cada país afiliado cuenta con una Sección Nacional de la IPA, con estatutos propios, que no pueden ir en contra de los internacionales, siendo un reflejo fiel de los mismos.

En la actualidad, contamos con 68 Secciones Nacionales afiliadas, una Sección Nacional con afiliación provisional (Colombia) cinco Secciones Nacionales en formación, esponsorizadas por la Sección Nacional de IPA España (Costa Rica, República Dominicana, México y Bolivia) y Uruguay esponsorizada por la Sección Nacional de Perú.

Cada Sección Nacional, según sus intereses administrativos, puede a su vez crear Delegaciones/Regiones/Departamentos dentro de su territorio, a fin de distribuir la información a sus afiliados y resto de miembros de las fuerzas de seguridad del País.

## Internacional Executive Board

	• <b>Martin Hoffmann</b>	
	International President	
	• <b>Michael Walsh</b>	
	Vice President & Treasurer Finances	
	• <b>Jože Senica</b>	
	Secretary General	
	• <b>Oliver Hoffmann</b>	
	Chair International Relations Commission	
	• <b>Diego Trolese</b>	
	Chair Professional Commission	
	• <b>Christos Parginos</b>	
	Chair Socio-Cultural Commission	
	• <b>Jean Pierre Allet</b>	
	Treasurer Social Affairs	
	• <b>Clive Wood</b>	
	Head of Administration	



## QUE OFRECE LA IPA A SUS MIEMBROS

Viajar, ser miembro de IPA ofrece una amplia gama de oportunidades de viaje. Un vistazo a la página de eventos y noticias de nuestro sitio web ilustrará la variedad de opciones disponibles, desde Semanas de la Amistad en Rusia o Canadá hasta eventos de interés especial a los que puede unirse en España o Irlanda. Tanto si le apetece hacer senderismo en los Alpes austriacos como descubrir los tesoros de Sri Lanka, la IPA tiene algo para todos los gustos.

Además de las opciones de viajes organizados en grupo, la IPA también ofrece asistencia para viajes individuales o en familia. Una oportunidad única para ver el mundo desde la perspectiva de un local e intercambiar con otros policías sobre las implicaciones del trabajo policial en su país. Muchos de estos encuentros han dado lugar a amistades para toda la vida.

### Casas IPA



IPA House Dublin, Ireland

IPA posee más de 40 propiedades en 14 secciones de la IPA donde los miembros pueden alojarse en alojamientos a precios razonables.

Con ubicaciones que van desde lugares turísticos como París y Berlín, hasta los hermosos alrededores invernales de Laponia en Finlandia, hasta nuestro apartamento en la Costa Dorada de Australia.

Además de estas casas, disponemos de cientos de opciones de 'otros alojamientos', incluidas casas de vacaciones para miembros y descuentos en hoteles, y el número de opciones aumenta cada año.

## Centro de Formación IBZ Castillo



El castillo IBZ de Gimborn, situado en un idílico entorno boscoso y montañoso en Alemania, alberga el Centro de Educación e Información de IPA y es considerado el buque insignia de la asociación.

Fundado en 1969, es donde se celebran seminarios, conferencias y reuniones profesionales de la IPA.

### La Beca Arthur Troop

Como legado del fundador del IPA, es una beca de educación profesional y capacitación avanzada, con el objetivo de ayudar a los miembros del IPA en sus carreras profesionales. Cada año, se invita a los miembros activos de la IPA a enviar sus solicitudes a su sección nacional para tener la oportunidad de recibir una beca de hasta 2500 € para un seminario o curso de su elección.

### Seminario para jóvenes policías

Cada dos años, la IPA organiza un Seminario para Jóvenes Policias, que ofrece a los nuevos reclutas la oportunidad de conocer a sus compañeros y participar en un programa de formación temático. En los últimos años, el YPOS ha llevado a participantes a Viena (2024), Sri Lanka (2022), el Reino Unido (2019), Estados Unidos (2017), Polonia (2015) y Australia (2013).

### Deportes

El deporte une a los miembros de la IPA sin necesidad de palabras. La membresía de la IPA brinda una multitud de oportunidades para participar en actividades deportivas en muchas secciones de la IPA.

### Juegos IPA

Inaugurados en 2018, los primeros Juegos IPA se celebraron en Lisboa, Portugal, con más de 350 miembros de la IPA de 23 secciones participando en competiciones de fútbol sala, tiro, voleibol y carrera. Los Juegos IPA no sólo se centran en los deportes, sino también en brindar la oportunidad de reunirse con amigos y recreación conjunta: un gran evento social lleno de diversión y entretenimiento.





## Torneo Mundial de Fútbol de la IPA

El Equipo del Proyecto Deportivo de la Comisión Sociocultural está organizando el 1er Torneo Mundial de Fútbol IPA en 2025.

## Grupos de interés

Uno de los muchos beneficios y oportunidades que ofrece la IPA son sus grupos de interés, presentes en todo el mundo, para el disfrute de nuestros miembros.

## Grupos de senderismo

Los grupos de senderismo han demostrado ser muy populares entre nuestras Secciones Nacionales y nuestros miembros. Actualmente, existen numerosos grupos de senderismo en todo el mundo que organizan eventos frecuentes para familias y personas de todos los niveles de condición física.



## IPAGAMES

No se trata solo de rivalidad deportiva; es, sobre todo, una oportunidad para intercambiar experiencias y forjar relaciones entre oficiales de diferentes países.

## Grupos de motociclistas

El motociclismo también es un pasatiempo muy popular en la IPA. Cada año se celebran numerosos eventos de motociclismo, que suelen consistir en largas carreras por paisajes idílicos, como los hermosos





## Clubes de coleccionistas

A muchos de nuestros miembros les encanta coleccionar e intercambiar objetos de recuerdo e insignias policiales, lo que ha dado lugar a numerosas ferias de intercambio y colecciónismo organizadas anualmente por varias de nuestras Secciones Nacionales. Estos eventos ofrecen una excelente oportunidad para intercambiar y ampliar su colección personal, además de forjar nuevas amistades con otros coleccionistas de la IPA.

## Clubes de tiro

Los clubes de tiro son otra actividad que disfrutan muchos miembros de nuestra asociación, y cada año se celebra una amplia gama de eventos y competiciones de diferentes disciplinas.

## Clubes de caravanas y camping

Los clubes de caravanas y camping de la IPA ofrecen a sus miembros la oportunidad de viajar y descubrir diferentes paisajes en compañía de personas afines que disfrutan de viajar y de la camaradería con sus compañeros.

## Club de Radio IPA (IPARC)

El Club de Radio IPA (IPARC) se fundó en marzo de 1976 y ha crecido hasta contar con unos 300 miembros de la IPA de diferentes sedes en Alemania. Alrededor de 2600 miembros de la IPA están conectados por su afición en todo el mundo. Se comunican y se reúnen en diversas bandas de radioaficionados en diferentes modos de oportunidad.

Otros ejemplos de grupos de interés que puedes encontrar son grupos de buceo, grupos de fotografía, grupos de esquí, y mucho más.

Esto, a grandes rasgos es la IPA, un lugar de encuentro para todos los policías del mundo, en el que cada uno puede desarrollar sus aficiones personales y compartir su experiencia profesional.

Autor:  
**José Miguel Prieto**, Policía Municipal de Madrid (España)



En situación de retirado por edad de jubilación. En 37 años de servicio ha acumulado experiencia en la investigación de delitos telemáticos, especialmente los cometidos contra menores y violencia de género. Además, es experto en la investigación de delitos cometidos contra la propiedad intelectual (comunicación pública de archivos musicales y videomusicales).

En la actualidad, es el Secretario General de la Sección Española de la International Police Association, (IPA España) desde febrero de 2022.

### CONTACTO:

+34 609 031 992  
secretariogeneral@ipaespana.org

**Recomendamos que visitéis nuestra página web internacional, <https://www.ipa-international.org/>, o contactéis con nuestra oficina internacional, iac@ieb-ipa.org, desde allí os dirigirán a la Sección Nacional de vuestro país de origen.**



# ASPROSEG

ASOCIACIÓN DE PROFESIONALES DE SEGURIDAD DE BOLIVIA



**La Asociación de Profesionales de Seguridad en Bolivia es una entidad privada, sin ánimo de lucro de carácter científico, académico y agremiación profesional, conformada por personas naturales y jurídicas con el propósito de socializar experiencias, debatir temas de actualidad y proyectar acciones en el contexto de la seguridad y la salud ocupacional del país.**



#### OBJETO

Asociar personas naturales y jurídicas en el contexto de la Seguridad en los ámbitos de los distintos sectores económicos del país.



#### MISIÓN

Liderar a nivel nacional las acciones académicas, investigativas y científicas en campos afines a la Seguridad.



#### VISIÓN

Ser reconocidos por nuestro liderazgo nacional con proyección internacional en el fomento de la seguridad integral con enfoque en sistemas de gestión.

**Contacto: 2780683**

Dirección: Zona Obrajes,  
Av. Hernando Siles, Calle 1, Edif. Torres Sur  
Sitio Web: [www.asprosegbolivia.com](http://www.asprosegbolivia.com)  
email: [info@asprosegbolivia.com](mailto:info@asprosegbolivia.com)

La Paz - Bolivia

# Reclutamiento y selección

## El primer filtro de la seguridad

**E**n el entorno actual de la seguridad corporativa, resulta cada vez más evidente que los sistemas tecnológicos, las políticas de control y las inversiones en infraestructura no alcanzan su pleno potencial si el recurso humano no está a la altura de los riesgos que enfrenta la organización. La seguridad empieza antes de que un guardia vista su uniforme o que un ejecutivo cruce la puerta de la empresa: comienza en el proceso de reclutamiento y selección.

Históricamente, muchas pérdidas en organizaciones provienen del propio personal.

Diversos estudios internacionales muestran que entre el 60 y el 70% de los incidentes internos —desde fraudes, fugas de información hasta actos de complicidad con delincuentes— tienen su origen en colaboradores que nunca debieron ser contratados o que ingresaron sin un filtro adecuado. Esta realidad resalta la necesidad de adoptar procedimientos de selección estructurados, objetivos y profesionales, que respondan a estándares globales y no a la improvisación.



# El proceso de reclutamiento y selección

No se limita a entrevistar candidatos o verificar experiencia laboral. Implica una investigación integral del perfil, donde convergen tres grandes componentes:

**1.**

## Screening documental

**y laboral:** Revisión de antecedentes judiciales, referencias laborales, historial académico y verificaciones de identidad.

**2.**

## Investigación de estilo de vida

**(lifestyle check):** Análisis de coherencia entre ingresos, entorno social y responsabilidades del cargo. Aquí se detectan vulnerabilidades como deudas excesivas, vínculos con grupos de riesgo o inconsistencias que podrían comprometer su desempeño.

**3.**

## Evaluaciones de integridad y confiabilidad:

Pruebas psicométricas, entrevistas estructuradas y, en ciertos casos, pruebas especializadas aplicadas bajo marcos legales.



“El que se equivoca al elegir a sus hombres, se condena a depender de ellos.” La advertencia de Maquiavelo, escrita hace siglos en su libro El Príncipe, mantiene hoy plena vigencia en el ámbito de la seguridad corporativa. Una mala selección no solo compromete la operación diaria, sino que abre la puerta a riesgos reputacionales y financieros. Basta un colaborador con acceso privilegiado que decida colaborar con un grupo delictivo para que meses de planificación y millones en inversión tecnológica se vean comprometidos en minutos.

Por el contrario, cuando el proceso se ejecuta correctamente, los beneficios son tangibles: reducción de incidentes, mayor lealtad del personal, disminución de rotación y fortalecimiento de la cultura organizacional. Además, permite que la inversión en capacitación tenga mayor retorno, ya que se forma a individuos que desde el inicio mostraron la actitud y los valores alineados a la institución.



**Otro error frecuente es considerar que, tras el ingreso, el control termina. Nada más lejos de la realidad. El ciclo de seguridad del talento humano exige seguimiento constante:** evaluaciones periódicas, programas de actualización y sistemas de alerta temprana. El personal cambia, sus contextos sociales evolucionan, y la organización debe estar preparada para identificar variaciones de riesgo que puedan poner en entredicho la integridad del servicio.

Es responsabilidad de la alta dirección respaldar estos procesos con recursos y políticas claras. De poco sirve que los encargados de seguridad o recursos humanos propongan lineamientos sólidos si no cuentan con el apoyo ejecutivo necesario para implementarlos. La prevención de pérdidas comienza con el compromiso de quienes toman decisiones estratégicas: invertir en selección no es un gasto, es un blindaje.

En conclusión, el reclutamiento y la selección profesional representan el punto de partida para construir una seguridad corporativa sólida. Una organización que apuesta por procesos rigurosos, integrales y basados en buenas prácticas internacionales, se coloca en ventaja frente a los riesgos internos y externos. El futuro de la seguridad depende tanto de la tecnología y los protocolos como de la calidad ética y profesional de las personas que los ejecutan.

Autor:  
**Mauricio  
Rolando Suárez  
Aguirre, CPP**



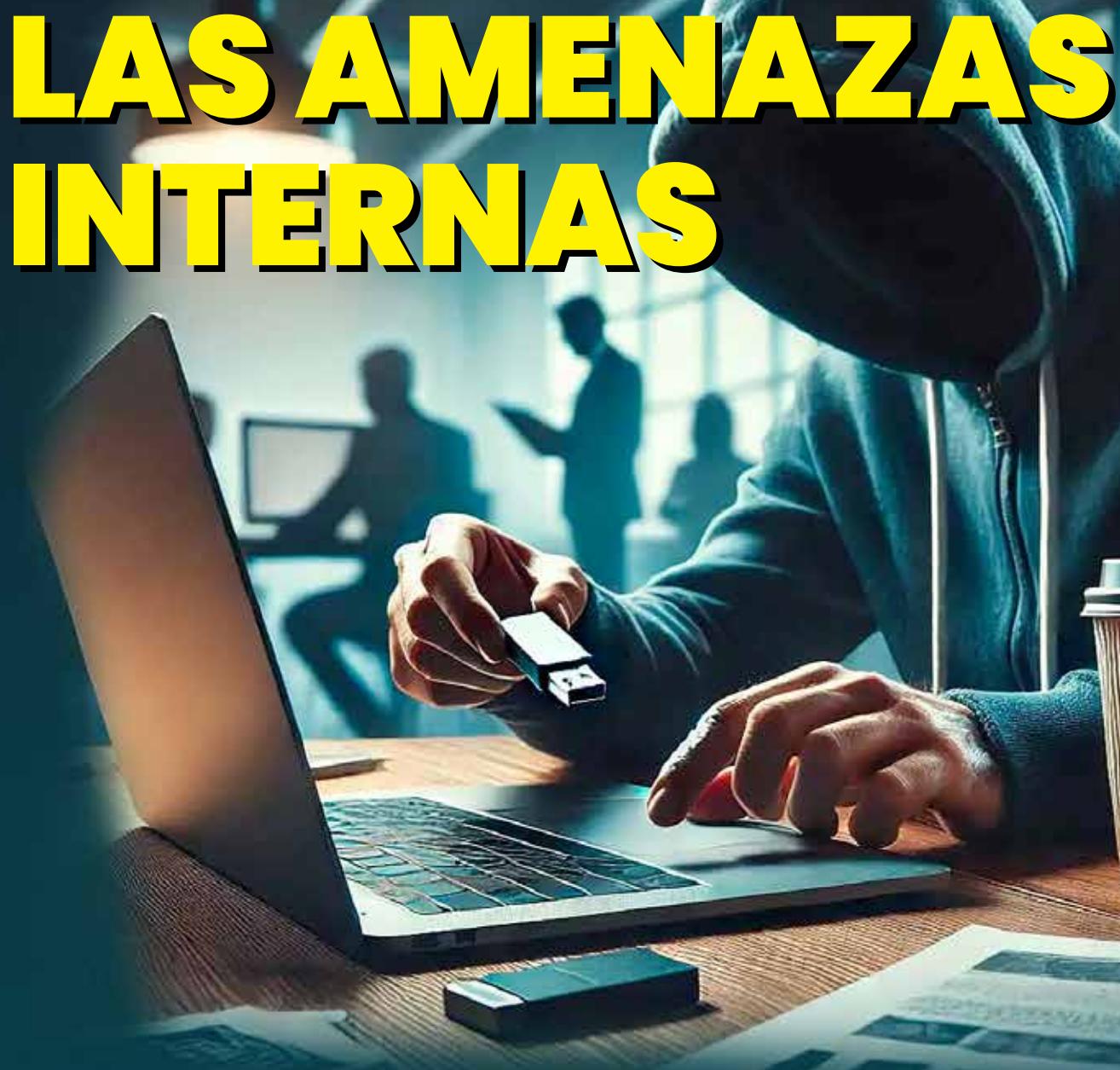
### **Director de Seguridad – Grupo Financiero Banrural**

Con más de 18 años de trayectoria en seguridad, gestión de riesgos y protección ejecutiva, Mauricio Suárez Aguirre ha liderado estrategias integrales en contextos de alta complejidad, dirigiendo equipos de más de 1,500 colaboradores a nivel nacional y regional. Actualmente es director de Seguridad del Grupo Financiero Banrural, presidente del Comité de Seguridad Bancaria de Honduras (AHIBA, 2022-2025) e integra el Comité Consultivo del Congreso Latinoamericano de Seguridad Bancaria (CELAES) de la Federación Latinoamericana de Bancos (FELABAN).

Es Certified Protection Professional (CPP) por ASIS International, la acreditación más prestigiosa a nivel global en gestión de seguridad, y posee una Maestría en Dirección Empresarial junto a un Programa de Habilidades Directivas (INCAE).

Cuenta con certificaciones internacionales en ISO 31000, ISO 18788, Active Shooter Response, terrorismo y crimen organizado, manejo de crisis y prevención de secuestro, además de la certificación internacional en seguridad bancaria. Su aporte profesional se centra en el fortalecimiento institucional, la estandarización de la seguridad privada y la creación de una cultura preventiva en el sector financiero, buscando ser un apoyo al sector público y privado, con una visión estratégica enfocada en resultados medibles (KPIs), reducción de incidencias y desarrollo integral de la seguridad en la región.

# LAS AMENAZAS INTERNAS



## El Enemigo Silencioso en la Seguridad Corporativa y su Contexto en LATAM

**E**n el panorama real de la ciberseguridad, ya las empresas reforzar sus perímetros con firewalls y sistemas de defensa avanzada contra amenazas externas, un riesgo igual de crítico y a menudo más insidioso prolifera dentro de dentro: la amenaza interna. Este reto representa uno de los mayores riesgos para la integridad, la confidencialidad y la continuidad del negocio, no solo por el potencial daño financiero y reputacional ya, sino que aquiete de donde se espera: personas con acceso legítimo.

# ¿Quién es un

# INSIDERS

## y por qué representa una amenaza?



Un “insider” o actor no es solo un empleado descontento. Es cualquier persona que tenga acceso a los sistemas, datos o instalaciones de la organización. Esta definición incluye a empleados actuales y anteriores, contratistas, socios comerciales y proveedores. La amenaza se clasifica en dos categorías principales:

**1 Maliciosos:** Individuos que actúan con intención deliberada de daño, ya sea por espionaje, robo de propiedad intelectual (para beneficiar a un competidor o iniciar su propia empresa), o sabotaje por descontento.

**2 Involuntarios o Negligentes:** Aquellos que, sin mala fe, provocan un incidente de seguridad. Esto incluye desde hacer clic en un enlace de phishing, perder un dispositivo, compartir credenciales por comodidad, hasta la incorrecta configuración de una base de datos en la nube, exponiendo información sensata. Este grupo es, estadísticamente, el más numeroso.

**El verdadero peligro reside en el abuso de la confianza. Estas personas ya están dentro del castillo; no necesitan saltar la muralla.**



# El Imperativo del Pensamiento Crítico y las Técnicas Analíticas

La detección efectiva de estas amenazas requiere un cambio de paradigma en las responsables de seguridad. Ya no es monitorear en solitario el exterior; es imperativo “empezar a-seudón dentro y después desde el exterior. Esto significa

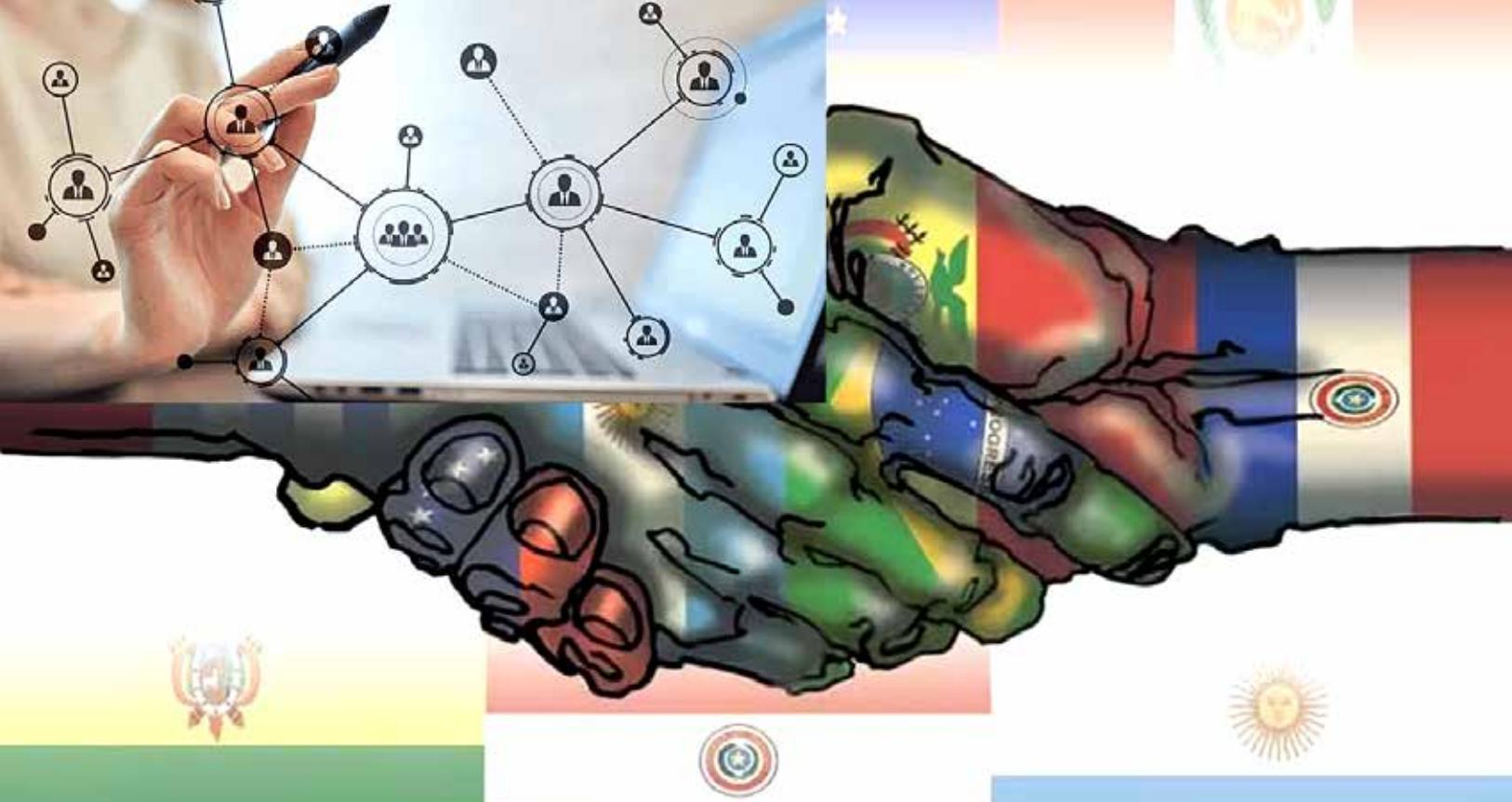
- **Pensamiento Crítico:** Cuestionar los segundos. “Realmente todos los usuarios necesitan acceso a todos los datos? Un empleado en el departamento de ventas necesita descargar toda la cartera de clientes? La mentalidad de “confianza cero” (Zero Trust) es fundamental: nunca confíes, verifica siempre.

**Técnicas Analíticas Estructuradas:** La Procuraduría se basa en la identificación Indicadores de Amenaza Interna (IATI) a través del análisis de datos conductuales y digitales. Algunos indicadores aplicables:

- **Comportamiento de Acceso:** Acceso a sistemas o datos fuera del horario laboral habitual, repetidos intentos de acceder a información no autorizada para su rol, o descargas masivas de datos.
- **Comportamiento Digital:** Uso frecuente de dispositivos de almacenamiento USB externos, cifrado de archivos que no era habitual, o un aumento significativo en el volumen de datos que se ha enviado fuera de la red corporativa.
- **Comportamiento Personal y Laboral:** Manifestaciones de insatisfacción laboral, conflictos con colegas o superiores, interés excesivo en áreas fuera de su responsabilidad, o aviones de renuncia.



La correlación de estos indicadores soluciones a través de Detección de Amenazas Internas (ITDR) Y Plataformas de Usuario y Entidad Comportamiento Analytics (UEBA) Permite establecer una línea base de comportamiento normal para cada usuario y alertar sobre las desviaciones que pueden señalar un riesgo potencial, permiten una investigación temprana de que ocurra un alcalde.



# Lecciones Globales y la Evolución en LATAM

**Países como Chile, Brasil y Colombia están liderando la modernización de sus marcos de seguridad cibernacional**

Iniciar la madurez de otros sectores es vital. El Departamento de Defensa de EE. UU. (DoD), trascaso como WikiLeaks, implementó su programa Amenaza interior El mandato de la Dirección 5205.16. Su estrategia se basa en la integración total: fusionando capacidades de ciberseguridad, monitorización de personal, controles de acceso físico y, crucialmente, análisis de comportamiento para identificar riesgos. Su enfoque holístico, donde la tecnología sustenta procesos claros y una cultura de reporte, es un modelo de referencia.

Inspirándose en estos estándares, LATAM ha estado transformando sus políticas. Países como Chile, Brasil y Colombia están liderando la modernización de sus marcos de seguridad cibernacional, a menudo vinculada a leyes críticas de protección de infraestructuras. Las empresas locales, especialmente en banca, energía y telecomunicaciones, se adoptan, se están adoptando programas de concienciación, implementando principios de menor privilegio y soluciones de la UEBA, se canalizan tanto por la regulación local de protección de datos como necesidad por la necesidad de proteger su propiedad intelectual en un mercado global competitivo.

# Sea Parte de la Solución Hoy



La seguridad corporativa moderna exige una visión holística que reconozca el riesgo puede venir tanto dentro de como fuera. Los líderes de seguridad deben abogar por estrategias que combinan tecnología avanzada de análisis de comportamiento, políticas y claras una cultura organizacional consciente.

La detección de amenazas internas ya no es un lujo, es una necesidad estratégica para la resiliencia del negocio en la era digital. La pregunta no es si su organización puede aplicar permitírsela, sino si puede permitirse el lujo de no hacer.

## RESUMEN PROFESIONAL

**Licenciado  
en Seguridad  
Pública y  
Criminología.  
Jonathan  
Hermida Sosa.**



Experto en Seguridad Corporativa Integral y Gestión de Riesgos con más de 15 años de experiencia. Certificado internacionalmente por el Centro de Excelencia del Departamento de Defensa (CDSE) como SAPPC, SFPC, CPO, DAS, ha liderado estrategias que se reducen hasta el 60% de la siniestralidad laboral y 45% las pérdidas patrimoniales. Especialista en aplicación de aplicación tecnológica (STPS, ISO, CTPAT, BASC) e implementación de sistemas tecnológicos. Reconocido entre los Top 3 en Seguridad Corporativa Integral en México.

- **SAPPC:** Certificación profesional de protección de activos de seguridad
  - Significado: Certificación Profesional en Protección de Activos de Seguridad.
  - Otorgada por: Departamento de Defensa de los Estados Unidos.
  - Enfoque: Evalúa y certifica los conocimientos en la protección de los físicos activos y de información crítica de una organización.
- **SFPC:** Certificación profesional de Fundamentos de Seguridad
  - Significado: Certificación Profesional en Fundamentos de la Seguridad.
  - Otorgada por: Departamento de Defensa de los Estados Unidos (CDSE).
  - Enfoque: Acredita el dominio de los conceptos básicos y principios fundamentales de los programas de seguridad industrial y de seguridad de la información.
- **CPO:** Oficial de Protección Certificado
  - Significado: Oficial de Protección Certificado.
  - Otorgada por: Fundación Internacional para Oficiales de Protección (IFPO).
  - Enfoque: Certifica las competencias para el desempeño en los roles de supervisión y gestión operativa en seguridad privada y corporativa.
- **DAS:** Diploma en Administración de la Seguridad
  - Significado: Diplomado en Administración de la Seguridad.
  - Otorgada por: Universidad Pontificia Comillas (ICADE), una institución académica de prestigio en España.
  - Enfoque: Un programa de posgrado que se centra en la gestión estratégica, la dirección y la administración de departamentos y proyectos de seguridad.

# SEGURIDAD EN ACCION

Grupo Corp. Rojo va un paso más allá en su estrategia de crear cultura de seguridad con el nacimiento de una nueva revista especializada en la seguridad en Bolivia



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!



## ¡PRÓXIMAMENTE AL AIRE!

Llega **SEGURIDAD EN ACCIÓN**, el programa radial donde expertos analizarán los problemas de seguridad que enfrentamos y brindarán recomendaciones clave para protegernos.



Estaremos en las mejores estaciones de radio del país  
Mantente atento, pronto más detalles.



[www.seguridadenaccionlatam.com](http://www.seguridadenaccionlatam.com)

REVISTA DE REFERENCIA DEL SECTOR DE LA SEGURIDAD  
PRIVADA, CIBERSEGURIDAD, PROTECCIÓN DE DATOS.





# **SEGURIDAD Y SALUD**

## **EL FUTURO DEL TRABAJO**

**H**oy trabajamos en todas partes, en cualquier momento nos enfrentamos a nuevas condiciones laborales y a nuevas formas de trabajo, pero ningún empleo debería arrebatarle, su seguridad, su salud, su bienestar o su vida; lamentablemente cada día 7,500 personas mueren en el mundo, debido a medios ambientes de trabajo inseguros e insalubres, de estas 7,500 muertes la mayoría son por causa de enfermedades relacionadas con el trabajo, las muertes relacionadas con el trabajo no son más que una parte del trágico panorama que se presenta ante nosotros.

Cada día más de un millón de personas se lesionan en el trabajo y ello tiene un fuerte impacto en los trabajadores y sus familias económicamente, físicamente y emocionalmente, pero también para las empresas y en la productividad; el aumento de los accidentes laborales, las enfermedades ocupacionales y el impacto tremendo de grandes catástrofes ocurridos en lugares de trabajo como Seveso (Italia 1976), Bhopal (India 1984), Chernóbil (Ucrania 1986), Rescate de la Mina San José (Chile 2010), Colapso de Rana Plaza (Bangladés 2013) y la Ruptura de la presa Valle (Brasil 2019); provocaron el llamamiento a una Cultura de Prevención de Riesgos a nivel mundial.

Por: Lic. Juan Díez Aragón  
Gerente Operaciones Latam  
ARGOS DAJE SAC

---

Durante 100 años la Organización Internacional del Trabajo (OIT) ha trabajado con los gobiernos, los empleadores y los trabajadores para ayudar a hacer del entorno de trabajo un lugar más seguro y saludable para las personas de todo el mundo; desde 1919 la Organización Internacional del Trabajo (OIT) ha adoptado más de 40 convenios sobre Seguridad y Salud en el Trabajo.

---

**Cada día más de un millón de personas se lesionan en el trabajo y ello tiene un fuerte impacto en los trabajadores y sus familias económicamente, físicamente y emocionalmente**



Durante 100 años la Organización Internacional del Trabajo (OIT) ha trabajado con los gobiernos, los empleadores y los trabajadores para ayudar a hacer del entorno de trabajo un lugar más seguro y saludable para las personas de todo el mundo; desde 1919 la Organización Internacional del Trabajo (OIT) ha adoptado más de 40 convenios sobre Seguridad y Salud en el Trabajo.

Es urgente que sumemos esfuerzos a nivel global ratificando los convenios fundamentales que proporcionan normas mínimas, dirigidas a proteger a los trabajadores de riesgos múltiples.

La Organización Internacional del Trabajo (OIT) también elabora repertorios de recomendaciones prácticas, directrices, publicaciones y material de información para mejorar los conocimientos; es importante centrar la atención nacional en la nece-

**Es urgente que sumemos esfuerzos a nivel global ratificando los convenios fundamentales que proporcionan normas mínimas, dirigidas a proteger a los trabajadores de riesgos múltiples.**



sidad de evitar muertes, lesiones y enfermedades por causa del trabajo, hoy nos enfrentamos a tendencias en el trabajo que comportan desafíos y oportunidades para la protección de nuestra salud y bienestar; la tecnología, la demografía en evolución constante, el desarrollo sostenible, los cambios en la organización del trabajo; algunas de estas tendencias traen consigo adelantos para la Seguridad y Salud, pero otras crean riesgos para los trabajadores.

**¿Qué puedo hacer?** Anticipar los principales riesgos emergentes para la Seguridad y Salud, incluir más disciplinas en la gestión de la Seguridad y Salud en el Trabajo, adquirir nuevas competencias, dirijamos nuestras mirada más allá del lugar de trabajo y abarquemos estrategias de prevención sobre salud pública más amplias; ratifiquen y apliquen las normas internacionales

del trabajo de la Organización Internacional del Trabajo (OIT) sobre Seguridad y Salud en el Trabajo, son pilares eternos en tiempos de grandes cambios, más que nunca debemos apoyar a los gobiernos, a los empleadores y a los trabajadores mientras el mundo del trabajo cambia, pero también debemos ampliar nuestras alianzas, juntos debemos aprovechar estas oportunidades para actuar a fin de crear un Presente y un Futuro Seguros y Saludables para todos.

Además de lograr siempre consensos entre los Gobiernos, empleadores y los trabajadores, antes de emitir leyes o normas, solo así; colaborando estos tres grupos, se podrán lograr grandes cambios para nuestras futuras generaciones.

¡¡ SEGURIDAD Y SALUD PARA LA VIDA !!



### **LIC. JUAN DÍEZ ARAGÓN**

Gerente Operaciones Latam  
ARGOS DAJE SAC

- Consejero Regional de Seguridad y Salud en el Trabajo Región Lambayeque.
- Presidente de la Asociación Internacional de Seguridad y Salud en el Trabajo AISST.
- Delegado Internacional de la Asociación de Jefes de Seguridad de España en Perú ISCA.
- Evaluador de Competencias Laborales en Prevención de Riesgos y Seguridad y Salud en el Trabajo.
- Vice Presidente del Gremio de Talento Humano de la Cámara de Comercio y Producción de Lambayeque.
- 1er Facilitador Internacional en Herramientas Didácticas y Sistémicas para el Desarrollo Humano y Empresarial en Perú en materia de Seguridad y Salud en el Trabajo.
- Gerente de Operaciones en la empresa Argos Daje SAC.

# **NEUROSEGURIDAD**

**Un nuevo concepto, entre Seguridad convencional, CPTED y la Neuroarquitectura**



**L**a seguridad ha dejado de ser entendida únicamente como un conjunto de medidas físicas o tecnológicas destinadas a prevenir el delito. Hoy, en el marco de los avances de la neurociencia y la aplicación de disciplinas emergentes como la neuroarquitectura, surge un nuevo concepto que redefine el modo en que las personas experimentan la protección de su entorno: la neuroseguridad.

Este enfoque integra la prevención del delito a través del diseño ambiental, tal como propone la metodología CPTED (Crime Prevention Through Environmental Design), con los conocimientos que aportan la neurociencia sobre el comportamiento humano y la influencia que los espacios ejercen en la mente y las emociones.

La neuroarquitectura ya ha demostrado cómo factores como la luz natural, los colores, las texturas, la organización espacial y la presencia de elementos naturales son capaces de generar bienestar, reducir el estrés y mejorar la productividad. Estos mismos elementos, aplicados desde la perspectiva de la seguridad, adquieren un valor esencial: contribuyen a disminuir la percepción de riesgo, a reforzar la sensación de control y a favorecer entornos donde los usuarios se sienten tranquilos, confiados y partícipes de su espacio.

---

**El diseño de un entorno seguro ya no puede concebirse como la suma de cámaras, cerramientos o sistemas electrónicos, sino como una integración de la dimensión objetiva de la seguridad con la dimensión subjetiva que percibe la persona.**

---

La neuroseguridad, por tanto, no se limita a proteger, sino que busca crear una experiencia emocional en la que la seguridad se perciba de manera natural, sin que el usuario se sienta vigilado de forma opresiva ni condicionado por elementos invasivos. El diseño de un entorno seguro ya no puede concebirse como la suma de cámaras, cerramientos o sistemas electrónicos, sino como una integración de la dimensión objetiva de la seguridad con la dimensión subjetiva que percibe la persona. Esto se traduce en informes de seguridad que, además de valorar las condiciones técnicas de un espacio, analizan el impacto emocional y psicológico que produce sobre sus ocupantes. La inclusión de esta perspectiva en los infor-



**la neuroseguridad se convierte en un puente entre la prevención del delito mediante el diseño ambiental de CPTED, la neuroarquitectura como disciplina centrada en el bienestar emocional, y la práctica profesional del consultor en seguridad, que traduce este conocimiento en estrategias concretas, aplicables y medibles.**



mes profesionales no solo enriquece el diagnóstico de riesgos, sino que aporta un valor añadido: permite diseñar entornos donde la seguridad se experimenta como parte de la vida cotidiana y no como una imposición.

El modelo de informe de seguridad que incorpora los principios de la neuroseguridad abre la puerta a una visión más amplia y adaptada a las demandas actuales de nuestra sociedad. Un informe que ya no se limita a evaluar vulnerabilidades físicas, sino que examina también cómo la arquitectura, la organización espacial y la atmósfera del entorno influyen en la percepción de las personas. En este sentido, la neuroseguridad se convierte en un puente entre la prevención del delito mediante el diseño ambiental de CPTED, la neuroarquitectura como disciplina centrada en el bienestar emocional, y la práctica profesional del consultor en seguridad, que traduce este conocimiento en estrategias concretas, aplicables y medibles.

**La seguridad del futuro se encuentra precisamente en esta convergencia: proteger desde la objetividad de los sistemas y estructuras, pero también desde la subjetividad de la mente humana. La neuroseguridad propone que cada informe, cada análisis y cada proyecto arquitectónico asuma que la verdadera eficacia no reside solo en la ausencia de incidentes, sino en la capacidad de un espacio para transmitir confianza, serenidad y pertenencia a quienes lo habitan.**



## FRAN MEDINA CRUZ

CONSULTOR. TÉCNICO URBANISTA Y CPTED.  
AUDITOR, PERITO JUDICIAL Y FORMADOR.

### Sobre mí

Apasionado de la Seguridad y la gestión de proyectos. Me defino por ser una persona con ganas de demostrar y un gran líder de equipos multidisciplinares. He desarrollado proyectos de seguridad propios como "LA MEDIDA DEL RIESGO" y "EL AMBIENTE URBANISTICO".

### EXPERIENCIA LABORAL

#### 1.-ESPECIALISTA TECNICO EN CPTED Y URBANISMO

Desde 2021: Asesoramiento de zonas residenciales y áreas comerciales.

Año 2023. Realización de informes CPTED con los requisitos de seguridad establecidos en la categoría de Seguridad y Bienes-  
tar (SyB 11) de Certificadora BREEAM.

Publicación del libro "Mi Hogar es mi Castillo" sobre la implementación cpted en residencias aisladas. ISBN 978-84-18840-53-1

#### 2. - SEGURIDAD (ver datos académicos)

- Vigilante de Seguridad; desde Jul. 2018 a Actualidad en: COFER.
- Seguridad - Director de la Asoc. Metrorisk. desde febrero 2021 a actualidad.
- Consultor en MR-CONSULTING desde septiembre a actualidad.

- Formador de Seguridad en área Técnico Profesional. Desde junio a actualidad

Con dos publicaciones realizadas: "La Medida del Riesgo" "El Ambiente Smart City."

### Datos académicos

- Titulo académico bachiller. Mérida (Badajoz). Diplomas y cursos realizados entre 1988/2016; Informática, Seguros ge-  
nerales y de salud, dominio de procesadores de texto, etc.  
Mérida (Badajoz)
- Vigilante de Seguridad TIP - Córdoba. 2018
- Director de Seguridad y Experto en Seguridad Integral. - Univ. Nebria - Madrid. 2019/20
- Perito Judicial en Seguridad Privada. -INISEG. Málaga. 2020
- Diploma de especialización en Auditor de Seguridad. INISEG
- Gestión de la Seguridad Portuaria.-INISEG. 2020
- Seguridad CPTED. ISO 22341.-CPTED México ICA Chapter 2021
- Auditor de Seguridad Privada. -INISEG 2022
- Experto en Urbanismo v Arquitectura Sostenible. INSTITU-  
TO EUROPEO DE ESTUDIOS EMPRESARIALES 2023
- Técnico Profesional en Urbanismo. UROINNOVA. BUSINESS  
SCHOOL 2023

# Aprendizaje SIN LÍMITE

Con Aprendo Ya encuentras la forma más fácil de vender profesionalizar tus cursos en Bolivia.

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



**APRENDOYA**  
APRENDIZAJE SIN LÍMITES Y FRONTERAS

El momento de actuar es

**AHORA**

Haz que tu conocimiento brille y tus ventas despeguen.

Dirección: Zona Obrajes, Av. Hernando Siles,  
Calle 1, Edificio Torres Sur, Of. TS17  
Correo: info@aprendoya.com  
Página web: www.aprendoya.com



## LLEVA TU MARCA AL SIGUIENTE NIVEL EN EL SECTOR MAS INFLUYENTE DEL MERCADO

Seguridad en Acción no es solo una revista digital, es una plataforma estratégica donde marcas, expertos y profesionales pueden posicionarse, influir y conectar con una audiencia clave en el mundo de la seguridad. Brindamos información de calidad, análisis especializado y oportunidades de networking para potenciar el impacto de tu empresa.



# CPTED

## (PREVENCIÓN DE LA DELINCUENCIA MEDIANTE EL DISEÑO AMBIENTAL) PARA CIUDADES RESILIENTES Y SEGURAS



**Dr. Macarena Rau Vargas**  
Presidente  
International CPTED Association  
Corporación Rojo SRL  
Agosto 2025

### 1. Introducción

La metodología CPTED (Crime Prevention Through Environmental Design) ha evolucionado a lo largo del tiempo desde su creación en USA hace más de 50 años, desarrollándose en tres generaciones (CPTED de primera, segunda y tercera generación), cada una con enfoques más integrales y participativos en la prevención del delito y el diseño urbano.

En el mundo, CPTED es difundida por la International CPTED Association, que está en más de 50 países ([www.cpted.net](http://www.cpted.net)), y que desde el año 2017, cuando su Presidenta Dra. Macarena Rau impulsó la Iniciativa de los Paraguas, ya cuenta con 10 capítulos oficiales en diversas regiones del mundo.

La Dra. Rau es presidenta actualmente de la International CPTED Association con sede en Canadá.

**Las normas ISO 22341 y 22344 se centran en la “Prevención del Delito a Través del Diseño Ambiental” (CPTED, por sus siglas en inglés), y ambas tienen una relación intrínseca con la gestión de riesgos que promueve la ISO 31000.**



## 2. Generaciones CPTED

La metodología CPTED es una metodología viva que desde su fundación en 1972 hasta la fecha ha evolucionado de una primer, segunda hasta tercera generación.

A continuación se detalla cada una de las generaciones.

### 2.1.CPTED de Primera Generación

Surgió en los años 70 y se enfocó en la reducción de oportunidades delictivas mediante el diseño físico del entorno. Sus principios clave incluyen:

- Control natural de acceso: Uso de barreras físicas y simbólicas para limitar el acceso.
- Vigilancia natural: Diseño que permite la visibilidad y supervisión de espacios.
- Reforzamiento de territorialidad: Creación de un sentido de propiedad y pertenencia en los residentes](<https://riskp.com/caracteristicas-del-cpted/>).

### 2.CPTED de Segunda Generación

A partir de los años 2000, se amplió el enfoque para incluir aspectos sociales y comunitarios en la prevención del delito. Se incorporaron elementos como:

- Cohesión social: Fomento de la participación comunitaria en el diseño urbano.
- Sentido de pertenencia: Creación de espacios que refuerzen la identidad local.
- Resiliencia comunitaria: Estrategias para fortalecer la capacidad de respuesta ante problemas de seguridad (<https://riskp.com/caracteristicas-del-cpted/>).

### 3.CPTED de Tercera Generación

Desde 2019, esta generación busca integrar la sostenibilidad y el bienestar en la prevención del delito. Se basa en:

- Diseño ecológico: Incorporación de elementos naturales para mejorar la seguridad.
- Participación infantil: Métodos como la Nube de los Sueños CPTED, que recogen la percepción de los niños sobre su entorno.
- Enfoque holístico: Consideración de factores ambientales, sociales y psicológicos en el diseño urbano.
- Cada generación ha ampliado la visión de CPTED, pasando de un enfoque físico a uno más social y sostenible.

### **3.1. Estándares ISO para la Prevención del Delito Mediante el Diseño Ambiental**

Las normas ISO 22341 y 22344 se centran en la "Prevención del Delito a Través del Diseño Ambiental" (CPTED, por sus siglas en inglés), y ambas tienen una relación intrínseca con la gestión de riesgos que promueve la ISO 31000.

ISO 22341:2021 - Directrices para la prevención del delito a través del diseño ambiental

- Descripción: La ISO 22341:2021, titulada "Seguridad y resiliencia - Seguridad protectora - Directrices para la prevención del delito a través del diseño ambiental", proporciona un marco para establecer los elementos, estrategias y procesos fundamentales para prevenir y reducir el delito y el miedo al delito en entornos construidos, tanto nuevos como existentes. Su objetivo principal es mejorar la seguridad de entornos urbanísticos y edificios al integrar consideraciones de seguridad desde la fase de diseño.
- Enfoque: Se basa en el principio de que el diseño y la gestión del entorno físico pueden influir en el comportamiento humano y, por lo tanto, disuadir el delito y mejorar la sensación de seguridad. Recomienda el establecimiento de contramedidas y acciones para tratar los riesgos de delito y seguridad de manera efectiva y eficiente, aprovechando el diseño ambiental. El término "seguridad" en esta norma es

amplio e incluye aplicaciones específicas de delito, seguridad y protección.

- Aplicabilidad: Es aplicable a organizaciones públicas y privadas, independientemente de su tipo, tamaño o naturaleza.

### **ISO 22344 (en desarrollo) - CPTED para instalaciones residenciales**

- Descripción: La ISO/DIS 22344 (actualmente en etapa de borrador o desarrollo) es parte de la serie de normas de seguridad y resiliencia. Específicamente, se enfoca en las "Directrices para la prevención del delito a través del diseño ambiental para instalaciones residenciales". Aunque su título puede sugerir un enfoque exclusivo en residencias, se ha señalado que es aplicable a cualquier instalación física.
- Objetivo: Esta norma busca proporcionar orientación detallada para la aplicación de los principios CPTED en entornos residenciales, abarcando tanto espacios privados como públicos dentro de las comunidades habitacionales. Su desarrollo apunta a complementar la ISO 22341, ofreciendo directrices más específicas para un tipo de entorno particular.



## Relación con ISO 31000:2018 - Gestión del Riesgo - Directrices

- ISO 31000:2018 es una norma internacional que proporciona principios, un marco y un proceso para gestionar el riesgo de manera efectiva en cualquier tipo de organización, independientemente de su tamaño o sector. No es una norma certificable, sino que ofrece directrices para integrar la gestión de riesgos en la toma de decisiones y las operaciones de una organización.

- Conexión entre las normas:

- Identificación y Evaluación de Riesgos: Las normas ISO 22341 y 22344 son herramientas clave para la identificación y evaluación de riesgos específicos relacionados con el delito y la seguridad física, que son componentes fundamentales del proceso de gestión de riesgos de la ISO 31000. Al aplicar los principios CPTED, las organizaciones pueden identificar vulnerabilidades en el diseño ambiental que podrían ser explotadas por delincuentes.
- Tratamiento de Riesgos: El CPTED (ISO 22341 y 22344) ofrece estrategias de tratamiento de riesgos al proponer soluciones de diseño que mitigan o reducen la probabilidad y el impacto de los eventos delictivos. En lugar de simplemente reaccionar ante el delito, estas normas permiten un enfoque proactivo de control de riesgos a través del diseño. Esto se alinea directamente con el proceso de "tratamiento del riesgo" de la ISO 31000, que implica seleccionar e implementar opciones para modificar el riesgo.
- Contexto y Criterios: La ISO 31000 enfatiza la importancia de comprender el contexto interno y externo de la organización y establecer criterios de riesgo. Las normas CPTED ayudan a definir este contexto en términos de seguridad física y a establecer criterios específicos para evaluar la efectividad de las medidas de diseño en la prevención del delito.
- Mejora Continua: Al igual que la ISO 31000 promueve la mejora continua del proceso de gestión de riesgos, la implementación de CPTED es un proceso iterativo que implica monitorear la efectividad de las medidas de diseño y ajustarlas según sea necesario para optimizar la seguridad y la resiliencia.

En resumen, las normas ISO 22341 y 22344 actúan como guías especializadas para abordar los riesgos de segu-



ridad física y delictiva a través del diseño ambiental. Se integran perfectamente dentro del marco general de gestión de riesgos de la ISO 31000, proporcionando un enfoque práctico y proactivo para identificar, evaluar y tratar los riesgos de seguridad en el entorno construido, contribuyendo así a la resiliencia y la protección general de una organización o comunidad.

## 4. CPTED y Resiliencia Urbana

La relación entre la Prevención del Delito a Través del Diseño Ambiental (CPTED, por sus siglas en inglés) y la resiliencia urbana es sinérgica y bidireccional. Ambas buscan crear entornos urbanos más seguros y habitables, pero desde perspectivas ligeramente distintas. CPTED se enfoca en la prevención del delito, mientras que la resiliencia urbana busca la capacidad de una ciudad para resistir, absorber, adaptarse y recuperarse de cualquier tipo de amenaza.

CPTED se integra como un componente esencial para construir ciudades más resilientes. Su aplicación directa en el diseño de espacios urbanos contribuye a la resiliencia al:

- Reducir la vulnerabilidad: Al disminuir la oportunidad para el crimen y el miedo a la inseguridad, CPTED hace que las comunidades sean menos vulnerables a las crisis relacionadas con la violencia.
- Fomentar la cohesión social: A través de la vigilancia natural y el reforzamiento territorial, CPTED promueve el sentido de pertenencia y la interacción social. Una comunidad cohesionada es más capaz de responder a desafíos, ya sean desastres naturales o problemas sociales, lo que es clave para la resiliencia.
- Mejorar la calidad de vida: Un entorno seguro y bien mantenido mejora el bienestar general de los residentes, lo que les permite enfocarse en otros aspectos de la vida comunitaria y económica, fortaleciendo así el tejido social de la ciudad.

CPTED contribuye a la resiliencia urbana al construir entornos que no solo previenen el crimen, sino que también empoderan a las personas y a las comunidades para que se apropien de sus espacios y los defiendan.

## 5. Conclusiones

La metodología CPTED es una metodología científica y robusta que cuenta con ya más de 50 años de evolución. Sus tres generaciones ofrecen una amplia gama de instrumentos y herramientas para abordar diversos escenarios delictivos de diversos niveles de complejidad. Ya desde el año 2021 cuenta con el respaldo de normas ISO 22341 y 22341-2 además de la norma 31000.

Lo que demuestra el Sistema de Evaluación de Riesgos e Impactos de Proyectos CPTED//Situacionales (ESU) es la relevancia de crear una masa crítica de profesionales certificados que aplique de acuerdo a los estándares internacionales la metodología CPTED de última generación lo que permitirá obtener mayor rendimiento en reducción delictiva y de percepción de temor urbano.

Desde el año 2008 ha funcionado en LATAM el siguiente campus CPTED en Español acreditado por ICA en formato sincrónico ([www.pbk.cl/campus](http://www.pbk.cl/campus)) y asincrónico <https://go.hotmart.com/M99393240J?dp=1>

CPTED como metodología funciona bien cuando se aplica correctamente y esa es una de las principales misiones de la International CPTED Association (ICA), velar por la promoción, difusión y aplicación de CPTED de la forma correcta a nivel mundial para el logro de la reducción delictiva, de violencia y de inseguridad urbana.



### DRA. MACARENA RAU VARGAS

#### CURRICULUM PROFESIONAL

Arquitecta, Magíster y Doctora en Urbanismo con amplia experiencia liderando Proyectos e Iniciativas de Seguridad Urbana, tanto públicas como privadas, en Chile y en varios países de América Latina y el Caribe.

Especialista en la metodología CPTED (Crime Prevention Through Environmental Design) con probado éxito en el diagnóstico, diseño, implementación y evaluación de proyectos de Prevención de la Violencia y el Delito desde una perspectiva Ambiental con experiencia en la aplicación y enseñanza de CPTED en diversos países del mundo.

Actualmente es Presidenta de la Asociación Internacional CPTED ([www.cpted.net](http://www.cpted.net)).

#### Cargos

- Presidenta de la Asociación Internacional CPTED (ICA; [www.cpted.net](http://www.cpted.net)).
- Presidenta y fundadora de la Corporación para la Prevención del Delito a través del Diseño Ambiental en Chile ([www.cpted-region.org](http://www.cpted-region.org)).
- Director Ejecutivo y fundador de Publika Consulting Company ([www.pbk.cl](http://www.pbk.cl)).
- Miembro del Comité Científico de Urban Life 2005, Suecia ([www.urbanlife2005.com](http://www.urbanlife2005.com)).
- Revisor del Journal of Applied Security Research 2020 (Routledge).



# NEUROSEGURIDAD Y SU IMPACTO EN LA PREVENCION DE ACCIDENTES DE TRABAJO

## INTRODUCCION

Después de leer los múltiples modelos que existen en el mundo para llegar a la causa básica del accidente de trabajo, puedo concluir que todos ellos buscan encontrar el error desde el mismo paradigma existente, pero ignoran que el funcionamiento del cerebro es donde radica la percepción del riesgo, el sentir y el pensar que originan el comportamiento humano con un desempeño positivo o negativo en tareas críticas o no críticas en forma diaria.

Siendo las neurociencias el sustento científico y su aplicación en el área de Seguridad y salud en el trabajo, esta anterior es la disciplina que evaluamos para el conocimiento del cerebro de los trabajadores, es relevante mencionar como cada día las investigaciones mundiales conocen mucho mejor el cerebro/mente para aplicarlo a la neuro prevención de accidentes y enfermedades laborales.

Definimos **NEUROSEGURIDAD** como el estudio del cerebro/mente para conocer la forma como percibimos el riesgo, pensamos, sentimos y tomamos decisiones en tareas críticas y no críticas en el trabajo.

### **Surge entonces una incógnita.**

¿porque a pesar de observar el comportamiento de los trabajadores, si se establecen los comportamientos de trabajo seguro, y se intervienen los riesgos en el medio laboral, y se capacita al trabajador y al equipo de trabajo, porque se siguen accidentando los trabajadores?

Desde las neurociencias aplicadas a la seguridad y salud en el trabajo, surge nuestra investigación, producto de nuestras intervenciones en campo en más de veinticinco mil empresas, un millón de horas hombre asesoradas e intervenidas y más de ciento cuarenta

mil evaluaciones medicas ocupacionales a empresas de distintas actividades económicas en Colombia y Latinoamérica, con el objetivo de contribuir a impactar la accidentalidad , desde un nivel más profundo, más allá de lo visible del comportamiento humano, que sería la punta de iceberg, observación que por décadas junto a todas esas teorías, nos han permitir explorar más profundamente buscando las verdaderas causas de estos accidentes, encontrando en consecuencia que algunas alteraciones biológicas y aprendizajes desde los estados conscientes del trabajador, se convierten en los precursores de los errores humanos que terminan en accidente con grandes pérdidas no solo materiales sino la vida misma.

**La mente: es la entidad que procesa toda la información que pasa por el cerebro. Tiene pensamientos, sentimientos y experiencia subjetiva. La mente es responsable de la conciencia, la percepción, la atención, la memoria, el aprendizaje y la toma de decisiones**

Para conocer mejor el cerebro existe una teoría didáctica que habla del cerebro triuno y nos explica en forma muy sencilla el autor MC. Lean que el cerebro está conformado por 3 cerebros, el cerebro reptiliano (instintivo), cerebro emocional y cerebro cortical

**1. El cerebro reptiliano:** se comporta como un cocodrilo, el cual realiza funciones instintivas o de supervivencia como: comer, dormir, atacar ante una amenaza y procrear buscando la perpetuidad de la especie

**2. El cerebro emocional:** está conformado por 3 estructuras básicas y son: amígdalas: es el centro donde se originan las emociones primarias y complejas. Las emociones primarias mas importantes son: miedo, ira, tristeza, alegría, sorpresa y asco. Todo el cerebro emocional juega un papel importante en la génesis del error humano, ya que estados como el estrés, fatiga y distracciones emocionales pueden ser factores precursores del error

**3. Cerebro cortical:** este es el cerebro que nos diferencia de los animales, ya que es el componente que



piensa, analiza, razona, con el fin de tomar decisiones conscientes y lógicas en el entorno. Este cerebro es muy importante en el error ya que hay un área denominada corteza prefrontal (cerca de los ojos) encargada de las funciones cerebrales superiores como: atención, memoria, control inhibitorio, flexibilidad cognitiva, gestión de las emociones, etc.

Ya conociendo el cerebro triuno, podemos definir que es el cerebro y la mente

**Cerebro:** es el órgano físico que se encuentra dentro de nuestra cabeza y es el encargado de controlar las funciones corporales, incluyendo las funciones ejecutivas cerebrales. Esta compuesto por billones de neuronas que se comunican entre si a través de trillones de sinapsis.

**La mente:** es la entidad que procesa toda la información que pasa por el cerebro. Tiene pensamientos, sentimientos y experiencia subjetiva. La mente es responsable de la conciencia, la percepción, la atención, la memoria, el aprendizaje y la toma de decisiones.

Daniel Kahneman siendo psicólogo gana el premio nobel de economía en el año 2002 a través de sus investigaciones del pensamiento rápido (automático) y el pensamiento (consciente), lo anterior es para explicar que la mente se divide en dos partes: la mente Consciente (voluntario) y mente no consciente (involuntario o automático). El problema para la gestión del error es que durante nuestras actividades la mente no Consciente solo ejecuta el 95% de nuestras actividades, mientras que la mente Consciente solo ejecuta el 5% restante de esa actividad. En otras palabras, el ser humano vive en total automatismo durante el día

El hombre gracias al funcionamiento de su cerebro tiene la capacidad de generar las estrategias que se necesitan para interactuar con el medio, esas estrategias son las que le han permitido sobrevivir a través de los siglos más sin embargo son las que llevan a cometer el error humano

"No hay error que no sea humano y no hay ser humano que no cometa errores", ante esta afirmación podemos decir que el error siempre ha existido y existirá por siempre en la humanidad.

Todos somos propensos a cometer errores. Desde los pequeños deslices cotidianos hasta las decisiones que

cambian vidas, el error humano es una parte intrínseca de nuestra existencia

### **Pero porque fallamos ¿que nos lleva a equivocarnos?, incluso cuando tenemos la mejor intención y la mayor preparación?**

Para el desarrollo de este artículo y hablar de NEUROSEGURIDAD he tenido en cuenta los indicadores de accidentalidad que se encuentran en la literatura del error que junto a mis 40 años de experiencia me permitieron concluir y observar el gran porcentaje de acciones que terminan en accidentes leves y graves.

#### **CAUSAS INMEDIATAS ACTOS INSEGUROS (ERROR) 2010-2018**

Falta de atención cond. Piso vecindades.....	30%
Adoptar posición insegura.....	18%
No asegurar o advertir .....	17%
Limpieza, lubricar o reparación de equipo móvil .....	15%
Uso inapropiado de manos o partes del cuerpo .....	7%
Omitir el uso de protección personal .....	5%
Uso inadecuado de equipo.....	4%
Colocar, mezclar, combinar etc. Inseguramente .....	3%
Operar/trabajar a velocidad insegura .....	2%
Errores de conducción.....	1%



## ¿CUAL ERA EL PROBLEMA?

¿Por qué nos accidentamos? 3 millones de personas mueren al Año?



En la anterior grafica que corresponde a la pirámide de nuestras investigaciones y llamada PIRAMIDE BUTRON que usamos en nuestro modelo de intervención neuro-conductual BRAIN SAFETY encontramos lo siguiente:

Dentro de los porcentajes que afectan los factores humanos o causas básicas:

EL 65% de los accidentes ocurren por problemas de Neuro competencias. El 30% de los accidentes laborales se producen por deficiencias de conocimiento en las tareas aplicadas

EL 5% de los accidentes de trabajo son por capacidad física o fisiológica inadecuada.

Al observar las cifras mencionadas encontramos que el 95% de las causas inmediatas son por actos inseguros y una de las alteraciones que más encontramos son la distracción, atención, y problemas de memoria(olvido). Al integrar esta información de causas inmediatas y básicas encontramos que el sistema emocional y Arousal juega un papel importante en los riesgos neurocognitivos, conocimientos, habilidades y en los procesos de atención, memoria, organización, planificación, control inhibitorio, Meta cognición, y flexibilidad cognitiva.

También pude comprobar que, en los factores de trabajo, el 50% se da por falta de liderazgo o supervisión

inadecuada, es decir, aunque existe un supervisor, no es un neurolíder en el control de los accidentes laborales.

En **NEUROSEGURIDAD** estudiamos una serie de estructuras y funciones neurocognitivas que a continuación detallamos:

### 1. Funciones ejecutivas superiores, ¿Qué son?

Son aquellas actividades mentales complejas que están en el cerebro del trabajador y que le permiten planear, organizar, revisar estrategias, evaluar comportamientos y tomar decisiones entre otras al momento de ejecutar una labor. Podemos gestionar el fortalecimiento de las funciones superiores para modificar los hábitos y conductas inconscientes del trabajador, gracias a la neuro plasticidad cerebral.

#### 1.1. La Atención.

Es el proceso que nos permite enfocarnos en un estímulo o tarea específica, ignorando gracias a Sara los otros distractores alrededor, es la capacidad que tenemos de seleccionar y concentrar nuestros recursos mentales en un objetivo a tarea en particular.

Es uno de los componentes de la cognición y su ausencia o deficiencia es uno de los elementos que pueden originar el error.

Existen varios tipos de atención:

La atención focalizada es la capacidad de concentrar la atención en una labor o actividad específica, es fundamental para realizar tareas complejas y disminuir la ocurrencia del error.

La atención dividida, una de las causas más frecuentes en la ocurrencia del error.

Es cuando se hacen dos cosas al mismo tiempo, seleccionando más de una información al mismo tiempo alternando tareas.

## 1.2. La Memoria.

Es la capacidad que tiene el cerebro para almacenar, retener y recuperar información, aun cuando al hacerlo reconstruya lo almacenado dependiendo de las emociones experimentadas en su almacenamiento.

La memoria nos permite recordar lo aprendido, y utilizar lo guardado para la toma de decisiones, resolver problemas, innovar, o interactuar con el mundo que nos rodea.

La memoria puede ser influenciada por factores como la atención, la motivación, estrés y la práctica.

Se divide en varias categorías, de largo plazo la que guarda lo aprendido y la de corto plazo con la que guardamos nuevos sucesos o procedimientos para ejercer nuestras actividades diarias.

## 2. ¿Qué es una emoción?

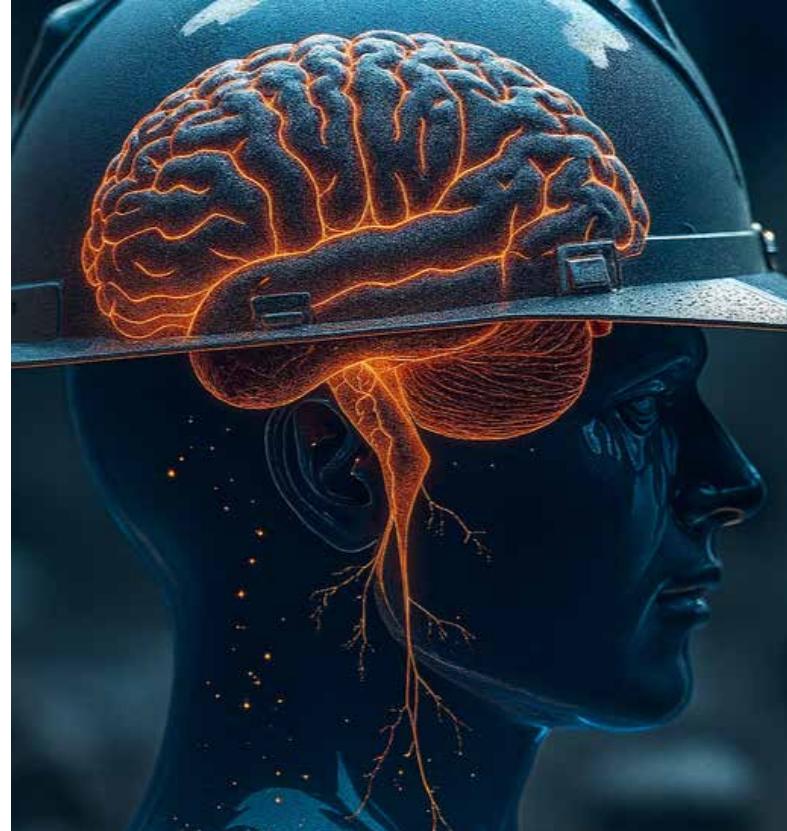
Es el conjunto de cambios que se producen en el estado corporal de una persona, inducidos por los terminales de las neuronas situadas en los diferentes órganos del cuerpo y que están controladas por las determinadas áreas del sistema cerebral, las cuales a su vez responden a el pensamiento del sujeto.

## 3. Conocimiento y habilidades

Es muy importante en la prevención del accidente que el trabajador tenga los conocimientos, habilidades y destreza para el oficio y la tarea requerida. El hombre adulto aprende mediante la disciplina de la andragogía que es muy diferente al aprendizaje de los niños. El cerebro adulto aprende con tres variables importantes: motivación al aprendizaje, atención y memoria, y al integrar estas tres variables se adquiere la nueva competencia para la tarea

### Cognición: Interpretación del significado y del conocimiento.

El conocimiento es la información que una persona adquiere a través de la educación, habilidades experimentación, observación.



**El problema para la gestión del error es que durante nuestras actividades la mente no Consciente solo ejecuta el 95% de nuestras actividades, mientras que la mente Consciente solo ejecuta el 5% restante de esa actividad.**



La reflexión es la capacidad que adquirimos para comprender, interpretar, aplicar lo aprendido, para tomar decisiones, resolver problemas y alcanzar los objetivos que nos planteamos.

#### **4. Estrés**

Es el conjunto de síntomas que comienzan aparecer lentamente en la medida que nuestros neurotransmisores en nuestro sistema nervioso central se van consumiendo por sobreuso y mal uso de nuestras funciones

#### **5. Fatiga**

Es el estado de cansancio físico o mental que resulta en una disminución del estado de alerta con el deterioro o perdida del rendimiento, la eficacia y la habilidad

La alerta es la situación de vigilancia, atención y control que debe de tener un trabajador para percibir el peligro

#### **6. Cognición social**

En el año 1996 el neurocientífico Giacomo Rizzolatti descubre las neuronas espejo que son la base neurobiológica de la empatía. La empatía no es colocarse en los zapatos de otro. En neurociencia definimos varios conceptos de empatía y para efectos del neuro liderazgo en seguridad existe 3 tipos de empatía:

Empatía cognitiva: Es cuando el líder es capaz de saber como ve las cosas la otra persona Empatía emocional: Es cuando el líder siente lo que siente la otra persona

Preocupación empática: Es cuando el líder esta predisposto a ayudar alguien necesitado

Autor :

Dr Efraín Butrón Palacio

Gerente técnico

CINCO- NEUROCINCO

Consultor, investigador, autor 11 libros neuropreven-ción



#### **EFRAÍN BUTRÓN PALACIO**

- Médico Especialista en Medicina del trabajo.
- Medico Especialista gerencia en organizaciones.
- Coach Neurocognitiva internacional.
- Certificado en neurolingüística.
- Consultor e Investigador de las Neurociencias cognitivas aplicadas a la seguridad y salud laboral (Neuroseguridad y Neuroliderazgo)
- Conferencista Nacional e Internacional y docente universitario
- Autor de 10 libros de Neuroseguridad y Neuroliderazgo,
- Creador del modelo BRAIN SAFETY CINCO.
- Premiado en España, Colombia y otros países por sus aportes e investigaciones en el campo de las Neurociencias aplicadas.
- Director técnico en múltiples empresas intervenidas en riesgo crítico y director de NEUROCINCO BRAIN SAFETY



# PREPARACIÓN INTEGRAL EN SEGURIDAD PARA UN FUTURO MÁS PROTEGIDO



**CON FORMACIÓN PRÁCTICA Y  
ESTRATEGIAS EFECTIVAS**

[www.corporacionrojo.com](http://www.corporacionrojo.com)



## IDEAS QUE DETONAN RESULTADOS, NO RIESGOS

En un mundo donde la seguridad es clave, nosotros encendemos la chispa de la **creatividad estratégica**. Creamos campañas que hacen explotar la rutina, protegiendo la **esencia de tu marca** y elevando su presencia.

**Innovación audaz. Seguridad total.**





100%  
VIRTUAL

Síncrono y Asíncrono

# GESTION ESTRATEGICA

## DE SEGURIDAD BANCARIA



Convierte la seguridad bancaria  
**EN ESTRATEGIA CORPORATIVA**



**Inicio:** 27 de octubre 2025  
**Duración:** 60 horas certificados