# REAL

RED DE EXPERTOS & ANALISTAS LATINOAMERICANOS

REAL
RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

TEMA DE LA EDICIÓN

# El nuevo mapa

*Cómo América Latina produce, protege y aplica su inteligencia*

EN ESTA EDICIÓN


| | |
|---|---|
| GEOPOLÍTICA | Escenario geopolítico latinoamericano |
| SALUD DIGITAL | Salud digital bajo asedio |
| CIBERSEGURIDAD | Identidades no humanas |


N.º 02 ABRIL–JUNIO 2026 REVISTA DE ANÁLISIS ESTRATÉGICO

# En esta edición


01 GEOPOLÍTICA 6

## Escenario geopolítico latinoamericano

*El nuevo ciclo político latinoamericano abre oportunidades de cooperación regional en seguridad, pero también amenazas de autoritarismo electoral y militarización si se reduce a discursos de mano dura sin reforma institucional.*

General PNP (r) Mauricio Quiroga Camacho

02 INTELIGENCIA ESTRATÉGICA 18

## Inteligencia para el desarrollo

*América Latina y el Caribe deben modernizar sus sistemas de inteligencia como ya lo hacen las democracias desarrolladas, con un doble mandato: proteger los intereses vitales de la Nación e impulsarlos.*

Licenciado Edgardo Glavinich

03 SALUD DIGITAL 29

## Salud digital bajo asedio

*La región conectó sus hospitales antes de aprender a protegerlos: un análisis de la exposición técnica, los vacíos regulatorios y los nuevos riesgos que introduce la inteligencia artificial clínica.*

Magíster Norman Oré Olivera

04 CIBERSEGURIDAD 42

## Identidades no humanas

*La incorporación de agentes autónomos de inteligencia artificial obliga a repensar la identidad digital: ya no basta con proteger contraseñas humanas, hay que gobernar identidades que actúan por sí solas.*

Magíster Fernando Margarito Velázquez Flores

05 ANÁLISIS DE INTELIGENCIA 52

## La sabiduría popular aplicada al análisis de inteligencia estratégica

*Cinco refranes populares como marco para explicar los principios fundamentales del buen análisis de inteligencia: especialización, oportunidad, prevención, humildad intelectual y aprendizaje del error.*

Antropólogo Francisco Girao Morales

06 SEGURIDAD PATRIMONIAL 57

## Seguridad patrimonial en la Amazonía peruana

*La agroindustria, la acuicultura y el biocomercio amazónicos generan nuevos activos y nuevos riesgos: proteger un territorio extenso exige información, tecnología y procedimientos, no solo más cercos y vigilantes.*

Ingeniera Dunia Valencia Felices

Editorial · Quiénes somos · Sobre los autores · Equipo editorial · REAL en el mundo

# Pensar la región en tiempos de recomposición

América Latina y el espacio iberoamericano atraviesan un período de profundas transformaciones, tensiones e incertidumbres. Los desafíos en materia de seguridad, defensa, desarrollo y democracia ya no pueden ser comprendidos ni abordados desde miradas aisladas, fragmentadas o estrictamente nacionales.

Esta segunda edición de la Revista REAL reúne seis análisis que, desde disciplinas y experiencias distintas, convergen en una misma pregunta: cómo piensa y produce inteligencia estratégica una región que atraviesa, simultáneamente, una revolución tecnológica de sus capacidades de análisis y una recomposición política de su mapa de gobiernos.

Mauricio Quiroga Camacho abre el número con un análisis extenso del nuevo mapa político latinoamericano, tras el retroceso del ciclo progresista y el ascenso de gobiernos de derecha en la región, y sus efectos sobre la gobernabilidad y la seguridad transfronteriza. Edgardo Glavinich ofrece el marco conceptual: la revolución de los asuntos de inteligencia del siglo XXI y su doble mandato de proteger e impulsar los intereses de la región. Norman Oré Olivera examina la exposición de los sistemas sanitarios latinoamericanos ante las ciberamenazas, y sostiene que la región conectó sus hospitales antes de aprender a protegerlos. Fernando Velázquez Flores prolonga esa reflexión hacia los agentes autónomos de inteligencia artificial como nuevas identidades operativas dentro de las organizaciones. Francisco Girao Morales aporta una mirada cercana y aplicada, articulando la sabiduría popular con los principios fundamentales del análisis profesional. Y finalmente Dunia Valencia Felices cierra la edición llevando la seguridad al territorio amazónico, donde proteger un patrimonio exige información y tecnología antes que presencia física.

Seis voces, seis disciplinas, un mismo compromiso: producir conocimiento riguroso, plural y útil para quienes toman decisiones en materia de seguridad, defensa, desarrollo y democracia en las Américas.

Comité Editorial

**REAL — Red de Expertos y Analistas Latinoamericanos**

LA CIFRA DE LA EDICIÓN

# 25%

de los homicidios del mundo ocurren en América Latina y el Caribe,
una región que reúne apenas el **8 %** de la población global

---

Dato citado en el artículo de Edgardo Glavinich · Fuente: Fundación Sherman Kent (2025)

# Quiénes somos

La Red de Expertos y Analistas Latinoamericanos (R.E.A.L.) es una ONG internacional con sede en Washington, D.C., que se dedica a ofrecer servicios de asesoría y consultoría estratégica a nivel internacional.

Su misión es proporcionar servicios de asesoría y consultoría estratégica autónomos, transparentes y profesionales en temas de seguridad, defensa, desarrollo y democracia. R.E.A.L. se enfoca en la creación de un continente americano resiliente, seguro y próspero, donde la democracia, las libertades individuales y los derechos humanos sean fundamentales.


● Sede institucional ● Países con expertos y analistas de la red (13)

La red REAL: sede en Washington, D.C. y expertos en trece países de América y Europa.

ENSAYO CENTRAL

GEOPOLÍTICA

# Escenario geopolítico latinoamericano

*Tras la pérdida del ciclo petrista en Colombia y el viraje hacia la derecha regional: impactos en gobernabilidad y seguridad transfronteriza*

El nuevo ciclo político latinoamericano abre oportunidades de cooperación regional en seguridad, pero también amenazas de autoritarismo electoral y militarización si se reduce a discursos de mano dura sin reforma institucional.

01

**General PNP (r) Mauricio Quiroga Camacho**

derecha regional · fronteras · crimen organizado · gobernabilidad

**General PNP (r) Mauricio Quiroga Camacho**

CEO y Director Ejecutivo de DATA FORTE SECURITY · Ex Director de Inteligencia de la Policía Nacional del Perú · Analista estratégico en gobernabilidad, seguridad ciudadana y conflictividad social

CEO y Director Ejecutivo de DATA FORTE SECURITY. Ex Director de Inteligencia de la Policía Nacional del Perú

## Resumen

El escenario político latinoamericano atraviesa un proceso de recomposición ideológica marcado por el debilitamiento del ciclo progresista que alcanzó su punto alto durante la llamada «marea rosa» de inicios de la década de 2020. La derrota del proyecto político asociado a Gustavo Petro en Colombia, sumada al ascenso de gobiernos de derecha o centroderecha en Argentina, Chile, Perú, Ecuador, Bolivia, Panamá y otros países, configura un nuevo mapa regional orientado hacia agendas de seguridad, control migratorio, apertura económica, reducción del Estado, cooperación con Estados Unidos y endurecimiento frente al crimen organizado.

Sin embargo, este viraje no debe interpretarse como una consolidación homogénea ni estable de la derecha latinoamericana. La mayoría de estos gobiernos emerge en contextos de alta fragmentación social, márgenes electorales estrechos, crisis de representación, malestar económico, demandas por seguridad y desconfianza ciudadana hacia las instituciones. Por ello, el nuevo ciclo político abre oportunidades para fortalecer la cooperación regional en seguridad, atraer inversión, recomponer vínculos diplomáticos y mejorar la coordinación contra economías ilícitas; pero también genera amenazas vinculadas al autoritarismo electoral, la militarización de la seguridad pública, la protesta social, el deterioro de derechos, la polarización y la posible instrumentalización política del combate al crimen.

El presente documento analiza los beneficios y amenazas de este nuevo escenario para la gobernabilidad democrática y la seguridad transfronteriza, con especial atención a Colombia, Argentina, Chile y Perú, así como a los impactos regionales sobre narcotráfico, migración, crimen organizado, fronteras, minería ilegal, tráfico de armas, trata de personas y cooperación interagencial.

Palabras clave: América Latina, derecha regional, Colombia, Petro, seguridad transfronteriza, gobernabilidad, crimen organizado, narcotráfico, migración, geopolítica.

## 1. Introducción

que prometieron reformas sociales, redistribución, ampliación de derechos y autonomía frente a Washington, diversos países de la región han girado hacia liderazgos de derecha, centroderecha o derecha radical. Este cambio no surge únicamente de una preferencia doctrinaria, sino de una acumulación de frustraciones sociales: inseguridad ciudadana, expansión del crimen organizado, crisis migratoria, bajo crecimiento económico, inflación, deterioro de servicios públicos, corrupción, informalidad y percepción de pérdida de autoridad estatal.

La pérdida del proyecto petrista en Colombia tiene un valor simbólico especial. Colombia fue, durante décadas, un país asociado a gobiernos conservadores, liberales o de centroderecha. La llegada de Gustavo Petro al poder representó una ruptura histórica: por primera vez, la izquierda gobernaba el país con una propuesta de paz total, transición energética, reforma social y rediseño de la política antidrogas. La derrota de ese ciclo no solo expresa el desgaste del progresismo colombiano, sino también el retorno de una demanda ciudadana por orden, seguridad, autoridad y resultados inmediatos frente al crimen.

Este fenómeno se conecta con una tendencia política más amplia en América Latina. En Argentina, Javier Milei consolidó una reacción libertaria frente al gasto público, la inflación y el descrédito de la política tradicional. En Chile, José Antonio Kast llegó a la presidencia capitalizando, entre otros factores, la preocupación ciudadana por la delincuencia, la migración irregular y el deterioro del orden público. En Perú, la elección de Keiko Fujimori en 2026 confirmó un giro hacia una opción de derecha y conservadora, aunque en un país que mantiene profundas fracturas territoriales, sociales y políticas. En Ecuador, Daniel Noboa profundizó una estrategia de seguridad caracterizada por una mayor intervención de las Fuerzas Armadas frente al crimen organizado.

En Centroamérica, la influencia del modelo de Nayib Bukele continuó reforzando una idea cada vez más presente en la región: que la seguridad, el control territorial y la recuperación del orden pueden convertirse en importantes activos de legitimidad política. En ese contexto, la seguridad ha dejado de ser únicamente una política sectorial para convertirse en uno de los principales ejes de reorganización del poder político latinoamericano.

El problema central es que el viraje hacia la derecha ocurre en sociedades fracturadas. La ciudadanía exige orden, pero también empleo; seguridad, pero también derechos; autoridad, pero también legitimidad; frontera controlada, pero también integración regional. En ese equilibrio se jugará la gobernabilidad del nuevo ciclo.

## 2. Hipótesis de trabajo

La hipótesis principal de este documento es que el viraje hacia la derecha en América Latina puede generar una ventana de oportunidad para fortalecer la cooperación en seguridad, recomponer la autoridad estatal y construir una agenda regional contra el crimen organizado; sin em-

bargo, si esa agenda se implementa desde enfoques puramente punitivos, personalistas o militarizados, puede agravar la polarización, erosionar instituciones democráticas y desplazar las economías criminales hacia nuevas rutas transfronterizas.

En otras palabras, el giro político puede ser beneficioso si produce coordinación, inteligencia, interoperabilidad, control territorial, desarrollo fronterizo y fortalecimiento institucional. Pero puede ser riesgoso si se reduce a discursos de «mano dura» sin reforma policial, sin justicia eficaz, sin control financiero del crimen, sin inclusión social y sin cooperación internacional sostenida.

## 3. El nuevo mapa político regional

El nuevo escenario latinoamericano tiene cinco características centrales.

Primero, la seguridad se ha convertido en el principal eje electoral. El miedo al crimen organizado, la extorsión, el sicariato, el narcotráfico, la trata de personas y la migración irregular ha desplazado a otros temas tradicionales de campaña. La ciudadanía ya no evalúa únicamente ideologías, sino capacidad de control.

Segundo, la derecha regional no es uniforme. Existen derechas libertarias, como la argentina; derechas conservadoras de orden, como la chilena; derechas de seguridad territorial, como la ecuatoriana; derechas populistas de alta confrontación, como algunas expresiones colombianas; y derechas institucionales o pragmáticas, presentes en sectores empresariales y tecnocráticos. Esta heterogeneidad puede dificultar una agenda común.

Tercero, la nueva derecha se articula más por reacción que por proyecto. Su crecimiento responde al rechazo al progresismo, al hartazgo con la inseguridad y al deterioro económico. Esto le otorga fuerza electoral, pero no necesariamente capacidad de gobierno.

Cuarto, Estados Unidos recupera influencia estratégica en la región. La convergencia de gobiernos de derecha facilita acuerdos en lucha antidrogas, migración, inversión, defensa, energía, minerales críticos y control de influencia china. Sin embargo, también puede generar tensiones con países que mantienen gobiernos de izquierda o posiciones más autónomas.

Quinto, la gobernabilidad será el principal desafío. Muchos de estos gobiernos enfrentan congresos divididos, protestas sociales, sindicatos fuertes, movimientos indígenas, oposición organizada, judicaturas independientes y sociedades altamente polarizadas.

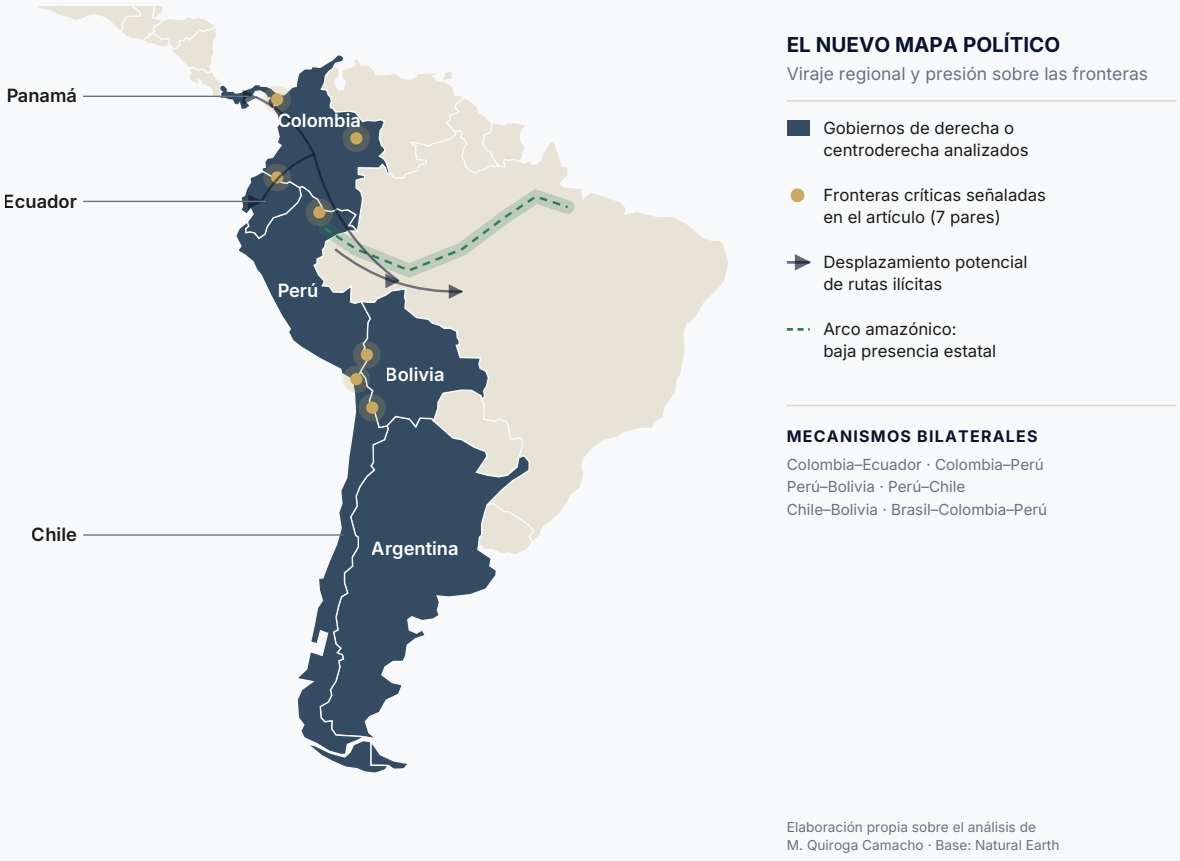
## 4. Colombia como punto de inflexión

Colombia ocupa un lugar estratégico en este análisis por tres razones: su ubicación geográfica, su rol en la economía mundial de la cocaína y su importancia en la relación entre América del Sur, Centroamérica, el Caribe y Estados Unidos.

La derrota del proyecto petrista implica el probable abandono o rediseño de la política de «paz total», así como un retorno a estrategias más duras contra grupos armados, narcotráfico, cultivos ilícitos, minería ilegal y control territorial. Esto puede generar beneficios inmediatos si fortalece la presencia estatal en zonas abandonadas y reactiva la cooperación internacional. Sin embargo, también puede producir riesgos si se rompe el equilibrio entre acción militar, negociación política, desarrollo alternativo y protección de comunidades.

Colombia enfrenta una estructura criminal compleja: disidencias de las FARC, ELN, Clan del Golfo, redes narcotraficantes, grupos locales, minería ilegal, corredores hacia Venezuela, Ecuador, Panamá, Perú, Brasil y el Pacífico. No se trata de un problema únicamente policial; es un problema de soberanía efectiva, economías ilícitas, gobernanza territorial y captura criminal de comunidades.

El nuevo gobierno colombiano podría buscar una nueva etapa de cooperación con Estados Unidos, Perú, Ecuador, Panamá y Chile. Esto abriría oportunidades para una arquitectura regional de seguridad. Pero también podría generar tensiones con Venezuela y con sectores sociales internos si la agenda se percibe como represiva o subordinada a intereses externos.




Los países del viraje, las fronteras críticas y el desplazamiento potencial de rutas ilícitas.

## 5. Argentina: giro libertario y reposicionamiento externo

Argentina representa una variante particular dentro del giro político regional. El liderazgo de Javier Milei no se articula principalmente alrededor de la seguridad pública, sino de una ruptu-

ra económica, política e ideológica con el estatismo, el intervencionismo y buena parte de la tradición peronista. Su proyecto se sustenta en la liberalización económica, la reducción del peso del Estado y una intensa "batalla cultural" contra sectores que identifica con la izquierda y el progresismo. En política exterior, su gobierno ha profundizado un alineamiento estratégico con Estados Unidos e Israel, acompañado de una creciente articulación con sectores liberales y conservadores de la derecha internacional.

El beneficio geopolítico para la región es que Argentina puede convertirse en un actor relevante en energía, litio, alimentos, minería, defensa y cooperación tecnológica. Una Argentina más abierta al capital privado y alineada con Occidente puede atraer inversiones y fortalecer cadenas estratégicas regionales.

No obstante, el riesgo está en la conflictividad social derivada de ajustes fiscales, reducción del gasto, pérdida de poder adquisitivo y tensión con sindicatos. La gobernabilidad argentina dependerá de si el programa económico logra estabilización sin romper la cohesión social. Si fracasa, puede producir un efecto búmeran contra la derecha regional.

## 6. Chile: seguridad, migración y orden institucional

Chile es relevante porque su giro hacia la derecha se produce en un país históricamente valorado por su institucionalidad. El ascenso de José Antonio Kast expresa una demanda de orden frente al aumento de delitos violentos, migración irregular y percepción de debilitamiento estatal.

El beneficio potencial es la recuperación de capacidades de control fronterizo, especialmente en el norte chileno, donde convergen rutas migratorias, contrabando, trata de personas y tráfico de drogas. Chile también puede impulsar cooperación con Perú y Bolivia en materia de inteligencia fronteriza, control documental, biometría, lucha contra redes de tráfico de migrantes y persecución patrimonial.

La amenaza es que una política centrada exclusivamente en expulsiones, zanjas, presencia militar o retórica antimigrante puede desplazar rutas ilegales sin resolverlas. Además, puede tensionar relaciones con Perú, Bolivia, Venezuela y organismos internacionales. Chile requiere un modelo de seguridad fronteriza inteligente, con tecnología, inteligencia financiera, cooperación judicial y canales humanitarios ordenados.

## 7. Perú: gobernabilidad frágil y seguridad transfronteriza

Perú ocupa una posición estratégica por sus fronteras con Colombia, Ecuador, Brasil, Bolivia y Chile, y por su papel en la producción y tránsito de cocaína, minería y tala ilegales, contrabando, trata de personas y flujos migratorios. El gobierno de Keiko Fujimori tiene la posibilidad de fortalecer la cooperación con Colombia, Ecuador y Chile en seguridad fronteriza, intensificar la lucha contra las economías ilícitas en el VRAEM, la Amazonía, la frontera norte y el corredor

sur, y promover mayor interoperabilidad entre Policía Nacional, Fuerzas Armadas, Migraciones, SUNAT, inteligencia financiera, fiscalías especializadas y gobiernos regionales.

Un eventual gobierno de derecha o centroderecha puede reforzar la cooperación con Colombia, Ecuador y Chile en seguridad fronteriza. Puede, además, impulsar una política más activa contra economías ilícitas en el VRAEM, la Amazonía, la frontera norte y el corredor sur. También puede promover interoperabilidad entre Policía Nacional, Fuerzas Armadas, Migraciones, SUNAT, inteligencia financiera, fiscalías especializadas y gobiernos regionales.

Sin embargo, el nuevo gobierno enfrenta una amenaza interna severa: fragmentación política, desconfianza institucional, conflictividad social, informalidad económica y profundas brechas territoriales. Una estrategia de seguridad que ignore el malestar del sur andino, las economías informales y la débil representación política puede generar protestas, bloqueos, violencia social y un rápido desgaste gubernamental.

La seguridad peruana no puede reducirse al control policial. El desafío para la nueva administración será articular inteligencia estratégica, inversión social focalizada, recuperación de carreteras, puertos y pasos fronterizos, lucha contra el lavado de activos, modernización policial, justicia eficaz y control de mercados ilícitos, combinando autoridad estatal con presencia territorial y legitimidad institucional.

## 8. Beneficios estratégicos del viraje hacia la derecha

El viraje regional puede generar varios beneficios para la gobernabilidad y la seguridad.

8.1. Mayor convergencia en seguridad regional. La coincidencia ideológica entre gobiernos de derecha puede facilitar acuerdos operativos contra el narcotráfico, la minería ilegal, el tráfico de armas, la trata de personas y el lavado de activos. Una región con prioridades comunes puede compartir inteligencia, bases de datos, alertas migratorias, perfiles criminales, rutas ilícitas y mecanismos de persecución patrimonial.

8.2. Reactivación de la cooperación con Estados Unidos. La región puede acceder a cooperación técnica, equipos, capacitación, tecnología, vigilancia aérea, control marítimo, interdicción y asistencia financiera. Esto puede fortalecer a policías, fuerzas armadas, fiscalías, unidades de inteligencia financiera y agencias migratorias.

8.3. Atracción de inversión privada. Gobiernos con agendas de apertura económica pueden atraer inversión en energía, minería, infraestructura, agroindustria, puertos, logística y tecnología. Si esa inversión se distribuye territorialmente, puede reducir economías ilegales y generar empleo formal en zonas vulnerables.

8.4. Recuperación del principio de autoridad. En sociedades afectadas por extorsión, sicariato y crimen organizado, el restablecimiento de autoridad estatal puede mejorar la confianza ciuda-

dana. La población suele demandar presencia policial, justicia efectiva y control de espacios públicos.

8.5. Posibilidad de una arquitectura regional contra el crimen organizado. El nuevo escenario permite pensar en una alianza sudamericana contra economías ilícitas, con énfasis en inteligencia criminal, control financiero, vigilancia marítima, fronteras amazónicas, pasos terrestres, puertos, aeródromos clandestinos y redes digitales criminales.

## 9. Amenazas para la gobernabilidad

Los beneficios anteriores no están garantizados. Existen amenazas relevantes.

9.1. Polarización y legitimidad débil. Muchos gobiernos de derecha llegan al poder con sociedades divididas. Si gobiernan bajo lógica de revancha, pueden activar protestas, radicalización opositora y bloqueo legislativo. La gobernabilidad requiere pactos mínimos, no solo victoria electoral.

9.2. Tentación autoritaria. La demanda por seguridad puede justificar estados de excepción permanentes, debilitamiento de controles judiciales, restricciones a derechos, persecución política y militarización de la vida civil. Esto puede producir resultados aparentes de corto plazo, pero deteriorar la democracia.

9.3. Militarización sin reforma institucional. El despliegue militar puede ser útil en situaciones excepcionales, pero no reemplaza a la policía, la fiscalía, la inteligencia ni el sistema penitenciario. Sin investigación criminal, sin jueces, sin cárceles controladas y sin inteligencia financiera, la mano dura solo desplaza el delito.

9.4. Protesta social por ajustes económicos. La reducción del gasto público, la eliminación de subsidios o las reformas laborales pueden generar conflictividad social. Si estas medidas coinciden con inseguridad, inflación o desempleo, los gobiernos pueden perder apoyo rápidamente.

9.5. Tensiones diplomáticas. El giro hacia gobiernos de derecha o centroderecha en varios países de Sudamérica puede fortalecer la cooperación con Estados Unidos en seguridad, defensa, comercio y lucha contra el crimen organizado, pero también generar nuevas tensiones con gobiernos de izquierda de la región y obligar a una relación más pragmática con China. El desafío será evitar una polarización ideológica que fracture los mecanismos de integración regional y convierta las diferencias políticas en obstáculos para la cooperación fronteriza, energética, comercial y de seguridad. En este nuevo escenario, Sudamérica deberá equilibrar afinidades ideológicas, intereses económicos y competencia geopolítica sin quedar atrapada entre bloques enfrentados.

## 10. Amenazas para la seguridad transfronteriza

10.1. Reacomodo de rutas del narcotráfico. Cuando un país endurece controles, las organizaciones criminales no desaparecen necesariamente: se desplazan. Mayor presión en Colombia puede mover rutas hacia Ecuador, Perú, Brasil, Panamá o el Caribe. Mayor control en Chile puede mover flujos hacia pasos clandestinos de Bolivia o Perú.

10.2. Fragmentación criminal. La captura de grandes líderes puede producir atomización de bandas, disputas por territorios y aumento de violencia. Esto se ha visto en varios países donde la desarticulación parcial de organizaciones genera guerras internas.

10.3. Criminalización de la migración. Las redes criminales aprovechan la migración vulnerable. Pero si el Estado confunde migrante con delincuente, debilita la cooperación comunitaria, alimenta xenofobia y empuja a sectores vulnerables hacia redes ilegales.

10.4. Fronteras amazónicas débiles. La Amazonía sudamericana es un espacio crítico. Allí convergen minería ilegal, tala, tráfico de drogas, trata, pistas clandestinas, ríos sin control, comunidades abandonadas y baja presencia estatal. La seguridad transfronteriza debe mirar más allá de los pasos oficiales.

10.5. Lavado de activos y economías legales contaminadas. El crimen organizado ya no opera solo en la calle. Invierte en construcción, minería, comercio, transporte, casas de cambio, fintech, apuestas, exportaciones, pesca, agroindustria y política local. Sin inteligencia financiera regional, cualquier política de seguridad será incompleta.

MATRIZ PROSPECTIVA

## Cuatro escenarios para el nuevo ciclo

Según el grado de coordinación regional y la calidad institucional del giro político


Elaboración propia sobre la sección 11 del artículo de M. Quiroga Camacho

Los cuatro escenarios del artículo, ordenados por coordinación regional y calidad institucional.

## 11. Escenarios prospectivos

Escenario 1: Convergencia democrática de seguridad. Los gobiernos de derecha coordinan políticas regionales, fortalecen instituciones, respetan controles democráticos, mejoran capacidades policiales y judiciales, y reducen espacios criminales. Es el escenario más favorable.

Escenario 2: Mano dura fragmentada. Cada país aplica medidas punitivas sin coordinación regional. El delito se desplaza, las cárceles se saturan, crece la violencia y se debilitan derechos. Es un escenario probable si predomina la improvisación.

Escenario 3: Polarización y crisis de gobernabilidad. Los gobiernos enfrentan protestas por ajustes económicos, acusaciones de autoritarismo y oposición legislativa. La seguridad se politiza, las instituciones se desgastan y el crimen aprovecha la distracción estatal.

Escenario 4: Reconfiguración geopolítica proestadounidense. La mayoría de gobiernos de derecha se alinea con Washington en seguridad, migración, energía y China. Puede fortalecer cooperación, pero también tensionar relaciones comerciales con Asia y dividir organismos regionales.

## 12. Recomendaciones estratégicas

Primero, construir una agenda regional de seguridad transfronteriza basada en inteligencia, no solo en fuerza. Los países deben compartir información sobre rutas, personas, empresas de fachada, movimientos financieros, armas, vehículos, embarcaciones, aeronaves y redes digitales.

Segundo, crear mecanismos bilaterales permanentes en fronteras críticas: Colombia-Ecuador, Colombia-Perú, Perú-Bolivia, Perú-Chile, Chile-Bolivia, Brasil-Colombia-Perú y la zona amazónica. Estos mecanismos deben incluir policía, fiscalía, migraciones, aduanas, inteligencia financiera y fuerzas armadas cuando corresponda.

Tercero, fortalecer la persecución patrimonial. El crimen organizado se derrota afectando su dinero, no solo capturando operadores. Deben priorizarse lavado de activos, extinción de dominio, testaferros, contratación pública contaminada y economías legales infiltradas.

Cuarto, evitar la militarización permanente. La participación militar debe ser excepcional, regulada, temporal y subordinada a autoridad civil. La seguridad ciudadana requiere policías profesionales, inteligencia criminal y justicia eficaz.

Quinto, diferenciar migración de criminalidad. La migración debe ser ordenada, registrada y controlada, pero no criminalizada de manera general. Las redes de trata y tráfico de migrantes sí deben ser tratadas como organizaciones criminales transnacionales.

Sexto, vincular seguridad con desarrollo territorial. En zonas de frontera, el Estado debe llegar con escuelas, salud, carreteras, internet, formalización, justicia, bancos y empleo. Donde no llega el Estado, llega el crimen.

> **Donde no llega el Estado, llega el crimen.**

Séptimo, preservar la gobernabilidad democrática. Los nuevos gobiernos de derecha deben entender que seguridad sin legitimidad puede ser combustible para nuevas crisis. La autoridad estatal debe actuar con firmeza, pero también con legalidad, transparencia y rendición de cuentas.

## 13. Conclusiones

El viraje hacia la derecha en América Latina expresa una respuesta ciudadana al miedo, la inseguridad, el deterioro económico y el agotamiento de proyectos progresistas que no lograron satisfacer expectativas de orden y bienestar. La pérdida del ciclo petrista en Colombia tiene un impacto simbólico y geopolítico profundo porque desplaza a uno de los principales referentes de la izquierda regional y acerca a Colombia a una constelación de gobiernos más próximos a agendas de seguridad dura, mercado y cooperación con Estados Unidos.

No obstante, el nuevo ciclo no está exento de fragilidad. La derecha regional llega con apoyo social, pero también con sociedades divididas, economías tensionadas, congresos fragmentados y crimen organizado adaptativo. El mayor error sería creer que la mano dura, por sí sola, resuelve problemas estructurales. El crimen organizado latinoamericano opera como sistema económico, político, territorial y transnacional. Por tanto, requiere una respuesta integral.

> **El mayor error sería creer que la mano dura, por sí sola, resuelve problemas estructurales.**

> **eficaces, instituciones confiables y democracias capaces de proteger a sus ciudadanos frente al crimen.**

La oportunidad histórica consiste en convertir la convergencia política regional en una verdadera arquitectura de seguridad democrática: inteligencia compartida, fronteras controladas, persecución financiera, cooperación judicial, control migratorio ordenado, modernización policial y desarrollo territorial. La amenaza es que el viraje derive en populismo punitivo, autoritarismo electoral, polarización y desplazamiento del delito hacia nuevas rutas.

La gobernabilidad del nuevo ciclo dependerá de una fórmula compleja: autoridad sin abuso, seguridad sin autoritarismo, mercado sin exclusión, frontera sin xenofobia y cooperación internacional sin pérdida de autonomía estratégica. América Latina no necesita solo gobiernos fuertes; necesita Estados eficaces, instituciones confiables y democracias capaces de proteger a sus ciudadanos frente al crimen, sin convertirse ellas mismas en una fuente de arbitrariedad.

*Lima, 20 de junio de 2026*

INTELIGENCIA ESTRATÉGICA

# Inteligencia para el desarrollo

*La revolución de los asuntos de inteligencia del siglo XXI: amenazas, oportunidades y modernización del Estado en América Latina y el Caribe*

América Latina y el Caribe deben modernizar sus sistemas de inteligencia como ya lo hacen las democracias desarrolladas, con un doble mandato: proteger los intereses vitales de la Nación e impulsarlos.

02

**Licenciado Edgardo Glavinich**

revolución de la inteligencia · FIMI · seguridad económica · control democrático

> «La inteligencia es conocimiento, y conocimiento para la acción.»
>
> Sherman Kent (1949)

**Licenciado Edgardo Glavinich**

Director Ejecutivo, Fundación Sherman Kent · Consultor en inteligencia estratégica · Docente de posgrado

Director Ejecutivo de la Fundación Sherman Kent (fundacionkent.org). Consultor para gobierno y el sector privado en materia de inteligencia estratégica

## Introducción

Toda época tiene una transformación que redefine el modo en que los Estados se protegen y prosperan. La del siglo XXI es la revolución de los asuntos de inteligencia: un cambio tan profundo en las capacidades, los métodos y el alcance de la inteligencia como el que, en su momento, produjeron la aviación o la energía nuclear en los asuntos militares. La irrupción de las fuentes abiertas, la inteligencia artificial, la analítica de grandes volúmenes de datos y la manipulación informativa a escala industrial alteraron, en menos de dos décadas, aquello que un Estado puede observar, anticipar y decidir. Comprender esa revolución, y actuar en consecuencia, es hoy una condición del desarrollo, no un tecnicismo de especialistas.

Esa revolución tiene dos caras que este artículo se propone no separar. La primera es la agenda de amenazas, que no se desvanece, se transforma y se agrava. La segunda es la agenda de oportunidades, que la mirada puramente defensiva suele desatender. Un servicio de inteligencia moderno cumple, por eso, un doble mandato: protege a la Nación de lo que la amenaza e ilumina las oportunidades que le permiten crecer. Las democracias desarrolladas ya reorganizan sus sistemas bajo esa lógica; América Latina y el Caribe, en cambio, corren el riesgo de importar las capacidades sin modernizar la gestión, la gobernanza ni la doctrina.

## 1. La revolución de los asuntos de inteligencia: qué cambió

Cuatro fuerzas definen esta revolución. La primera es la democratización de las fuentes abiertas: el conocimiento estratégico dejó de ser un monopolio estatal, y hoy es posible producir inteligencia de alto valor a partir de información pública, con una fracción del costo y del riesgo de los métodos clásicos. La segunda es la inteligencia artificial y la analítica de datos, que permiten clasificar, correlacionar y anticipar patrones a una velocidad inédita, pero introducen

una doble opacidad, la del secreto y la del algoritmo, que plantea desafíos nuevos de gobernanza. La tercera es la manipulación informativa extranjera —conocida por su sigla FIMI—, producida de manera deliberada como instrumento de competencia entre Estados; y la cuarta es la seguridad económica: la conversión de los recursos, las tecnologías y las cadenas de suministro en cuestiones de inteligencia y de Estado.

> **Estas fuerzas comparten un rasgo decisivo: desplazan el centro de gravedad de la inteligencia desde el secreto hacia el procesamiento.**

Estas fuerzas comparten un rasgo decisivo: desplazan el centro de gravedad de la inteligencia desde el secreto hacia el procesamiento. El valor ya no reside tanto en poseer un dato que nadie más tiene, sino en interpretar mejor y más rápido una información crecientemente disponible. Es la definición que Sherman Kent (1949) y, tras él, Washington Platt (1974) anticiparon al concebir la inteligencia como conocimiento elaborado para la acción, y no como mero acopio de secretos. Esa revolución multiplica el poder analítico del Estado y, con él, tanto su capacidad de proteger como su capacidad de intrusión: por eso es, de manera inseparable, una revolución de las capacidades y un problema de control.

## 2. La agenda de amenazas no desaparece: se transforma

Sería un error leer la revolución de la inteligencia como una invitación a bajar la guardia. En

su historia contemporánea. El primer informe de la Fundación Sherman Kent, que evalúa 33 países de la región, lo documenta con precisión: la región alberga apenas el 8 % de la población mundial, pero registra alrededor del 25 % de los homicidios globales, mientras las organizaciones criminales transnacionales generan ingresos anuales superiores a los 150.000 millones de dólares (Fundación Sherman Kent, 2025). No se trata de delincuencia común, sino de estructuras con capacidad de disputar el control territorial al Estado.

A esa base tradicional se suman amenazas que la revolución tecnológica potencia. El terrorismo internacional mantiene presencia operativa en la región; la ciberseguridad revela vulnerabilidades alarmantes, con un promedio de ataques semanales por organización muy por encima de la media global; y la penetración estratégica extranjera, mediante inversión dirigida y control de infraestructura crítica, avanza de manera sistemática (Fundación Sherman Kent, 2025). La inteligencia extranjera y las operaciones de influencia completan un cuadro en el que las amenazas ya no son solo físicas, sino también digitales, económicas y cognitivas. La revolución de los asuntos de inteligencia no eliminó la agenda de amenazas, la volvió multidimensional, y por eso exige sistemas más sofisticados, no menos.

## 3. Cómo se moderniza Occidente: cuatro respuestas a la revolución

Las democracias desarrolladas entendieron que la revolución de los asuntos de inteligencia obliga a reformar los sistemas, y lo hicieron atacando distintas dimensiones del problema. Cuatro casos recientes ofrecen un mapa útil. Japón, tradicionalmente reticente en materia de inteligencia, sancionó en mayo de 2024 la Ley de Protección y Utilización de Información Importante de Seguridad Económica, en vigor desde mayo de 2025, que instauró por primera vez un sistema de habilitaciones de seguridad para funcionarios y personal del sector privado; en paralelo, impulsa elevar su Oficina de Inteligencia e Investigación del Gabinete a una Agencia Nacional de Inteligencia, crear un Consejo Nacional de Inteligencia presidido por el primer ministro y establecer un registro de agentes extranjeros (The Diplomat, 2026; The Japan Times, 2026). Es la respuesta al eje de la seguridad económica.

Los Países Bajos abordaron el eje cibernético: su Ley Temporal de Operaciones Cibernéticas, en vigor desde julio de 2024, amplió las facultades de sus servicios (AIVD y MIVD) para responder con mayor rapidez a las amenazas de Estados hostiles, aunque de manera reveladora acompañó esa ampliación con un reajuste del control, desplazando parte de la autorización previa hacia una revisión posterior a cargo de su comisión independiente de supervisión (AboutIntel, 2024). Suecia atacó el eje cognitivo: creó en 2022 su Agencia de Defensa Psicológica, única en su tipo, para blindar a la población, las organizaciones y las empresas frente a la manipulación informativa extranjera, y en 2026 lanzó su primera estrategia nacional de defensa psicológica (Swedish Psychological Defence Agency, 2026). Alemania, por su parte, reformó el eje del control: tras la sentencia de su Tribunal Constitucional Federal de 2020, que declaró inconstitucional la vigilancia exterior de su servicio, instituyó en 2021 un consejo de control independiente de rango cuasi judicial (Bundesverfassungsgericht, 2020).

La lección para América Latina es doble. Primero, que la modernización no es un lujo de países ricos, sino la condición para que la revolución de las capacidades se traduzca en seguridad y desarrollo, y no en dependencia o abuso. Segundo, que en todos estos casos la ampliación del poder vino acompañada de una recalibración del control; ninguna de estas democracias amplió sus capacidades sin, a la vez, reforzar los mecanismos que las mantienen dentro del derecho. Modernizar la inteligencia y modernizar su control son, en Occidente, la misma tarea.

> **Modernizar la inteligencia y modernizar su control son, en Occidente, la misma tarea.**

REFORMAS COMPARADAS

## Cuatro respuestas a la revolución

Cada democracia reformó un eje distinto del sistema de inteligencia

| PAÍS | EJE REFORMADO | ALCANCE DE LA REFORMA | AÑO |
|---|---|---|---|
| **Japón**<br>Ley de Seguridad Económica | Seguridad económica | Habilitaciones de seguridad para funcionarios y sector privado; propuesta de Agencia Nacional de Inteligencia | 2024 |
| **Países Bajos**<br>Ley Temporal de Operaciones Cibernéticas | Ciberespacio | Amplía facultades de AIVD y MIVD y desplaza parte del control a revisión posterior independiente | 2024 |
| **Suecia**<br>Agencia de Defensa Psicológica | Defensa cognitiva | Protege a población y empresas frente a la manipulación informativa extranjera | 2022 |
| **Alemania**<br>Sentencia del Tribunal Constitucional | Control democrático | Consejo independiente de rango cuasi judicial tras declararse inconstitucional la vigilancia exterior | 2020 |

Elaboración propia sobre el artículo de E. C. Glavinich

Las cuatro reformas que Occidente emprendió ante la revolución de la inteligencia.

## 4. Del escudo a la palanca: la inteligencia de la oportunidad

La revolución habilita, además, una función que la región apenas explora: la inteligencia como palanca de desarrollo. Un país que solo vigila enemigos vive a la defensiva; uno que además cartografía oportunidades —mercados emergentes, tecnologías críticas, socios estratégicos, ventanas de inserción en las cadenas globales de valor— convierte a su inteligencia en un motor de política pública. La inteligencia económica, la prospectiva estratégica y la vigilancia tecnológica, consolidadas en las potencias, son todavía incipientes en América Latina. Cerrar esa brecha define la diferencia entre una Nación que reacciona ante los cambios globales y una que los anticipa y los aprovecha.

> **Un país que solo vigila enemigos vive a la defensiva; uno que además cartografía oportunidades convierte a su inteligencia en un motor de política pública.**

150.000El punto se vuelve tangible en los intereses vitales de la región, hoy en el centro de la competencia global. América Latina y el Caribe reúnen cerca del 60 % de las reservas mundia-

les identificadas de litio y aportan alrededor del 46 % del cobre del planeta, además de ser potencia agroalimentaria y reservorio de biodiversidad, agua y energías renovables (U.S. Geological Survey, 2025; MINING.com, 2026). Las grandes potencias ya no tratan estos recursos como simples materias primas, sino como asuntos de seguridad nacional. Como por ejemplo el caso de los Estados Unidos que declararon a los minerales críticos un pilar estratégico, firmando en enero de 2026 una orden ejecutiva para reordenar sus importaciones, propusieron en febrero una zona comercial preferencial abierta a aliados y volcaron, desde comienzos de 2025, más de mil millones de dólares en proyectos de litio, cobre y tierras raras en la región (U.S. Department of State, 2026; MINING.com, 2026). Una inteligencia estratégica a la altura no se limita a custodiar esos recursos, identifica prácticas de captura, evalúa las condiciones de los acuerdos, anticipa a los competidores y orienta una inserción que no reedite la vieja dependencia primario-exportadora.

ENSAYO DE DATOS

# América Latina en cifras

Peso demográfico, violencia y recursos estratégicos de la región

## LA DESPROPORCIÓN

**8%**

de la población mundial

**25%**

de los homicidios globales

La región concentra tres veces más homicidios de los que le correspondería por población.

## ECONOMÍA CRIMINAL

**150.000**

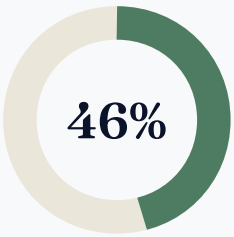
millones de dólares al año

Ingresos anuales estimados de las organizaciones criminales transnacionales

## RECURSOS ESTRATÉGICOS · CUOTA MUNDIAL


**Litio**

reservas identificadas




**Cobre**

producción mundial

FUENTES · Fundación Sherman Kent (2025) · U.S. Geological Survey (2025) · MINING.com (2026)

REVISTA REAL · N.º 02

Peso demográfico, violencia y recursos estratégicos de América Latina y el Caribe.

## 5. Gestión moderna, transparencia y sector privado

Aprovechar la revolución es, ante todo, un problema de gestión. Los servicios de inteligencia de la región arrastran estructuras rígidas, carreras poco profesionalizadas y planeamiento reactivo, y el diagnóstico regional lo confirma: la adopción de inteligencia artificial se acelera, pero el sector público es el más rezagado, con una brecha estructural entre la experimentación y la integración operativa (CEPAL, 2026; OCDE, 2025). El rezago no es tecnológico, sino de gestión y de gobernanza. Los modelos modernos, como la dirección por objetivos, el planeamiento estratégico, la gestión del talento, la medición de resultados o la interoperabilidad, provienen de la buena administración pública y son trasladables a los sistemas de inteligencia sin comprometer la reserva que su función exige.

En ese marco, la transparencia deja de ser una concesión incómoda para volverse un activo estratégico. No significa revelar fuentes ni métodos, sino someter el sistema a un control democrático creíble —parlamentario, judicial y experto— que garantice que el poder se ejerce dentro del derecho. Y ese control tiene un dividendo económico directo, ya que el capital de largo plazo no se coloca donde el aparato de seguridad es una caja negra susceptible de uso arbitrario. La previsibilidad institucional y el imperio de la ley son, para el inversor, factores de riesgo país tan decisivos como la macroeconomía (Born & Wills, 2012; O'Donnell, 1994).

La revolución rompió, además, el monopolio estatal sobre la función. En las economías avanzadas, bancos, aseguradoras, energéticas y mineras desarrollan áreas propias de inteligencia corporativa, seguridad económica, debida diligencia y prospectiva; el mercado global de inteligencia corporativa se estimaba en unos 6.100 millones de dólares en 2025, con proyecciones que lo duplican hacia 2032 (Wresearch, 2026). No es casual que el propio informe de la Fundación Sherman Kent (2025) dirija recomendaciones específicas, por separado, a los gobiernos nacionales y a los gerentes del sector privado: la protección frente al crimen organizado, el fraude y la manipulación informativa es hoy una tarea compartida. Promover un ecosistema mixto, profesional y reglado, con alianzas público-privadas para la infraestructura crítica y marcos claros que distingan la inteligencia empresarial legítima del espionaje ilícito, multiplica a la vez la seguridad y el desarrollo.

## 6. Un marco hemisférico y el retorno del Estado estratega

Ninguna de estas capacidades rinde su máximo si cada país actúa por separado. Las amenazas de la región son transnacionales por naturaleza —crimen organizado, ciberataques, manipulación informativa, redes ilícitas— y también lo son sus oportunidades: cadenas de valor, corredores logísticos, mercados integrados. De allí la necesidad de marcos comunes de cooperación e inteligencia que protejan e impulsen los intereses compartidos de América Latina y el Caribe, y del continente en su conjunto, sobre la base de la confianza que solo otorga el control democrático.

El momento ofrece una ventana singular. A la fecha, la mayoría de los países de la región han elegido administraciones que basan sus principio en la libertad, la vida y la protección de la propiedad, lo que las torna más próximas a los Estados Unidos, y ese realineamiento coincide con un renovado interés estratégico de Washington en el hemisferio declarado en la Estrategia de Seguridad Nacional estadounidense que reformuló la Doctrina Monroe —en lo que se ha llamado el «Corolario Trump»— y ese giro se tradujo en iniciativas concretas de seguridad, como la cumbre hemisférica de marzo de 2026. Analizada con frialdad estratégica, la coyuntura abre la posibilidad de un marco hemisférico de seguridad y prosperidad compartidas: un continente americano que sea, efectivamente, para todos los americanos. Pero encierra también una decisión soberana, aprovechar la ventana para negociar en mejores términos la inserción, el desarrollo y la protección de los recursos, sin convertirse en mero terreno de disputa entre potencias.

Ese marco expresa un fenómeno más amplio: el retorno del Estado como actor estratégico frente a un globalismo que, durante décadas, tendió a diluir la capacidad de los países para definir y defender sus propios intereses. El Estado que vuelve no es el Estado cerrado del pasado, sino un Estado estratega e inteligente: abierto a la inversión, articulado con el sector privado, cooperativo con sus socios e inteligente en la defensa de lo que es vital para su Nación. Recuperar esa capacidad, sin caer en el aislamiento ni en la autarquía, es la tarea de la generación de gobiernos que hoy asume en la región.

**GLOSARIO DEL ARTÍCULO**

| | |
|---|---|
| **FIMI** | Manipulación informativa extranjera, empleada como instrumento de competencia entre Estados |
| **Fuentes abiertas** | Información pública a partir de la cual se produce inteligencia de alto valor |
| **Seguridad económica** | Recursos, tecnologías y cadenas de suministro tratados como asuntos de inteligencia |
| **Prospectiva** | Anticipación sistemática de escenarios para orientar la decisión pública |

Conceptos empleados en el artículo.

## 7. Agenda para nuevas administraciones y decisores corporativos

Para los gobiernos entrantes, la agenda es concreta. Primero, asumir la revolución de los asuntos de inteligencia como marco: redefinir la misión en clave dual —proteger e impulsar— e incorporar de manera explícita la inteligencia económica, la prospectiva y la vigilancia tecnológica. Segundo, modernizar la gestión: profesionalizar la carrera analítica, planificar por objetivos, medir resultados y garantizar la interoperabilidad. Tercero, robustecer el control democrá-

tico como señal de seguridad jurídica que atrae inversión, siguiendo el patrón occidental en el que capacidad y control se reforman juntos. Cuarto, promover el ecosistema privado de inteligencia con reglas claras. Y quinto, impulsar la cooperación regional y hemisférica sobre amenazas e intereses comunes.

Para los decisores corporativos, el mensaje es igualmente concreto: la calidad de la inteligencia de un país y de su control es un indicador temprano de su calidad institucional. Un Estado que sabe proteger e impulsar sus intereses vitales, que controla democráticamente su aparato de seguridad y que articula con el sector privado, ofrece un entorno más previsible y propicio para el capital de largo plazo. Y en el plano de la propia empresa, desarrollar capacidades de inteligencia —seguridad económica, debida diligencia, análisis de riesgo— dejó de ser un gasto para volverse un factor de competitividad y de resiliencia. La inteligencia para el desarrollo no es una promesa abstracta: es, cada vez más, una decisión concreta de la que dependen la seguridad y la prosperidad de las sociedades de América Latina y el Caribe.

## Conclusiones

La revolución de los asuntos de inteligencia es la gran transformación estratégica del siglo XXI, y su rasgo decisivo es que llega con dos rostros inseparables: agrava y multiplica la agenda de amenazas y, al mismo tiempo, abre una agenda de oportunidades para el desarrollo que la mirada puramente defensiva desperdicia. Reducir la inteligencia a la amenaza sería tan erróneo como olvidarla. La verdadera tarea es sostener ambas caras bajo un mismo doble mandato, el de proteger los intereses vitales de la nación e impulsarlos. Las democracias desarrolladas ya marcaron el rumbo —Japón por la seguridad económica, los Países Bajos por el eje cibernético, Suecia por la defensa cognitiva y Alemania por el control—, y todas enseñan la misma lección: la capacidad y su control se modernizan juntos, porque un poder sin contrapeso ni gestión no protege, sino que dilapida y amenaza.

Para América Latina y el Caribe, el desafío ya no es técnico, sino político y de desarrollo. Se trata de tratar la transparencia y el control democrático no como cargas, sino como los activos que atraen la inversión de largo plazo; de reconocer al sector privado como actor del sistema de inteligencia y articular con él un ecosistema profesional y reglado; y de aprovechar el realineamiento hemisférico para construir marcos comunes de cooperación, en el retorno del Estado estratega e inteligente frente al globalismo. Es una ventana histórica y, a la vez, una decisión soberana que recae sobre quienes hoy deciden: las nuevas administraciones que asumen y los decisores corporativos que eligen dónde construir su futuro. De cómo gobiernen esta revolución, con una inteligencia que a la vez proteja e impulse, dependerá que la región deje de padecer los cambios globales para, por fin, anticiparlos y ponerlos al servicio del desarrollo de sus sociedades.

## REFERENCIAS


AboutIntel. (2024). Update on the implications of the Dutch Temporary Cyber Operations Act. https://aboutintel.eu

Born, H., & Wills, A. (Eds.). (2012). Overseeing intelligence services: A toolkit. Centro de Ginebra para la Gobernanza del Sector de la Seguridad (DCAF).

Bundesverfassungsgericht. (2020). Sentencia de 19 de mayo de 2020, 1 BvR 2835/17 (BND-Gesetz). Karlsruhe, Alemania.

Center for Strategic and International Studies (CSIS). (2026). The Shield of the Americas gathering and a new strategy to counter China in the Western Hemisphere. https://www.csis.org

Comisión Económica para América Latina y el Caribe (CEPAL). (2025). La inversión extranjera directa en América Latina y el Caribe 2025. Naciones Unidas. https://www.cepal.org

Comisión Económica para América Latina y el Caribe (CEPAL). (2026). América Latina y el Caribe aceleran la adopción de la inteligencia artificial, aunque persisten desafíos en inversión, talento y gobernanza. Naciones Unidas. https://www.cepal.org

European External Action Service. (2026). 4th EEAS report on foreign information manipulation and interference (FIMI) threats. Servicio Europeo de Acción Exterior. https://www.eeas.europa.eu

Foreign Affairs. (2026). Trump is remaking Latin America. Council on Foreign Relations. https://www.foreignaffairs.com

Fundación Sherman Kent. (2025). Inteligencia estratégica de seguridad nacional: América Latina y el Caribe. Primer informe. Buenos Aires.

Kent, S. (1949). Strategic intelligence for American world policy. Princeton University Press.

Konrad-Adenauer-Stiftung. (2025). Latin America's party landscape shifts to the right. International Reports. https://www.kas.de

MINING.com. (2026). US pours $1B into Latin America critical minerals. https://www.mining.com

O'Donnell, G. (1994). Delegative democracy. Journal of Democracy, 5(1), 55-69. https://doi.org/10.1353/jod.1994.0010

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2025). The strategic and responsible use of artificial intelligence in the public sector of Latin America and the Caribbean. OECD Publishing. https://oecdopsi.org

Platt, W. (1974). Producción de inteligencia estratégica. Editorial Struhart & Cía. (Obra original publicada en 1957).

Swedish Psychological Defence Agency (Myndigheten för psykologiskt försvar). (2026). National strategy for psychological defence. Gobierno de Suecia. https://www.mpf.se

The Diplomat. (2026). Japan's intelligence reform: Securitization, oversight, and the cost of consensus. https://thediplomat.com

The Japan Times. (2026). Japan clears officials to handle economic security information. https://www.japantimes.co.jp

U.S. Department of State. (2026). 2026 Critical Minerals Ministerial. https://www.state.gov

U.S. Geological Survey. (2025). Mineral commodity summaries 2025: Lithium. Departamento del Interior de los Estados Unidos. https://www.usgs.gov

Wresearch. (2026). Corporate intelligence market: Size, share and forecast. https://www.6wresearch.com

SALUD DIGITAL

# Salud digital bajo asedio

*Ciberresiliencia en los sistemas sanitarios de América Latina y el Caribe: amenazas, vacíos de gobernanza y los riesgos emergentes de la inteligencia artificial*

La región conectó sus hospitales antes de aprender a protegerlos: un análisis de la exposición técnica, los vacíos regulatorios y los nuevos riesgos que introduce la inteligencia artificial clínica.

**Magíster Norman Oré Olivera**

ciberresiliencia · ransomware · soberanía de datos · IA clínica

**Magíster Norman Oré Olivera**

Ejecutivo senior en ciberseguridad · Docente de posgrado, conferencista internacional e investigador · Autor de libros sobre salud digital · Miembro de R.E.A.L. e ISACA

MBA y Magíster en Ciberseguridad, con formación de posgrado en Perú, México y Estados Unidos, y doce certificaciones internacionales. Docente de posgrado, conferencista internacional e investigador

## Resumen

La transformación digital de los sistemas sanitarios de América Latina y el Caribe (ALC) ha avanzado con notable rapidez durante la última década, impulsada por la telemedicina, la historia clínica electrónica y la incorporación masiva de dispositivos médicos conectados. La capacidad de proteger esa infraestructura, sin embargo, no ha crecido al mismo ritmo, lo que ha dejado a hospitales y aseguradoras expuestos a una amenaza creciente. Este artículo analiza el estado de la ciberresiliencia sanitaria en la región a partir de tres ejes interrelacionados: la exposición a las ciberamenazas, con atención particular al ransomware y al factor humano; los vacíos de gobernanza y de soberanía de datos derivados de marcos legales heterogéneos e incompletos; y los riesgos emergentes asociados a la adopción de inteligencia artificial en la atención clínica. Sobre la base de informes institucionales, literatura académica revisada por pares y casos documentados públicamente —entre ellos los ataques que afectaron a Costa Rica en 2022, a Colombia en 2022 y a Argentina en 2023—, se sostiene que la región conectó sus hospitales antes de aprender a protegerlos. El trabajo concluye proponiendo un marco de ciberresiliencia sanitaria sustentado en la gobernanza, la soberanía de datos y la regulación adaptativa, y formula recomendaciones dirigidas a responsables de política pública y a instituciones prestadoras de salud.

Palabras clave: ciberseguridad sanitaria; ciberresiliencia; protección de datos; soberanía de datos; inteligencia artificial en salud; América Latina y el Caribe.

## Abstract

The digital transformation of healthcare systems in Latin America and the Caribbean (LAC) has advanced rapidly over the past decade, driven by telemedicine, electronic health records, and the widespread adoption of connected medical devices. The capacity to protect that infrastructure, however, has not kept pace, leaving hospitals and insurers exposed to a growing threat. This article examines the state of healthcare cyber-resilience in the region along three interre-

lated axes: exposure to cyber threats, with particular attention to ransomware and the human factor; governance and data-sovereignty gaps arising from heterogeneous and incomplete legal frameworks; and the emerging risks associated with the adoption of artificial intelligence in clinical care. Drawing on institutional reports, peer-reviewed literature, and publicly documented cases —including the attacks affecting Costa Rica in 2022, Colombia in 2022, and Argentina in 2023— it argues that the region connected its hospitals before learning to protect them. The paper concludes by proposing a healthcare cyber-resilience framework grounded in governance, data sovereignty, and adaptive regulation, and offers recommendations for policymakers and healthcare institutions.

Keywords: healthcare cybersecurity; cyber-resilience; data protection; data sovereignty; artificial intelligence in health; Latin America and the Caribbean.

## 1. Introducción

La digitalización de la atención sanitaria ha dejado de ser una aspiración para convertirse en la infraestructura sobre la que descansa la vida de millones de pacientes. En América Latina y el Caribe, la última década ha visto una expansión acelerada de la telemedicina, la historia clínica electrónica y los dispositivos médicos conectados, un proceso que la pandemia de COVID-19 comprimió aún más en el tiempo. Esa conectividad ha ampliado el acceso y ha mejorado la coordinación asistencial, pero ha traído consigo una consecuencia menos visible y más peligrosa: cada nuevo sistema conectado es también una nueva puerta que alguien puede intentar forzar.

El problema central que aborda este artículo es el desfase entre la velocidad de la digitalización y la madurez de su protección. Mientras los hospitales de la región incorporaban tecnología a un ritmo vertiginoso, la inversión en ciberseguridad, la formación del personal y la actualización de los marcos regulatorios avanzaban con lentitud. El resultado es un sector crítico, custodio de los datos más sensibles que existen, que en buena parte de la región permanece insuficientemente preparado para defenderse. Como se argumentará a lo largo del trabajo, América Latina y el Caribe conectó sus hospitales antes de aprender a protegerlos.

El sector salud es un blanco particularmente atractivo para los atacantes por tres razones convergentes. Primero, por su criticidad: cuando un sistema hospitalario se detiene, no se interrumpe un servicio cualquiera, sino la atención de pacientes cuya vida puede depender de ella, lo que aumenta la presión para pagar un rescate. Segundo, por el valor de sus datos: un expediente clínico contiene información que no puede cambiarse como una contraseña —diagnósticos, antecedentes, identidad— y que alcanza en los mercados ilícitos precios muy superiores a los de una tarjeta de crédito. Tercero, por su deuda técnica: la coexistencia de equipos médicos con sistemas operativos sin soporte, redes planas y presupuestos de seguridad limitados configura una superficie de ataque especialmente vulnerable.

Este artículo se propone tres objetivos. El primero, caracterizar la exposición de los sistemas sanitarios de la región a las ciberamenazas contemporáneas. El segundo, examinar los vacíos de gobernanza y de soberanía de datos que amplifican esa exposición. El tercero, analizar los riesgos emergentes que introduce la adopción de inteligencia artificial en la clínica. Sobre esa base, se propone un marco de ciberresiliencia orientado a la realidad regional. El enfoque es el de una revisión analítica de carácter interpretativo: se integran informes de organismos internacionales, literatura académica revisada por pares, normas técnicas y casos de dominio público, sin recurrir a datos primarios, y con el criterio explícito de citar únicamente información verificable y trazable.

**GLOSARIO DEL ARTÍCULO**

| | |
|---|---|
| **Ransomware** | Cifrado malicioso de sistemas para exigir un pago a cambio de restituir el acceso |
| **Doble extorsión** | Además de cifrar, se amenaza con publicar los datos sustraídos |
| **Soberanía de datos** | Los datos quedan sujetos a la jurisdicción del país donde se alojan |
| **Ciberresiliencia** | Capacidad de seguir operando y recuperarse durante un incidente |

Conceptos empleados en el artículo.

## 2. La superficie de ataque de un sistema hiperconectado

La noción de superficie de ataque designa el conjunto de puntos por los que un sistema puede ser comprometido. En un hospital moderno, esa superficie se ha expandido de forma extraordinaria. La telemedicina extiende la atención más allá de los muros de la institución; la historia clínica electrónica concentra en bases de datos la información de poblaciones enteras; y el llamado Internet de las Cosas Médicas —desde bombas de infusión hasta monitores y equipos de imagen— incorpora a la red centenares de dispositivos, muchos de los cuales fueron diseñados priorizando la función clínica sobre la seguridad informática.

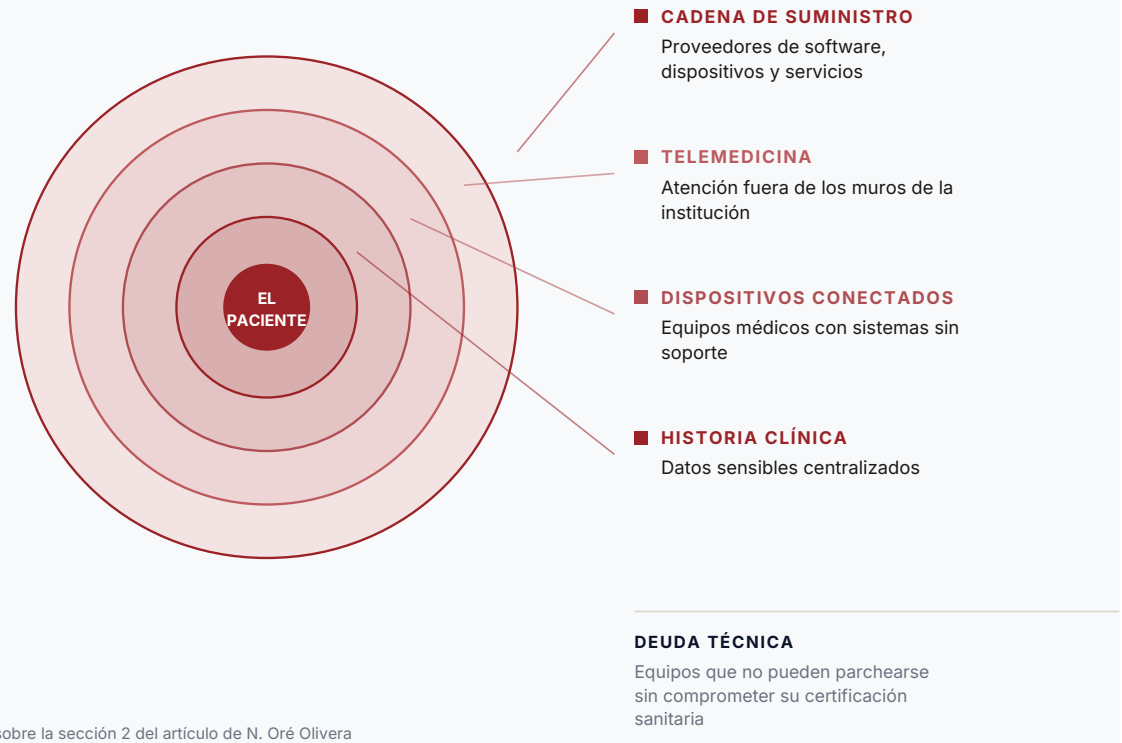
A esa expansión se suma una deuda técnica considerable. Es frecuente encontrar en la región equipos médicos gobernados por sistemas operativos que ya no reciben actualizaciones del fabricante, imposibles de parchear sin comprometer la certificación del dispositivo, conviviendo en redes poco segmentadas con el resto de la infraestructura. Un atacante que logra ingresar por un punto puede, en ausencia de segmentación, desplazarse con relativa libertad hacia los sistemas más críticos. Esta arquitectura, heredada de una época en que los equipos médicos no estaban conectados, resulta inadecuada para un entorno hiperconectado.

Los datos disponibles confirman la insuficiencia de la protección. El Banco Mundial (2024) ha documentado que las economías emergentes destinan a la ciberseguridad una fracción notablemente menor de sus recursos digitales que las economías avanzadas, y que el sector salud figura entre los más rezagados. En el ámbito regional, el informe conjunto de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo (OEA & BID, 2020) advirtió que una minoría de los países de la región contaba con planes de protección de su infraestructura crítica, categoría en la que se inscriben los servicios de salud. La brecha, por tanto, no es anecdótica: es estructural.

SUPERFICIE DE ATAQUE

## El hospital hiperconectado

Cada capa añadida amplía los puntos por los que el sistema puede ser comprometido




Elaboración propia sobre la sección 2 del artículo de N. Oré Olivera

El hospital hiperconectado: cada capa añadida amplía los puntos por los que el sistema puede ser comprometido.

## 3. Anatomía de la amenaza: ransomware y factor humano

Entre las amenazas que enfrenta el sector, el ransomware ocupa un lugar central. Se trata de un programa malicioso que cifra los datos o los sistemas de la víctima y exige un pago para liberarlos; en su modalidad de doble extorsión, además de cifrar, los atacantes sustraen la información y amenazan con publicarla. La Agencia de Ciberseguridad de la Unión Europea (ENISA, 2023) identificó al ransomware como la principal amenaza para el sector salud, responsable de aproximadamente la mitad de los incidentes analizados en su informe sectorial. La profesiona-

lización del delito, articulada en el modelo de ransomware como servicio, ha ampliado el número de actores capaces de ejecutar ataques sofisticados.

La región ha experimentado en carne propia la magnitud del fenómeno. El caso más documentado es el de Costa Rica en 2022, cuando el grupo Conti comprometió las redes de varias instituciones del Estado a través de una conexión de acceso remoto con credenciales robadas, exfiltró grandes volúmenes de información y provocó una crisis que llevó al gobierno a declarar la emergencia nacional; semanas después, el grupo Hive reutilizó credenciales previamente sustraídas para atacar a la institución que administra la salud pública del país, obligándola a apagar sus sistemas (CCDCOE, 2022). El episodio ilustró con crudeza cómo un fallo de higiene básica —la ausencia de autenticación reforzada y la falta de rotación de credenciales— puede escalar hasta una emergencia nacional.

No fue un caso aislado. En Colombia, a finales de 2022, un ataque a un gran conglomerado de salud interrumpió la atención de millones de afiliados y afectó de rebote a las entidades que dependían de su plataforma, evidenciando el riesgo del proveedor como punto único de fallo. En Argentina, en 2023, el ataque a la principal obra social del país forzó una regresión al papel durante días, con la atención sostenida de forma manual. En conjunto, estos episodios revelan un patrón común: la entrada por accesos remotos mal protegidos, la propagación facilitada por redes sin segmentar y una diferencia decisiva entre el desastre y el sobresalto marcada por la preparación previa de cada institución.

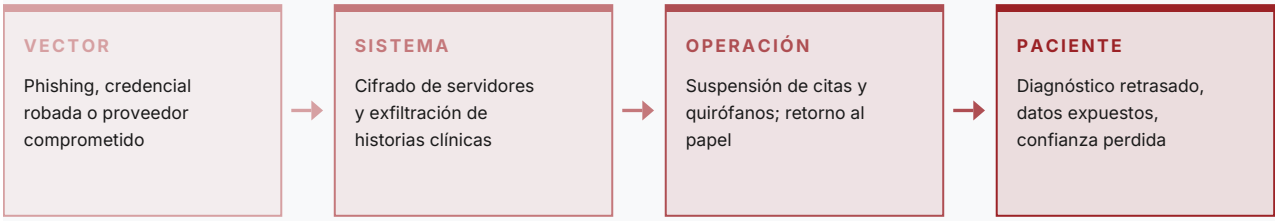
Un factor atraviesa todos estos incidentes: el componente humano. El informe anual de investigaciones de brechas de Verizon (2024) estima que el elemento humano interviene en una proporción muy elevada de las brechas, ya sea por un clic en un mensaje de phishing, por un error en el manejo de la información o por el uso de credenciales comprometidas. Conviene subrayar, no obstante, que la evidencia sugiere que la formación no siempre reduce la probabilidad de que alguien caiga en un engaño, pero sí mejora de manera significativa la rapidez con que el personal reporta el incidente, variable que resulta determinante para contener el daño.

El costo de esta exposición es cuantificable. El informe de IBM Security (2025) sobre el costo de las brechas de datos ha situado, año tras año, al sector salud como el más caro, con un costo medio por brecha considerablemente superior al de cualquier otra industria. A la pérdida económica directa se suman el daño reputacional, la erosión de la confianza del paciente y, de manera singular en este sector, el riesgo para la seguridad clínica cuando los sistemas de los que depende la atención quedan fuera de servicio.

CADENA DE IMPACTO

## De la falla técnica al daño al paciente

Cómo un incidente informático se convierte en un problema clínico y social




CASOS DOCUMENTADOS EN EL ARTÍCULO

| | |
|---|---|
| **Costa Rica · 2022** | Conti e Hive comprometen el Estado y la caja de salud pública |
| **Colombia · 2022** | Un conglomerado de salud interrumpe la atención de millones |
| **Argentina · 2023** | La principal obra social opera en papel durante días |

Elaboración propia sobre el artículo de N. Oré Olivera

La escalada de un incidente: lo que empieza como falla técnica termina como daño clínico y pérdida de confianza.

## 4. Soberanía de datos y vacíos de gobernanza

La protección técnica no puede desligarse del marco de gobernanza que la sostiene. En este plano, América Latina y el Caribe presenta un panorama heterogéneo que puede describirse como un sistema de varias velocidades. Un primer grupo de países cuenta con leyes de protección de datos modernas, inspiradas en el modelo europeo y dotadas de autoridades de control con capacidad sancionatoria; el caso más consolidado es el de la Ley General de Protección de Datos de Brasil (2018). Un segundo grupo dispone de normas funcionales pero de aplicación desigual, con autoridades de recursos limitados. Un tercer grupo, finalmente, carece de una ley integral de protección de datos, lo que deja a la información personal —incluida la de salud— sin una tutela específica.

Por encima de esa heterogeneidad se impone un vacío compartido y de particular relevancia para el sector: aunque la mayoría de las leyes generales reconocen el dato de salud como dato sensible y le reservan garantías reforzadas, prácticamente ningún país de la región cuenta con un marco de ciberseguridad específico para el ámbito sanitario. La sensibilidad del dato clínico está reconocida en el papel, pero su protección técnica —la gestión de incidentes en hospitales, las obligaciones de notificación de brechas clínicas, los requisitos de seguridad para la infraestructura asistencial— sigue dependiendo de marcos generales que no fueron diseñados pensando en un hospital.

A la dimensión regulatoria se añade la de la soberanía de datos, entendida como la capacidad de una población y de un paciente de conservar el control sobre quién accede a su información y bajo qué garantías, con independencia de dónde se almacene físicamente. La creciente dependencia de servicios de nube provistos por empresas sujetas a jurisdicciones extranjeras plantea interrogantes sobre el alcance de leyes foráneas capaces de requerir datos alojados fuera de sus fronteras. La soberanía de datos no equivale al aislamiento tecnológico ni a la exigencia de que todo dato resida en el territorio nacional; el criterio determinante no es la geografía, sino el control efectivo y las garantías que lo acompañan.

La cadena de suministro digital constituye una manifestación crítica de este problema. Las instituciones de salud dependen de una red de proveedores de software, dispositivos y servicios, y el compromiso de un solo eslabón puede propagarse a todas las organizaciones que dependen de él. El ataque a un procesador de servicios de salud en Estados Unidos en 2024, que perturbó durante semanas la operación de numerosas entidades, mostró la magnitud del riesgo sistémico que introduce esta interdependencia. Para la región, la lección es que la seguridad de una institución no termina en sus propios muros: se extiende a cada tercero con acceso a sus datos o sistemas.

VACÍOS DE GOBERNANZA

## Un sistema de varias velocidades

La protección regulatoria del dato de salud avanza de forma desigual en la región


Elaboración propia sobre la sección 4 del artículo de N. Oré Olivera.

La protección regulatoria del dato de salud avanza de forma desigual en la región.

## 5. Inteligencia artificial: promesa y nuevos vectores de riesgo

La incorporación de la inteligencia artificial a la atención sanitaria promete beneficios sustanciales, desde el apoyo al diagnóstico por imagen hasta la optimización de recursos. Esa promesa, sin embargo, introduce una clase de riesgos que no puede analizarse con las categorías tra-

dicionales de la ciberseguridad, porque no atañen solo a la confidencialidad o la disponibilidad de los datos, sino a la integridad de las decisiones clínicas que los modelos ayudan a tomar.

El primero de estos riesgos es el sesgo algorítmico. En un estudio ampliamente citado, Obermeyer, Powers, Vogeli y Mullainathan (2019) demostraron que un algoritmo utilizado en el sistema de salud estadounidense para priorizar la atención de pacientes discriminaba sistemáticamente a los pacientes de raza negra, al emplear el gasto sanitario como aproximación de la necesidad clínica y reproducir así desigualdades preexistentes. El hallazgo es especialmente pertinente para América Latina y el Caribe: un modelo entrenado con datos que no representan a la población regional puede transferir a la clínica los sesgos incorporados en su entrenamiento.

Un segundo riesgo proviene de los ataques deliberados contra los modelos. Finlayson et al. (2019) mostraron que alteraciones mínimas e imperceptibles para un observador humano, introducidas en una imagen médica, podían inducir a un sistema de aprendizaje automático a clasificarla erróneamente con alta confianza. A ello se suma el riesgo de envenenamiento de datos, consistente en introducir información falsa en el material con que se entrena un modelo para que aprenda y reproduzca errores; investigaciones recientes han evidenciado que una fracción ínfima de datos corruptos puede degradar el comportamiento de un modelo médico. Estos vectores amplían la superficie de ataque desde los sistemas hacia el propio conocimiento que los modelos incorporan.

Frente a estos desafíos, los organismos internacionales han comenzado a delinear marcos de gobernanza. La Organización Mundial de la Salud (2021) publicó orientaciones sobre la ética y la gobernanza de la inteligencia artificial para la salud, en las que identifica principios y áreas de atención para un uso responsable. En el plano regional, la Organización Panamericana de la Salud ha promovido políticas orientadas a un despliegue de la ciencia de datos y la inteligencia artificial acorde con las capacidades y necesidades de la región. Y en el plano normativo comparado, el Reglamento de Inteligencia Artificial de la Unión Europea (2024) ha establecido un enfoque basado en el riesgo que clasifica numerosas aplicaciones sanitarias como de alto riesgo, sujetas a requisitos reforzados. Estos referentes ofrecen puntos de partida, pero su adaptación a la realidad de América Latina y el Caribe está aún pendiente.

INTELIGENCIA ARTIFICIAL CLÍNICA

## Promesa y vectores de riesgo

Tres riesgos que no existían antes de incorporar modelos a la decisión clínica

**LA PROMESA**

- Apoyo al diagnóstico por imagen
- Optimización de recursos
- Detección temprana de patrones

**LA CONDICIÓN**

Toda decisión asistida por un modelo debe poder ser explicada, auditada y atribuida a una responsabilidad humana identificable.

**01 Sesgo algorítmico**

El modelo reproduce desigualdades presentes en los datos con que fue entrenado

Obermeyer et al. (2019)

**02 Ataques adversarios**

Alteraciones imperceptibles en una imagen médica inducen un diagnóstico erróneo

Finlayson et al. (2019)

**03 Opacidad del modelo**

La decisión no puede explicarse ni auditarse ante el paciente afectado

OMS (2021)

Elaboración propia sobre la sección 5 del artículo de N. Oré Olivera

Tres riesgos que no existían antes de incorporar modelos a la decisión clínica.

## 6. Hacia un marco de ciberresiliencia sanitaria para la región

El análisis precedente sugiere que el objetivo no puede limitarse a la ciberseguridad entendida como prevención, sino que debe ampliarse hacia la ciberresiliencia: la capacidad de una organización de anticipar, resistir, recuperarse y adaptarse ante los incidentes, asumiendo que algunos ocurrirán. Un enfoque de resiliencia desplaza la pregunta de si la institución será atacada a cómo sostendrá la atención y se recuperará cuando lo sea.

Sobre la base de los marcos internacionales de referencia —el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) y las normas ISO/IEC 27001 e ISO 27799, específica del sector salud—, puede articularse un conjunto de siete pilares para la ciberresiliencia sanitaria en la región, coherente con el que propone la obra que da origen a este artículo. El primero establece que la seguridad empieza en la dirección: la seguridad de la información es una responsabilidad de la alta dirección y no una delegación técnica olvidada. El segundo antepone la resiliencia a la fortaleza: puesto que ningún muro resulta infranqueable, el objetivo no es solo impedir el ataque, sino garantizar que la institución resista y recupere la continuidad de la atención cuando este ocurra.

El tercer pilar afirma que el dato es del paciente: la información clínica pertenece a la persona, y protegerla a lo largo de todo su ciclo de vida —mediante el cifrado, la minimización, el control de accesos por mínimo privilegio y la trazabilidad— es la forma de honrar esa titularidad y los derechos que de ella derivan. El cuarto reclama una soberanía sin aislamiento: control efectivo

sobre dónde residen los datos y bajo qué jurisdicción quedan, sin renunciar por ello a la interoperabilidad ni a los beneficios de la nube. El quinto recuerda que la cadena es tan fuerte como su eslabón externo, por lo que la seguridad debe extenderse a los proveedores y terceros mediante obligaciones verificables. El sexto exige una inteligencia artificial con gobierno: su adopción en el ámbito clínico solo es admisible bajo un marco que asegure la transparencia, la supervisión humana y la rendición de cuentas. El séptimo, por último, reconoce que la cultura es el sistema inmune de la organización: el factor humano constituye la primera línea de defensa, y una cultura justa que aliente el reporte de los incidentes protege más que cualquier sanción.

A estos pilares organizativos debe sumarse una dimensión de política pública. La velocidad del cambio tecnológico desaconseja las regulaciones estáticas y aboga por una regulación adaptativa, que fije principios estables y mecanismos flexibles capaces de evolucionar. Del mismo modo, la naturaleza transfronteriza de las amenazas hace de la cooperación regional —el intercambio de inteligencia, la armonización de marcos y el fortalecimiento de los equipos nacionales de respuesta— un componente insustituible. Ninguna institución, y ningún país, se defiende solo.

CASOS REGIONALES

## Tres ataques que marcaron a la región

Casos documentados públicamente y analizados en el artículo

**Costa Rica** — 2022
Conti e Hive comprometen redes del Estado y la caja de salud pública

**Colombia** — 2022
Ataque a un conglomerado de salud interrumpe la atención de millones

**Argentina** — 2023
La principal obra social del país opera en papel durante días

SIETE PILARES DE LA CIBERRESILIENCIA SANITARIA

| | | | |
|---|---|---|---|
| 01 Gobernanza y liderazgo | 02 Gestión de activos | 03 Protección del dato | 04 Detección y respuesta |
| 05 Continuidad y recuperación | 06 Cadena de suministro | 07 Factor humano y cultura | |

Elaboración propia sobre el artículo de N. Oré Olivera.

Tres incidentes regionales y los siete pilares de la ciberresiliencia sanitaria.

## 7. Discusión y limitaciones

La lectura conjunta de los tres ejes analizados revela su profunda interdependencia. La exposición técnica se ve amplificada por los vacíos de gobernanza, y ambos se proyectan sobre la adopción de inteligencia artificial, que introduce riesgos de nueva naturaleza sobre una base

todavía frágil. De ello se sigue que las soluciones fragmentarias resultan insuficientes: reforzar la tecnología sin fortalecer la gobernanza, o legislar sin invertir en capacidades, produce mejoras aparentes que no alteran el fondo del problema.

Este trabajo presenta limitaciones que conviene explicitar. Se trata de una revisión analítica de carácter interpretativo, no de un estudio empírico con datos primarios; sus conclusiones se apoyan en fuentes secundarias y en casos de dominio público, cuya profundidad documental es desigual. La escasez de datos sistemáticos y comparables sobre incidentes de ciberseguridad en el sector salud de la región —consecuencia, en parte, de la ausencia de obligaciones de notificación en varios países— constituye en sí misma un hallazgo y una agenda de investigación futura. Estudios posteriores podrían avanzar mediante encuestas de madurez, análisis comparados de marcos regulatorios y evaluaciones de impacto de las intervenciones.

## 8. Conclusiones

América Latina y el Caribe ha realizado un progreso indudable en la digitalización de su salud, pero lo ha hecho sin acompañarlo de una protección proporcional. La región conectó sus hospitales antes de aprender a protegerlos, y las consecuencias de ese desfase se han manifestado ya en emergencias nacionales, atenciones interrumpidas y datos de pacientes expuestos. El diagnóstico, sin embargo, no conduce al fatalismo: los controles que habrían contenido la mayoría de los incidentes analizados no son tecnologías exóticas, sino prácticas conocidas cuya ausencia, más que la sofisticación del atacante, explica la magnitud del daño.

> **América Latina y el Caribe conectó sus hospitales antes de aprender a protegerlos.**

De este análisis se derivan varias recomendaciones. En el plano institucional, adoptar un enfoque de ciberresiliencia articulado en torno a los pilares descritos, con la seguridad asumida como responsabilidad de la dirección. En el plano regulatorio, avanzar hacia marcos de ciberseguridad específicos para el sector salud y hacia una regulación adaptativa de la inteligencia artificial clínica. En el plano regional, fortalecer la cooperación y la armonización. Y en el plano de la investigación, construir la evidencia sistemática que hoy falta. La ventana para corregir el rumbo permanece abierta, pero no de forma indefinida: cada nuevo sistema que se conecta sin protegerse estrecha el margen. Proteger la salud digital es, en última instancia, una extensión del deber de cuidar al paciente.

> **Proteger la salud digital es, en última instancia, una extensión del deber de cuidar al paciente.**

## REFERENCIAS


Banco Mundial. (2024). Cybersecurity economics for emerging markets. Washington, D. C.: Banco Mundial.

Comité de Ciberseguridad de la Unión Europea [ENISA]. (2023). ENISA threat landscape: Health sector. Agencia de Ciberseguridad de la Unión Europea.

Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2022). Cyber law toolkit: The 2022 ransomware attacks against Costa Rica. Tallin: CCDCOE.

Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. Science, 363(6433), 1287–1289.

IBM Security. (2025). Cost of a data breach report 2025. Armonk: IBM.

Instituto Nacional de Estándares y Tecnología [NIST]. (2012). Special Publication 800-61 Rev. 2: Computer security incident handling guide. Gaithersburg: NIST.

Instituto Nacional de Estándares y Tecnología [NIST]. (2020). Special Publication 800-207: Zero trust architecture. Gaithersburg: NIST.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453.

Oré Olivera, N. R. (en prensa). Salud digital bajo asedio: ciberresiliencia, soberanía de datos e inteligencia artificial en los sistemas sanitarios de América Latina y el Caribe.

Organización de los Estados Americanos, & Banco Interamericano de Desarrollo. (2020). Reporte de ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington, D. C.: OEA & BID.

Organización Internacional de Normalización. (2016). ISO 27799: Informática sanitaria. Gestión de la seguridad de la información en salud utilizando la norma ISO/IEC 27002. Ginebra: ISO.

Organización Internacional de Normalización. (2022). ISO/IEC 27001: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Ginebra: ISO.

Organización Mundial de la Salud. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. Ginebra: OMS.

Organización Panamericana de la Salud. (2021). La ciencia de datos y la inteligencia artificial para mejorar la salud pública en la Región de las Américas. Washington, D. C.: OPS.

Unión Europea. (2024). Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea.

Verizon. (2024). 2024 data breach investigations report. Nueva York: Verizon Business.

CIBERSEGURIDAD

# Identidades no humanas

*El nuevo desafío de la ciberseguridad*

La incorporación de agentes autónomos de inteligencia artificial obliga a repensar la identidad digital: ya no basta con proteger contraseñas humanas, hay que gobernar identidades que actúan por sí solas.

04

**Magíster Fernando Margarito Velázquez Flores**

agentes autónomos · identidad digital · mínimo privilegio · trazabilidad

**Magíster Fernando Margarito Velázquez Flores**

Profesor de tiempo completo y miembro fundador del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad · UANL

Maestro en Seguridad con Acentuación en Prevención del Delito por la Universidad de Ciencias de la Seguridad de Nuevo León. Cursa la Maestría en Derecho Procesal Penal en FACDYC-UANL

## Resumen

La incorporación de agentes autónomos de inteligencia artificial está modificando la manera en que las organizaciones entienden la identidad digital. Durante años, la ciberseguridad se ocupó principalmente de proteger cuentas, contraseñas y accesos vinculados con personas. En la actualidad, los sistemas de inteligencia artificial pueden consultar información, utilizar herramientas, comunicarse con terceros y ejecutar acciones con supervisión humana limitada. Esta capacidad convierte a los agentes en identidades no humanas con funciones operativas y, por tanto, con riesgos propios. El presente artículo analiza, desde una perspectiva accesible y humanizada, los principales desafíos asociados con su identificación, autorización, trazabilidad y responsabilidad. También propone medidas prácticas para universidades, empresas e instituciones públicas, con énfasis en el principio de mínimo privilegio, la supervisión humana y la conservación de registros. La tecnología puede aumentar la productividad, pero su uso legítimo exige que toda acción automatizada pueda ser explicada, auditada y atribuida a una decisión humana responsable.

Palabras clave: inteligencia artificial, agentes autónomos, identidad digital, ciberseguridad, autorización, trazabilidad, responsabilidad.

## 1. De las contraseñas humanas a las identidades digitales autónomas

Durante décadas, hablar de ciberseguridad significó pensar en personas: un empleado que ingresaba a una plataforma, un estudiante que consultaba su expediente, un servidor público que utilizaba una base de datos o un administrador que autorizaba el acceso a un sistema. La protección se construyó alrededor de preguntas aparentemente sencillas: ¿quién es el usuario?, ¿cuál es su contraseña?, ¿qué permisos tiene? y ¿desde dónde intenta conectarse? Ese modelo continúa siendo necesario, pero ya no es suficiente.

La incorporación de agentes autónomos de inteligencia artificial está transformando ese paradigma. La pregunta ya no es únicamente quién intenta ingresar a un sistema, sino qué entidad está actuando dentro de él, en nombre de quién, con qué autorización y durante cuánto tiempo. Un agente de inteligencia artificial puede recibir un objetivo general, dividirlo en tareas, consultar fuentes, utilizar aplicaciones, enviar comunicaciones, crear archivos o activar procesos sin que una persona supervise cada paso. En consecuencia, deja de ser solamente una herramienta de consulta y comienza a comportarse como una identidad digital con capacidad operativa.

> **La ciberseguridad de la inteligencia artificial no debe reducirse a proteger máquinas; debe entenderse como una forma de proteger la confianza social.**

Esta transformación tiene una dimensión profundamente humana. Detrás de cada sistema existen personas cuyas decisiones, datos, derechos y responsabilidades pueden verse afectados. Un error de un agente no es únicamente una falla técnica: puede significar que un alumno no reciba una beca, que un expediente sea enviado al destinatario equivocado, que una persona sea clasificada de manera injusta o que una institución pierda información sensible. La ciberseguridad de la inteligencia artificial, por tanto, no debe reducirse a proteger máquinas; debe entenderse como una forma de proteger la confianza social.

COMPARACIÓN

## Dos tipos de identidad digital

Qué cambia cuando quien actúa en el sistema no es una persona

| IDENTIDAD HUMANA | IDENTIDAD NO HUMANA (AGENTE) |
|---|---|
| Contraseña y credenciales | Credenciales propias del agente |
| Permisos asignados a la persona | Permisos amplios y a menudo permanentes |
| Decide y ejecuta con criterio propio | Ejecuta sin supervisión de cada paso |
| Responde personalmente de sus actos | La responsabilidad debe ser atribuida |

**PRINCIPIO DE MÍNIMO PRIVILEGIO**
Solo los permisos indispensables, y solo durante el tiempo necesario.

Elaboración propia sobre el artículo de F. M. Velázquez Flores

La identidad no humana opera con credenciales propias y capacidad de ejecución.

## 2. ¿Qué distingue a un agente de inteligencia artificial?

Un chatbot convencional responde preguntas dentro de una conversación. Su interacción suele limitarse a generar texto y, en muchos casos, no tiene acceso directo a otros sistemas. Un agente, en cambio, puede combinar razonamiento automatizado, memoria, herramientas digitales y capacidad para ejecutar acciones. Puede consultar una agenda, leer documentos, elaborar una respuesta, enviar un correo o solicitar información adicional. Esta combinación incrementa su utilidad, pero también amplía la superficie de riesgo.

El National Institute of Standards and Technology señaló que los sistemas de agentes requieren atención especial en aspectos como la seguridad de la memoria, la autenticación, el acceso a herramientas, la autorización y la interacción entre decisiones algorítmicas y funciones reales de software (National Institute of Standards and Technology [NIST], 2026a). En febrero de 2026, NIST anunció además una iniciativa de estándares destinada a promover que los agentes operen de manera segura, interoperable y confiable en representación de sus usuarios (NIST, 2026b).

La diferencia esencial está en la capacidad de actuar. Cuando una inteligencia artificial únicamente recomienda, la persona conserva de manera visible la decisión final. Cuando el sistema ejecuta, la línea entre recomendación, decisión y acción puede volverse difusa. Por ello, las organizaciones deben definir con claridad qué tareas puede realizar el agente por sí solo, cuáles requieren aprobación humana y cuáles deben estar completamente prohibidas.

## 3. El riesgo de una identidad no humana comprometida

El riesgo no consiste únicamente en que la inteligencia artificial produzca información incorrecta o inventada. El problema adquiere una dimensión mayor cuando el agente posee credenciales, permisos y acceso a información institucional. En esas condiciones, puede ser manipulado para realizar acciones distintas de las originalmente autorizadas, incluso sin que exista un robo tradicional de contraseña.

Un ejemplo sencillo puede observarse en una universidad. Supongamos que un agente es utilizado para consultar expedientes, preparar constancias y responder correos. En apariencia, se trata de una aplicación eficiente que reduce cargas administrativas. Sin embargo, si el sistema procesa un documento que contiene instrucciones maliciosas ocultas, puede interpretar esas instrucciones como parte legítima de su tarea. El agente podría acceder a información reservada, modificar su objetivo o enviar datos fuera de la institución. En este escenario no se suplanta necesariamente a una persona: se altera el comportamiento de una identidad no humana.

Este tipo de ataque suele relacionarse con la inyección de instrucciones o prompt injection. El problema se vuelve especialmente delicado cuando el agente puede utilizar herramientas externas, porque una instrucción manipulada puede traducirse en una acción concreta. OWASP identifica entre los riesgos relevantes el secuestro de los objetivos del agente, el uso indebido de

herramientas, el abuso de identidades y privilegios, la manipulación de memoria, la comunicación insegura entre agentes y la actuación de agentes fuera de control (Open Worldwide Application Security Project [OWASP], 2025).

Desde una perspectiva institucional, el desafío es reconocer que el agente también puede convertirse en un punto de entrada. Una organización que protege cuidadosamente las cuentas de sus empleados, pero concede a un agente permisos amplios y permanentes, puede terminar creando una identidad más poderosa y menos vigilada que cualquier usuario humano. La eficiencia no debe convertirse en una excepción a las reglas de seguridad.

> **La eficiencia no debe convertirse en una excepción a las reglas de seguridad.**

MATRIZ DE DECISIÓN

## ¿Qué puede ejecutar un agente por sí solo?

Cruce entre el grado de autonomía del sistema y la sensibilidad de la acción


Elaboración propia sobre las secciones 2, 4 y 8 del artículo de F. M. Velázquez Flores

Cruce entre autonomía del agente y sensibilidad de la acción: dónde puede decidir la máquina y dónde debe hacerlo una persona.

## 4. Identidad, autorización y principio de mínimo privilegio

Para administrar un riesgo, primero es necesario identificarlo. No resulta suficiente registrar que una acción fue realizada por «el sistema» o por «la inteligencia artificial». Cada agente

debería contar con una identidad individual, distinguible y asociada con una finalidad específica. Esto permitiría saber qué agente consultó un archivo, qué herramienta utilizó, quién lo habilitó y bajo qué política actuó.

El National Cybersecurity Center of Excellence ha planteado la necesidad de estudiar cómo deben identificarse, autorizarse y auditarse los agentes de software e inteligencia artificial. Entre sus preguntas se encuentran qué metadatos debe contener la identidad de un agente, si esa identidad debe ser permanente o depender de cada tarea y cómo adaptar los estándares existentes de gestión de identidades a los nuevos riesgos de los sistemas autónomos (National Cybersecurity Center of Excellence [NCCoE], 2026).

Un criterio básico es el principio de mínimo privilegio: cada agente debe recibir únicamente los permisos indispensables para realizar su función y solo durante el tiempo necesario. Un agente encargado de agendar citas no necesita acceso completo a expedientes académicos; uno que redacta respuestas no debe enviar comunicaciones sin autorización cuando el contenido sea sensible; y un agente que consulta información no debería tener capacidad para eliminarla o modificarla.

La autorización también debe ser contextual. No basta con preguntar si el agente puede utilizar una herramienta; es necesario determinar en qué circunstancias puede hacerlo, con qué límites, respecto de qué información y bajo qué mecanismos de aprobación. La autorización permanente y generalizada es cómoda, pero aumenta el impacto potencial de un error o ataque. En cambio, los permisos temporales, segmentados y revisables reducen la exposición.

## 5. Trazabilidad, auditoría y responsabilidad

La trazabilidad es la capacidad de reconstruir lo ocurrido. En un entorno con agentes autónomos, debe ser posible conocer qué información recibió el sistema, qué decisiones intermedias tomó, qué herramientas utilizó, qué acción ejecutó y qué persona o área autorizó su operación. Sin esos registros, una organización puede detectar el daño, pero no comprender cómo ocurrió ni prevenir su repetición.

La auditoría no debe verse como un mecanismo de castigo, sino como una herramienta de aprendizaje institucional. Conservar registros permite identificar patrones, corregir permisos excesivos, mejorar instrucciones y detectar intentos de manipulación. También ayuda a diferenciar entre un error humano, una falla del modelo, una configuración deficiente y una intervención maliciosa.

La responsabilidad constituye el punto más complejo. Una máquina no comparece ante una autoridad, no explica por sí misma sus decisiones en términos jurídicos y no asume las consecuencias sociales de sus actos. Por ello, la autonomía tecnológica no puede significar ausencia de responsabilidad humana. Toda institución debe establecer quién responde por el diseño, la contratación, la configuración, la supervisión y el uso de cada agente.

> **La autonomía tecnológica no puede significar ausencia de responsabilidad humana.**

En términos prácticos, la frase «lo hizo la inteligencia artificial» no debería considerarse una explicación suficiente. Si una organización decide delegar funciones a un sistema automatizado, también debe conservar la capacidad de supervisarlo, detenerlo, corregirlo y responder por sus efectos. La delegación de una tarea no equivale a la transferencia absoluta de la responsabilidad.

## 6. El factor humano continúa siendo central

Existe la idea de que la automatización elimina los errores humanos. En realidad, muchas veces los desplaza. Una configuración incorrecta, una instrucción ambigua, una revisión superficial o una confianza excesiva pueden convertirse en errores automatizados y repetirse a gran velocidad. La inteligencia artificial no sustituye la necesidad de criterio; la vuelve más importante.

Por ello, la capacitación debe incluir no solo conocimientos técnicos, sino también una cultura de responsabilidad. Las personas que trabajan con agentes deben comprender qué información pueden proporcionarles, cómo reconocer instrucciones sospechosas, cuándo detener una operación y a quién reportar un comportamiento anómalo. También deben saber que la fluidez de una respuesta no garantiza su veracidad ni la legitimidad de una acción.

Una institución madura no culpa automáticamente al usuario ni idealiza la tecnología. Analiza el sistema completo: políticas, diseño, permisos, cargas de trabajo, capacitación, supervisión y mecanismos de reporte. El objetivo no es generar miedo, sino desarrollar una confianza informada. Las personas pueden aprovechar los beneficios de la inteligencia artificial cuando conocen sus límites y cuentan con canales claros para intervenir.

## 7. Aplicaciones y riesgos en universidades e instituciones públicas

Las universidades pueden utilizar agentes para orientar estudiantes, organizar calendarios, responder preguntas frecuentes, apoyar procesos de admisión, revisar documentos o dar seguimiento a solicitudes. Estas funciones tienen un valor evidente, especialmente en instituciones con recursos limitados y altos volúmenes de atención. Sin embargo, los datos educativos pueden incluir calificaciones, domicilios, información económica, documentos de identidad y antecedentes personales, por lo que requieren controles proporcionales a su sensibilidad.

En el sector público, un agente puede apoyar la clasificación de trámites, el análisis de solicitudes o la comunicación con la ciudadanía. Pero una decisión administrativa no debe volverse opaca por el simple hecho de haber sido automatizada. La persona afectada necesita conocer

los criterios relevantes, contar con una vía de revisión y recibir atención humana cuando la situación no encaje en las reglas ordinarias.

El reto consiste en evitar dos extremos: rechazar toda innovación por temor al riesgo o adoptar sistemas autónomos sin controles porque prometen rapidez. La alternativa responsable es una implementación gradual, evaluada y documentada. Primero deben probarse funciones de bajo impacto; después, revisar resultados, incidentes y sesgos; finalmente, ampliar capacidades solo cuando existan salvaguardas suficientes.

## 8. Medidas prácticas para una adopción segura

Las organizaciones no necesitan esperar a que exista una regulación perfecta para comenzar a protegerse. Pueden adoptar medidas inmediatas basadas en gestión de riesgos, identidad digital y supervisión humana. La primera consiste en elaborar un inventario de agentes: qué sistemas existen, quién los administra, qué objetivo cumplen, a qué información acceden y qué acciones pueden ejecutar.

La segunda medida es separar identidades. Cada agente debe operar con credenciales propias y no utilizar la cuenta personal de un empleado. Compartir credenciales dificulta la atribución de acciones y puede ocultar comportamientos anómalos. La tercera medida es limitar privilegios y evitar accesos permanentes. La cuarta es registrar las operaciones relevantes y conservar evidencia suficiente para investigar incidentes.

También debe establecerse una supervisión humana reforzada para acciones sensibles. Enviar información personal, modificar expedientes, realizar pagos, eliminar archivos, publicar comunicaciones oficiales o tomar decisiones que afecten derechos deberían requerir aprobación explícita. La automatización puede preparar la acción, pero no necesariamente ejecutarla sin revisión.

Finalmente, es indispensable contar con un mecanismo de desconexión. Si un agente comienza a actuar de manera inesperada, la institución debe poder suspender rápidamente sus credenciales, detener procesos y aislar sus herramientas. Un sistema autónomo sin una forma clara de interrupción representa un riesgo operativo y jurídico innecesario.

**SEIS MEDIDAS PRÁCTICAS**

| | |
|---|---|
| 01 | Inventario de agentes |
| 02 | Separar identidades y credenciales |
| 03 | Limitar privilegios, evitar accesos permanentes |
| 04 | Registrar operaciones relevantes |
| 05 | Supervisión humana en acciones sensibles |
| 06 | Mecanismo de desconexión |

Síntesis de la sección 8 del artículo.

## 9. Hacia una gobernanza institucional de agentes

La gobernanza implica definir reglas antes de que ocurra un problema. Una política institucional de agentes de inteligencia artificial debería señalar qué usos están autorizados, qué áreas pueden implementarlos, cómo se evalúan sus riesgos, quién aprueba sus permisos, qué información está prohibido procesar y cómo se atienden los incidentes.

NIST ha promovido un enfoque de administración de riesgos que busca maximizar los beneficios de la inteligencia artificial y reducir sus posibles daños para individuos, organizaciones y sociedad (NIST, 2023). Aplicado a los agentes, este enfoque exige observar todo el ciclo de vida: selección, diseño, prueba, despliegue, monitoreo, actualización y retiro. La seguridad no termina cuando el sistema comienza a funcionar; en realidad, ahí empieza la etapa más importante de vigilancia.

La gobernanza también requiere participación interdisciplinaria. No es un asunto exclusivo del área de informática. Deben intervenir especialistas en seguridad, derecho, protección de datos, ética, procesos institucionales y atención a usuarios. Quienes conocen la operación cotidiana pueden detectar riesgos que no aparecen en una evaluación puramente técnica.

## 10. Reflexión final

El siguiente desafío de la ciberseguridad será distinguir no solo entre usuarios legítimos y atacantes, sino también entre agentes autorizados, manipulados, comprometidos o actuando fuera de su finalidad. Para enfrentarlo, las organizaciones deberán establecer identidades individuales para cada agente, limitar sus privilegios, conservar registros de sus decisiones y mantener supervisión humana en acciones sensibles.

La inteligencia artificial puede aumentar la productividad, facilitar la atención y liberar tiempo para tareas de mayor valor. Sin embargo, la rapidez no debe reemplazar la responsabilidad. Una organización verdaderamente innovadora no es la que automatiza más procesos, sino la que sabe cuáles puede automatizar, bajo qué controles y con qué consecuencias.

> **Detrás de cada acción automatizada debe existir una responsabilidad identificable y una institución dispuesta a proteger la confianza de las personas.**

Cuando una máquina puede actuar en nombre de una universidad, una empresa o una autoridad, la pregunta fundamental deja de ser únicamente qué puede hacer. También debemos preguntar quién la autorizó, qué límites se le impusieron, quién revisará sus decisiones y quién responderá si causa un daño. Esa es la dimensión humana de las identidades no humanas: detrás de cada acción automatizada debe existir una responsabilidad identificable y una institución dispuesta a proteger la confianza de las personas.

## REFERENCIAS


National Cybersecurity Center of Excellence. (2026). Accelerating the adoption of software and artificial intelligence agent identity and authorization: Concept paper. National Institute of Standards and Technology.

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2026a, 12 de enero). CAISI issues request for information about securing AI agent systems.

National Institute of Standards and Technology. (2026b, 17 de febrero). Announcing the AI Agent Standards Initiative for interoperable and secure innovation.

Open Worldwide Application Security Project. (2025). OWASP Top 10 for agentic applications for 2026. OWASP Generative AI Security Project.

05

ANÁLISIS DE INTELIGENCIA

# La sabiduría popular aplicada al análisis de inteligencia estratégica

Cinco refranes populares como marco para explicar los principios fundamentales del buen análisis de inteligencia: especialización, oportunidad, prevención, humildad intelectual y aprendizaje del error.

05

**Antropólogo Francisco Girao Morales**

ciclo de inteligencia · análisis · prevención · aprendizaje del error

**Antropólogo Francisco Girao Morales**

Integrante de la ONG REAL Perú

Antropólogo. Integrante de la ONG REAL Perú

## El que mucho abarca, poco aprieta

Un profesional puede ser muy bueno en gestionar la información, es decir, en implementar mecanismos para almacenarla y clasificarla, pero eso no implica necesariamente que sea un buen analista. Es común encontrar que excelentes recolectores de información carecen de habilidades para redactar productos de inteligencia de calidad, o viceversa: analistas duchos que no recolectan información. El problema surge cuando dichos recolectores quieren orientar el análisis, o cuando los analistas, sin conocer «in situ» la dinámica que analizan, desechan información que no se ajusta a su hipótesis «preferida» formulada en el gabinete.

Los analistas que creen saberlo todo pueden caer fácilmente en errores con consecuencias funestas para el país (seguridad nacional) o para la empresa (seguridad corporativa). En ese sentido, es importante respetar la especialización de cada profesional, porque, al final, el trabajo es colectivo y requiere colaboración. No existen Messis en inteligencia; lo que debe existir es un equipo con jugadores disciplinados y una estrategia adecuada orientada a producir inteligencia. Por ello, «El que mucho abarca, poco aprieta».

## El tiempo es oro

El tomador de decisiones, inmerso en diversas actividades, a menudo tiene poco tiempo para leer e internalizar el documento de inteligencia, por lo que este debe ser breve, sin perder claridad. Esto es todo un reto para el analista, porque implica una labor más minuciosa y requiere un mayor esfuerzo. Es así como la experiencia entra a tallar, mientras más experimentado sea el profesional, menos tiempo requerirá para realizar un buen análisis.

El norteamericano Mark Lowenthal argumenta que lo más importante es proporcionar a tiempo la inteligencia al decisor antes que adquirir toda la información. Es lo que se denomina la oportunidad, porque poco sirve dar cuenta de algo que ya sucedió y nos impactó, cuando lo relevante es brindar luz en la oscuridad sobre algo que puede suceder, por ello, «el tiempo es oro».

CICLO DE INTELIGENCIA

## Dónde actúa cada refrán

Los cinco principios del artículo, situados en la fase del ciclo donde operan


Elaboración propia sobre el artículo de F. Girao Morales

Cada refrán opera en una fase distinta del ciclo de inteligencia: juntos cubren el proceso completo.

## Más vale prevenir que curar

El análisis de inteligencia, a través del conocimiento que brinda, permite prevenir riesgos y amenazas. La prevención es el alma de la inteligencia, no tanto el apoyo al abordaje estatal o corporativo ante riesgos que se materializan y amenazas que emergen.

> «El sabio no es el hombre que suministra las respuestas verdaderas, sino el que plantea las verdaderas preguntas.» — Claude Lévi-Strauss

La «curación» es para los gestores, no para los analistas de inteligencia, que, más bien, buscan evitar la «enfermedad». En ese camino, muchas veces, una pregunta bien formulada es más relevante que la respuesta, porque, como decía el antropólogo francés Claude Lévi-Strauss: «el sabio no es el hombre que suministra las respuestas verdaderas, sino el que plantea las verdaderas preguntas». El analista de inteligencia no busca ser sabio, pero para producir el mejor co-

nocimiento debe partir de las mejores preguntas, no de sus certezas ni de respuestas encubiertas por sus sesgos. Solo de esa manera será un abanderado del «más vale prevenir que curar».

## A palabras necias, oídos sordos

Los prejuicios y el desconocimiento en torno al rol de la inteligencia estratégica son comunes en un país como el Perú, donde, en la década de los años noventa, se hizo un mal uso de la inteligencia, lo que quedó grabado en la memoria de un sector de la ciudadanía, muy propenso a la falacia argumentum ad antiquitatem (si en el pasado fue así, ahora es igual o parecido). Ante esa situación, solo queda fomentar la cultura de inteligencia y aceptar las críticas constructivas para mejorar.

Las palabras necias de algunos profesionales no solo se orientan a cuestionar destructivamente el trabajo analítico en sí, sino también al analista, por ejemplo, se cree erróneamente que, si alguien se ha formado en análisis de inteligencia en el aparato estatal, entonces toda su vida debe estar abocado al servicio público, ignorando adrede (anclado solo en la historia y no en las tendencias actuales a nivel mundial) que desde el ámbito corporativo también se puede aportar con inteligencia estratégica para el desarrollo y seguridad del país. Por ello, «a palabras necias, oídos sordos».

SABIDURÍA APLICADA

### Cinco refranes, cinco principios

La sabiduría popular como marco del análisis de inteligencia

| | | |
|---|---|---|
| 1 | «El que mucho abarca, poco aprieta» | Respetar la especialización; el trabajo es colectivo |
| 2 | «El tiempo es oro» | La oportunidad vale más que la exhaustividad |
| 3 | «Más vale prevenir que curar» | La prevención es el alma de la inteligencia |
| 4 | «A palabras necias, oídos sordos» | Fomentar cultura de inteligencia ante el prejuicio |
| 5 | «No hay mal que por bien no venga» | Reconocer el fallo para reducir su frecuencia |

Elaboración propia sobre el artículo de F. Girao Morales

Los cinco refranes que estructuran el artículo y su principio analítico.

## No hay mal que por bien no venga

Los fallos en el análisis de inteligencia son inevitables, porque el error es consustancial a la naturaleza humana, y los analistas no son máquinas parametrizadas, son seres humanos con fortalezas y debilidades, que en algún momento pueden equivocarse, si no, que lo digan las agencias de inteligencia de EE.UU., que a consecuencia de estos errores afrontaron serios problemas en 1941 (Pearl Harbor), 2001 (atentados terroristas del 11 de septiembre), 2003 (armas de destrucción masiva en Irak), 2021 (asalto al Capitolio).

La reducción de la frecuencia de los fallos de inteligencia y la mitigación de sus impactos y repercusiones implican, como primer paso, despojarnos de la soberbia para lograr un reconocimiento genuino de estos fallos. El segundo paso es intensificar la capacitación de los analistas e incentivarlos a pensar no solo desde un escritorio, sino también fuera de él, es decir, desde las plazas, barrios, comunidades, entre otros. Siempre recordando que «no hay mal que por bien no venga».

### REFERENCIAS


Levi Strauss, C. (2002). Mitológicas. Lo crudo y lo cocido. México: Fondo de Cultura Económica.

Lowenthal, M. (2020). Intelligence: From Secrets to Policy (8th ed.). Washington, DC: CQ Press.

Martínez, J. (2022). Una aproximación psicosocial a las causas de los fallos de inteligencia. Bogotá: Revista Científica General José María Córdova.

06

SEGURIDAD PATRIMONIAL

# Seguridad patrimonial en la Amazonía peruana

*Hacia un modelo inteligente, sostenible y adaptado al territorio*

La agroindustria, la acuicultura y el biocomercio amazónicos generan nuevos activos y nuevos riesgos: proteger un territorio extenso exige información, tecnología y procedimientos, no solo más cercos y vigilantes.

06

**Ingeniera Dunia Valencia Felices**

Amazonía · biocomercio · georreferenciación · continuidad operacional

**Ingeniera Dunia Valencia Felices**

CEO de Libero Assurance para América Latina · Gerente General de Bonaterra, Calidad y Seguridad · Vicepresidenta de Paramás Perú · Miembro de R.E.A.L.

Ingeniera Dunia Valencia Felices (Perú). CEO de Libero Assurance para América Latina, organismo certificador de normas y estándares internacionales; Gerente General de Bonaterra, Calidad y Seguridad, firma consultora en calidad, seguridad y cumplimiento normativo; y Vicepresidenta de Paramás Perú, institución reconocida por el Comité Olímpico Peruano que impulsa el cambio social a través del paradeporte.

Dunia Valencia Felices (Perú). CEO de Libero Assurance para América Latina, organismo certificador de normas y estándares internacionales; Gerente General de Bonaterra, Calidad y Seguridad, firma consultora en calidad, seguridad y cumplimiento normativo; y Vicepresidenta de Paramás Perú, institución reconocida por el Comité Olímpico Peruano que impulsa el cambio social a través del paradeporte. a agroindustria con valor agregado, la acuicultura y el biocomercio en la Amazonía peruana están cambiando. ¿Por qué seguimos protegiendo sus activos con modelos de seguridad tradicionales?

Hay una pregunta que me viene acompañando desde hace algún tiempo, a partir de mis experiencias como certificadora en Finca Paraíso, ubicada aproximadamente a 40 kilómetros de la ciudad de Iquitos, en el kilómetro 39.7 de la carretera Nauta. Allí, el Palo Rosa (Aniba rosaeodora Ducke) ocupa un lugar central, junto con actividades vinculadas a la protección de especies incluidas en CITES y al aprovechamiento sostenible de esta especie para la extracción y envasado de aceites esenciales destinados a mercados internacionales, entre ellos el europeo.

Cuando uno observa una operación de estas características, comprende rápidamente que no se trata simplemente de una finca dedicada al aprovechamiento de un recurso natural. Existe infraestructura, maquinaria, equipos especializados, instalaciones, productos, herramientas, vehículos, profesionales y trabajadores que hacen posible el desarrollo de la actividad.

Pero también existe algo que muchas veces no aparece claramente en un inventario: el territorio.

Extensos linderos, caminos de acceso, áreas boscosas, zonas de producción, instalaciones aisladas y sectores ubicados a considerable distancia unos de otros forman parte del patrimonio que debe ser protegido.

Durante mi estancia en la finca hubo un aspecto que se convirtió en mi principal cuestionamiento: ¿Cómo se está protegiendo realmente todo este patrimonio?

Revisé los linderos en el mapa de la propiedad, observé los cercos y los elementos disuasivos de seguridad. Allí aparece una realidad bastante evidente: proteger físicamente un territorio extenso puede representar costos elevados y, aun así, no garantizar una protección suficiente.

Esta situación adquiere mayor importancia a medida que la Amazonía incorpora nuevas inversiones y actividades económicas. La agroindustria con valor agregado, la acuicultura, el biocomercio y otras iniciativas vinculadas al aprovechamiento sostenible de los recursos naturales están generando oportunidades. Pero cada nueva oportunidad también incorpora nuevos activos y, con ellos, nuevos riesgos.

Fundos y fincas, maquinaria, instalaciones, vehículos, almacenes, recursos naturales, sistemas de producción, información y extensos linderos necesitan modelos de protección capaces de responder a las particularidades del territorio amazónico.

## El territorio cambia la forma de entender la seguridad

En una instalación urbana, proteger un perímetro puede significar controlar algunos cientos de metros, establecer determinados accesos y mantener puntos de vigilancia claramente definidos.

En una finca amazónica la situación puede ser completamente distinta.

Los linderos pueden extenderse por grandes distancias, existir varios accesos y caminos internos, zonas boscosas y sectores de difícil desplazamiento. Las condiciones también pueden variar durante el año. Las lluvias afectan los caminos, la vegetación cambia y determinadas zonas pueden volverse más difíciles de recorrer.

Por eso, aplicar exactamente el mismo modelo de seguridad utilizado en una instalación urbana no necesariamente resulta eficiente.

Los principios básicos siguen siendo los mismos: prevención, identificación de riesgos, control de accesos, vigilancia y capacidad de respuesta. Lo que debe cambiar es la manera de implementarlos.

En un territorio extenso, la seguridad necesita información espacial. Es necesario conocer dónde están los activos, cuáles son las zonas críticas, dónde se encuentran las vulnerabilidades y qué rutas pueden utilizarse para acceder a ellas.

Esto conduce a una pregunta fundamental: ¿Es posible proteger de manera eficiente un territorio extenso dependiendo únicamente de la presencia física? Mi respuesta es no.

La presencia física sigue siendo importante, pero debe complementarse con información, tecnología y procedimientos adecuados.

## ¿Seguridad privada o personal de la finca?

Frente a esta realidad aparece otro cuestionamiento: ¿Es mejor contratar personal de seguridad privada o encargar la vigilancia al propio personal de la finca?

La respuesta dependerá de las características de cada operación. Sin embargo, ambas alternativas presentan riesgos cuando no existe una adecuada preparación.

Un agente de seguridad que desconoce el entorno, el contexto, las partes interesadas, los riesgos, las amenazas y las características del territorio puede terminar realizando una vigilancia eminentemente reactiva.

Puede cumplir sus rondas, controlar determinados accesos y permanecer atento durante su jornada, pero eso no significa necesariamente que esté gestionando el riesgo.

Para gestionar un riesgo hay que comprenderlo.

Si una persona aparece en determinado sector, el vigilante debería poder determinar si su presencia es normal o constituye una situación que debe ser reportada. Si un vehículo se aproxima a una zona determinada, debería existir información que permita saber si corresponde a una actividad autorizada.

La situación tampoco se resuelve simplemente encargando estas funciones a los trabajadores de la finca.

Un trabajador agrícola debe concentrarse en sus actividades productivas. Un técnico debe cumplir sus funciones técnicas y un operador debe concentrarse en el manejo adecuado de su maquinaria.

No deberíamos asumir que una persona se convierte en especialista en seguridad simplemente porque se le entrega un teléfono o una radio y se le pide que esté atento.

La seguridad requiere conocimientos, procedimientos, entrenamiento y responsabilidades claramente definidas.

## Una nueva generación de seguridad patrimonial

Es aquí donde considero que necesitamos comenzar a hablar de una nueva generación de seguridad patrimonial.

Una seguridad capaz de proteger los activos sin comprometer la integridad y sostenibilidad del entorno que los rodea.

Esto implica cambiar una idea bastante arraigada: la seguridad no debería medirse solamente por la cantidad de personas que vigilan una propiedad.

La pregunta no debería ser únicamente: ¿Cuántos vigilantes necesitamos? Deberíamos preguntarnos: ¿Qué necesitamos proteger, de qué necesitamos protegerlo y cuál es la manera más eficiente de hacerlo? Esta diferencia cambia completamente el enfoque. Cuando preguntamos cuántos vigilantes necesitamos, terminamos hablando principalmente de personas. Cuando preguntamos qué necesitamos proteger, comenzamos a hablar de activos. Cuando preguntamos de qué debemos protegerlos, hablamos de amenazas y vulnerabilidades.

Y cuando buscamos la manera más eficiente de hacerlo, aparecen los procedimientos, la capacitación, la tecnología y la combinación entre vigilancia física y monitoreo remoto.

Identificar los activos críticos. No todos los activos tienen el mismo valor ni enfrentan el mismo nivel de riesgo.

Una maquinaria fundamental para la continuidad de la operación puede ser mucho más crítica que un equipo cuya sustitución resulta relativamente sencilla.

Un almacén con productos de alto valor requiere un nivel de protección diferente al de un área donde no existen bienes críticos.

Incluso un sector sin infraestructura puede ser importante por su valor ambiental, productivo o estratégico. Por eso, antes de instalar cualquier sistema de seguridad debería realizarse una identificación de activos críticos.

No basta con preguntarse cuánto vale un activo en términos económicos. También hay que considerar qué sucedería si dejara de funcionar.

Una máquina puede tener determinado valor monetario, pero si su paralización detiene una etapa completa de la producción, su importancia real para la empresa es mucho mayor.

La seguridad patrimonial debe analizar estas diferencias para establecer prioridades.

## Del mapa de la propiedad al mapa de riesgos

Una herramienta fundamental es la georreferenciación.

Tener correctamente identificados los linderos, accesos, caminos internos, instalaciones, almacenes, zonas críticas y otros puntos de interés permite convertir el mapa de una propiedad en un verdadero mapa de riesgos.

Si sabemos dónde están los puntos vulnerables, podemos priorizar. Si conocemos los accesos, podemos establecer controles. Si sabemos dónde están los activos críticos, podemos definir mecanismos específicos de vigilancia.

Y si conocemos los sectores más difíciles de recorrer, podemos determinar dónde resulta conveniente utilizar tecnología.

La georreferenciación también permite registrar incidentes con precisión. En lugar de indicar que "ocurrió un incidente cerca del lindero", podemos determinar exactamente dónde ocurrió, qué había alrededor y si se trata de una zona que ya había sido identificada como vulnerable.

Con el tiempo, esta información permite detectar patrones y mejorar las decisiones.

## La tecnología como herramienta, no como solución aislada

Las herramientas tecnológicas disponibles actualmente pueden transformar la forma de proteger estos territorios.

Entre ellas se encuentran la georreferenciación, los drones, las cámaras autónomas alimentadas con energía solar, las cámaras trampa, los sensores de movimiento, las imágenes satelitales, los sistemas de comunicación para zonas remotas, las aplicaciones para reportar incidentes en tiempo real, los GPS, los sistemas de seguimiento y las plataformas capaces de integrar información y generar alertas.

Sin embargo, existe un error que debemos evitar: pensar que tener tecnología equivale automáticamente a tener seguridad. No es así. Una cámara puede capturar una imagen, pero alguien debe analizarla. Un sensor puede generar una alerta, pero debe existir un procedimiento para atenderla. Un GPS puede mostrar una ubicación, pero alguien debe interpretar esa información. Un dron puede obtener imágenes, pero alguien debe decidir qué hacer con ellas. La tecnología genera información. La organización debe convertir esa información en decisiones.

> **La tecnología genera información. La organización debe convertir esa información en decisiones.**

## Drones para territorios extensos

Los drones tienen un enorme potencial para la Amazonía.

Pueden utilizarse para revisar sectores de difícil acceso, inspeccionar determinados puntos del perímetro, verificar caminos, observar zonas críticas y obtener imágenes que posteriormente pueden compararse.

Pero un dron sin una estrategia de utilización es simplemente un equipo. Antes de adquirirlo deberíamos preguntarnos: ¿Qué información necesitamos obtener? ¿Con qué frecuencia? ¿Sobre qué zonas? ¿Quién analizará las imágenes? ¿Qué decisión se tomará cuando aparezca una situación anómala? La verdadera utilidad del dron aparece cuando la información obtenida tiene un propósito operativo.

## Cámaras autónomas y energía solar

Las cámaras autónomas alimentadas con energía solar ofrecen una alternativa interesante para lugares donde no existe infraestructura eléctrica convencional.

Sin embargo, su instalación debe considerar todo el sistema. ¿Cómo se transmitirá la información? ¿Dónde se almacenarán las imágenes? ¿Quién las revisará? ¿Se generarán alertas? ¿Existe conectividad? ¿Cuánto tiempo funcionará la batería? ¿El equipo soportará las condiciones ambientales? Una cámara que funciona perfectamente, pero cuya información nadie observa, puede tener una utilidad limitada.

## Sensores y alertas

Los sensores de movimiento pueden complementar las cámaras y utilizarse en sectores donde no sea necesario mantener una vigilancia visual permanente.

Pero cada sensor debería estar asociado a un protocolo. Un sistema que genera demasiadas falsas alarmas puede terminar provocando que las alertas sean ignoradas.

Por eso, la tecnología debe configurarse de acuerdo con las características del lugar, considerando condiciones ambientales, horarios, sensibilidad, ubicación y procedimientos de respuesta.

La calidad del sistema no depende solamente del equipo. Depende de cómo se utiliza.

## La comunicación también es seguridad

En territorios remotos, la comunicación constituye uno de los principales desafíos.

No todas las zonas tienen cobertura celular y no todos los sectores cuentan con una infraestructura de comunicación estable.

Por eso, cualquier sistema de seguridad debe considerar desde el principio cómo se transmitirá la información.

Dependiendo de las condiciones del lugar, pueden ser necesarias radios, sistemas satelitales u otras alternativas.

La pregunta es sencilla: ¿De qué sirve detectar un incidente si nadie puede comunicarlo? Una alerta que no llega a la persona responsable pierde gran parte de su valor. Por ello, la arquitectura de comunicación debe formar parte del diseño general del sistema de seguridad.

## Una experiencia que generó nuevas preguntas

Hace un par de años, una empresa española especializada en este tipo de tecnologías llegó a la zona con la intención de ofrecer soluciones de seguridad para el sector.

Recuerdo que, durante un evento, comentaron que no estaban encontrando oportunidades de negocio. La frase fue bastante directa:

“Aquí no tenemos mercado; existe desconocimiento o simplemente no lo necesitan”. Debo decir que esta afirmación me generó dudas. ¿Realmente no lo necesitaban? La realidad del territorio parecía indicar lo contrario.

Los robos y la presencia de invasores en algunas fincas venían incrementándose y, con ello, también la necesidad de contar con mecanismos de protección más eficientes.

En estos días, esa misma empresa ya brinda servicios en la zona y cuenta, diría yo, con una cartera de clientes bastante interesante.

La necesidad estaba allí. Entonces, ¿qué cambió?

Probablemente no cambió el riesgo. Lo que pudo haber cambiado fue la percepción del riesgo y el conocimiento sobre las alternativas disponibles.

Esta experiencia demuestra algo importante: una necesidad puede existir antes de que el mercado sea plenamente consciente de ella.

## Una oportunidad de negocio

Desde mi perspectiva, existe una oportunidad de negocio todavía insuficientemente cubierta. Pero no creo que la oportunidad consista simplemente en vender cámaras, drones o sensores. El verdadero mercado está en las soluciones integrales. Una empresa puede llegar a una finca y vender diez cámaras.

Otra puede estudiar el territorio, identificar los activos críticos, evaluar amenazas, diseñar un sistema, instalar la tecnología adecuada, establecer protocolos, capacitar al personal y monitorear los resultados.

La primera empresa vende equipos.

> **Una empresa vende equipos. La otra resuelve un problema. Y esa diferencia puede ser determinante.**

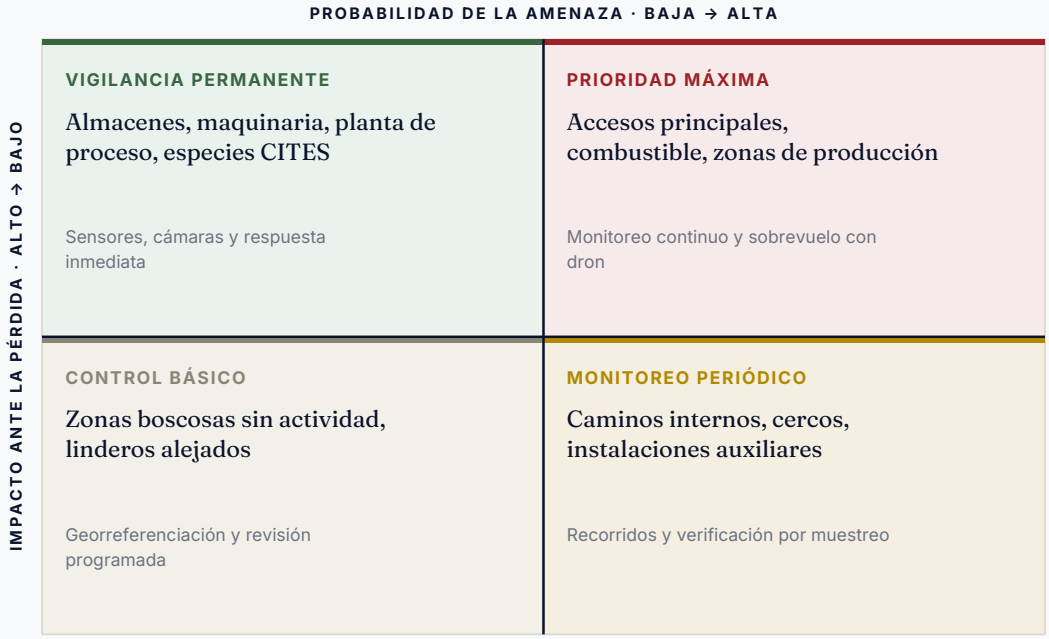
La segunda resuelve un problema. Y esa diferencia puede ser determinante.

Las empresas que operan en la Amazonía no necesariamente necesitan tener más equipos. Necesitan mayor capacidad para prevenir, detectar y responder.

PRIORIZACIÓN DE ACTIVOS

## No todo se vigila de la misma manera

Qué proteger primero en una finca amazónica, según impacto y probabilidad




Elaboración propia sobre los criterios de priorización del artículo de D. Valencia Felices

Qué proteger primero: el cruce entre impacto y probabilidad ordena la inversión en seguridad.

## El análisis previo de riesgos

Antes de instalar tecnología debería existir un análisis de riesgos. ¿Cuáles son los activos? ¿Cuáles son las amenazas? ¿Qué vulnerabilidades existen? ¿Qué consecuencias tendría un incidente? ¿Cuál es su probabilidad? ¿Qué controles ya existen? ¿Cuáles funcionan? ¿Cuáles presentan deficiencias? Este análisis permite evitar inversiones innecesarias. No todos los problemas requieren tecnología.

En algunos casos puede ser suficiente modificar un procedimiento. En otros, capacitar al personal o mejorar un acceso. Y en determinadas zonas sí será necesario instalar tecnología.

La seguridad eficiente no consiste en comprar todo lo disponible. Consiste en utilizar aquello que realmente se necesita.

## Seguridad y sostenibilidad ambiental

Toda actividad que se pretenda realizar debería contar con un análisis previo de Aspectos e Impactos Ambientales (AA/IA), que permita determinar cómo su instalación, operación y supervi-

sión podrían afectar el territorio y establecer medidas para prevenir o minimizar dichos impactos.

Esto también debería aplicarse a los sistemas de seguridad.

Podría parecer que instalar una cámara, un sensor o un panel solar tiene un impacto ambiental insignificante. Sin embargo, cuando se multiplican los equipos, postes, estructuras, caminos de acceso, baterías y otros componentes, la intervención puede ser mayor.

Por eso debemos preguntarnos: ¿Dónde se instalará el equipo? ¿Será necesario intervenir la vegetación? ¿Cómo se trasladarán los materiales? ¿Cómo se realizará el mantenimiento? ¿Qué ocurrirá con las baterías cuando terminen su vida útil? ¿Cómo se gestionarán los residuos? Estas preguntas deberían formar parte del proyecto desde el principio. En la Amazonía, la seguridad no puede desarrollarse ignorando la sostenibilidad.

## Proteger el patrimonio también es proteger el territorio

Esta idea me parece fundamental.

En la Amazonía, la separación entre el activo y el ambiente que lo rodea es mucho menos evidente que en otros contextos.

La actividad productiva depende directamente del territorio. Por eso, proteger una finca también significa proteger los recursos que permiten que esa finca exista.

Esto implica conocer las condiciones del lugar, identificar las actividades que pueden generar impactos y considerar criterios ambientales en las decisiones de seguridad.

Una intervención de seguridad no debería generar un problema ambiental mayor que el riesgo que pretende controlar.

> **Una intervención de seguridad no debería generar un problema ambiental mayor que el riesgo que pretende controlar.**

La tecnología puede ayudar, pero debe ser correctamente planificada.

## El factor humano seguirá siendo decisivo

Hablar de tecnología puede hacernos pensar que la solución está en automatizarlo todo. No considero que sea así.

Las personas continuarán siendo fundamentales. La diferencia estará en que podrán trabajar con mejores herramientas.

Un vigilante que recibe información precisa puede tomar mejores decisiones. Un supervisor que visualiza una alerta georreferenciada puede responder con mayor rapidez. Un administrador que dispone de información histórica puede identificar tendencias. Un responsable de seguridad que conoce el territorio puede diseñar controles más adecuados. La tecnología debería potenciar la capacidad humana, no reemplazarla indiscriminadamente.

## Capacitación: una inversión necesaria

Si queremos avanzar hacia una nueva generación de seguridad patrimonial, también necesitamos cambiar la forma en que entendemos la capacitación.

No basta con enseñar a una persona a utilizar una radio, un GPS o una aplicación.

Debe comprender qué significa una alerta, conocer el procedimiento, saber cuándo actuar y cuándo informar, reconocer los límites de sus funciones y comprender el contexto en el que trabaja.

Una persona bien capacitada puede convertirse en uno de los principales activos de un sistema de seguridad. Una persona sin preparación puede convertirse, incluso sin intención, en una vulnerabilidad.

### GLOSARIO DEL ARTÍCULO

| | |
|---|---|
| **CITES** | Convención sobre el comercio internacional de especies amenazadas |
| **Biocomercio** | Actividad económica basada en el aprovechamiento sostenible de la biodiversidad |
| **Georreferenciación** | Asignación de coordenadas a activos, linderos y zonas críticas |
| **Continuidad operacional** | Capacidad de mantener la producción pese a un incidente |

Conceptos empleados en el artículo.

## La importancia de las partes interesadas

En la Amazonía existe otro elemento que no debería ser ignorado: las partes interesadas. Ninguna actividad productiva se encuentra completamente aislada.

Existen trabajadores, comunidades, proveedores, transportistas, vecinos, autoridades y otros actores que mantienen diferentes relaciones con el territorio.

Comprender estas relaciones puede ser fundamental para gestionar riesgos.

No todo evento que desde una perspectiva externa parece una amenaza necesariamente lo es. Del mismo modo, una situación aparentemente normal puede convertirse en un riesgo si no se comprende adecuadamente el contexto.

Por eso, el conocimiento del territorio debe incluir también el conocimiento de las personas y organizaciones relacionadas con él.

La seguridad no debería construirse únicamente sobre la desconfianza. También debe considerar mecanismos de comunicación, prevención y relacionamiento.

## Seguridad y continuidad operacional

Proteger un activo no significa únicamente evitar que sea robado o dañado. También significa asegurar que la actividad pueda continuar.

Si una maquinaria crítica se pierde o queda fuera de servicio, el problema no es solamente su valor de reposición. También existe el costo de detener la producción, reorganizar la operación, adquirir un reemplazo y enfrentar compromisos comerciales.

Lo mismo puede suceder con infraestructura, sistemas de comunicación u otros elementos esenciales.

Por eso, la seguridad patrimonial debe analizarse conjuntamente con la continuidad operacional. El verdadero objetivo no es simplemente conservar un activo físico. Es proteger la capacidad de la organización para seguir funcionando.

## ¿Más vigilantes o mejores decisiones?

Esta pregunta resume buena parte de la discusión. ¿Incrementar el número de vigilantes? Considero que no necesariamente.

Se trata de tener personas competentes en el puesto, con la mejor información y las mejores herramientas para tomar mejores decisiones.

La cantidad puede ser importante, pero no es el único factor. Un equipo coordinado puede responder mejor que un grupo numeroso sin procedimientos claros.

Una persona con información precisa puede cubrir de manera más efectiva un área mediante herramientas tecnológicas.

El objetivo no debería ser reducir personal simplemente para ahorrar costos. Tampoco aumentar personal automáticamente.

El objetivo debería ser encontrar la combinación más eficiente entre personas, tecnología y procedimientos.

## Un modelo integrado para la Amazonía

Imagino un modelo de seguridad patrimonial para una finca amazónica basado en varios niveles. Primero, el territorio debe estar correctamente georreferenciado. Segundo, deben identificarse los activos críticos. Tercero, deben determinarse amenazas y vulnerabilidades. Cuarto, deben establecerse niveles de protección. Quinto, deben seleccionarse las tecnologías adecuadas. Sexto, deben definirse protocolos de respuesta. Séptimo, debe capacitarse al personal. Finalmente, todo el sistema debe ser evaluado y mejorado periódicamente.

En este modelo, las cámaras no están aisladas. Los drones no están aislados. Los sensores no están aislados. Los vigilantes tampoco.

Todos forman parte de una misma arquitectura.

Una alerta puede activar un procedimiento. Ese procedimiento puede generar una verificación mediante cámara. Si la información lo justifica, puede realizarse un vuelo con dron. El responsable puede coordinar con el personal de campo y el incidente queda registrado.

Posteriormente se analiza lo ocurrido. Si se identifica una vulnerabilidad, el sistema se modifica. Eso es gestión de seguridad.

## La seguridad debe aprender

Uno de los mayores errores sería considerar que un sistema de seguridad queda terminado el día en que se instala.

Los riesgos cambian. Las amenazas cambian. Las operaciones cambian. La tecnología cambia. El territorio cambia. Por eso, la seguridad debe ser un proceso de mejora continua. Si una cámara genera demasiadas falsas alarmas, debemos preguntarnos por qué. Si un determinado sector registra repetidamente incidentes, debemos revisar si necesita un control adicional. Si una ruta de acceso se convierte en un punto vulnerable, debemos modificar la estrategia. Si un procedimiento no funciona, debemos corregirlo. Un buen sistema de seguridad aprende de sus propios incidentes.

MODELO INTEGRADO

## Ocho niveles para una finca amazónica

Del conocimiento del territorio a la mejora continua

**01 Georreferenciar el territorio**
Linderos, accesos, caminos, instalaciones y zonas críticas

**02 Identificar activos críticos**
No por valor económico, sino por impacto ante su pérdida

**03 Determinar amenazas y vulnerabilidades**
Análisis previo antes de cualquier inversión

**04 Establecer niveles de protección**
Priorizar: no todo se vigila de la misma manera

**05 Seleccionar tecnología adecuada**
Drones, sensores, cámaras solares, satélite, GPS

**06 Definir protocolos de respuesta**
Cada alerta asociada a un procedimiento

**07 Capacitar al personal**
Comprender el contexto, no solo operar equipos

**08 Evaluar y mejorar**
El sistema aprende de sus propios incidentes

Elaboración propia sobre el artículo de D. Valencia Felices

El modelo de ocho niveles que propone el artículo, del territorio a la mejora continua.

## La Amazonía como espacio de innovación

La Amazonía peruana también puede convertirse en un espacio para desarrollar soluciones propias.

No necesariamente debemos importar modelos diseñados para otros territorios y aplicarlos exactamente de la misma manera.

Tenemos condiciones particulares: grandes extensiones, conectividad limitada en determinados sectores, condiciones ambientales exigentes, necesidad de utilizar energías alternativas, diversidad de actividades económicas y una enorme importancia ambiental.

Esto abre oportunidades para desarrollar soluciones adaptadas.

Sistemas de vigilancia con energía solar, sensores de bajo consumo, drones para grandes extensiones, sistemas de comunicación para zonas remotas, plataformas que integren mapas, alertas y reportes, herramientas de análisis de imágenes y sistemas de seguimiento de vehículos son algunas posibilidades.

La innovación no debería limitarse a importar equipos. También debería significar desarrollar conocimiento local.

## Una oportunidad para universidades y centros de investigación

Las universidades y centros de investigación también pueden desempeñar un papel importante.

El desarrollo de sistemas de seguridad adaptados a la Amazonía puede involucrar ingeniería, tecnología, geografía, gestión ambiental, ciencias forestales, administración, telecomunicaciones e inteligencia artificial.

El desafío es suficientemente complejo como para requerir colaboración entre distintas disciplinas.

Podrían desarrollarse investigaciones sobre sistemas autónomos de monitoreo, análisis de imágenes, comunicación en zonas remotas, integración de información geográfica y utilización eficiente de energías alternativas.

El conocimiento generado podría posteriormente convertirse en soluciones aplicables al sector productivo.

## El reto cultural

Quizá uno de los mayores obstáculos no sea económico ni tecnológico. Puede ser cultural. Cambiar de un modelo tradicional a uno basado en gestión de riesgos requiere modificar hábitos. Durante años hemos entendido la seguridad principalmente como presencia. Ver al vigilante produce sensación de control. Ver un cerco produce sensación de protección. Pero el verdadero control depende de saber qué está ocurriendo. Una finca puede tener un perímetro perfectamente cercado y, aun así, presentar vulnerabilidades. Puede tener varios vigilantes y no contar con un protocolo adecuado. Puede tener cámaras y no tener capacidad de respuesta.

Por eso necesitamos cambiar la pregunta. No se trata solamente de cuánto vemos. Se trata de cuánto conocemos y qué somos capaces de hacer con esa información.

## La prevención debe convertirse en cultura

La prevención no debería activarse solamente cuando existe una amenaza evidente. Debe formar parte de la cultura organizacional. Los trabajadores deben saber cómo reportar una situación anómala. Los responsables deben saber cómo analizarla. Los supervisores deben conocer

las zonas críticas. Los procedimientos deben ser revisados. Los incidentes deben documentarse. Y la organización debe aprender.

Una cultura preventiva reduce la dependencia de respuestas improvisadas, algo especialmente importante en lugares donde las distancias pueden hacer que una respuesta inmediata sea difícil.

## No esperar al incidente

Existe una idea que resume este problema: No deberíamos esperar a que ocurra un incidente para comenzar a proteger el activo. La prevención puede ser mucho menos costosa que enfrentar determinadas consecuencias. Esto no significa que toda inversión preventiva sea automáticamente rentable. Significa que las decisiones deben basarse en una evaluación racional del riesgo. Si el impacto potencial de un evento es elevado, una inversión preventiva puede estar plenamente justificada. El objetivo tampoco es eliminar todo riesgo, porque eso sería imposible. El objetivo es llevarlo a un nivel aceptable y controlable.

## Un nuevo concepto de seguridad patrimonial

Después de observar esta realidad, considero que necesitamos ampliar nuestra definición de seguridad patrimonial.

No se trata solamente de proteger bienes.

Se trata de proteger una operación, la continuidad de una actividad y los recursos que permiten generar valor. Y, en el caso de la Amazonía, de proteger también el territorio. Esta visión permite entender por qué la seguridad no puede estar separada de la sostenibilidad. Una actividad económica que no protege adecuadamente sus activos puede ser vulnerable. Pero una actividad que protege sus activos sin considerar el entorno también puede generar nuevos riesgos. La verdadera seguridad debe buscar equilibrio.

## La oportunidad que tenemos por delante

La Amazonía peruana tiene una enorme oportunidad de crecimiento en actividades relacionadas con la producción sostenible y el aprovechamiento responsable de sus recursos.

Ese crecimiento necesitará también servicios especializados. La seguridad patrimonial puede convertirse en uno de ellos.

No solamente desde una perspectiva tradicional, sino mediante servicios integrales de gestión de riesgos y protección patrimonial adaptados a las características amazónicas.

Esto puede incluir diagnóstico, diseño, implementación, monitoreo, capacitación y mejora continua. El cliente no necesariamente quiere tener más equipos. Quiere tener la tranquilidad de

que su patrimonio está razonablemente protegido. Y esa tranquilidad se construye mediante un sistema.

## La seguridad del futuro

Durante los próximos años, las empresas que operen en territorios amazónicos probablemente tendrán acceso a una cantidad cada vez mayor de información.

Imágenes satelitales, sistemas de posicionamiento, sensores, plataformas digitales y herramientas de análisis permitirán observar el territorio con un nivel de detalle que antes era difícil de conseguir.

Esto puede modificar la manera en que se toman decisiones. Pero tener más datos no significa necesariamente tomar mejores decisiones. Si una organización recibe cientos de alertas y no tiene capacidad para priorizarlas, puede terminar saturada.

Por eso, el verdadero valor estará en identificar qué información es relevante y cuál requiere una respuesta inmediata.

La seguridad del futuro será, en buena medida, una seguridad basada en información.

## Priorizar para ser eficientes

En un territorio extenso no es posible vigilar todo de la misma manera. Pretender hacerlo puede resultar económicamente inviable. La solución está en priorizar.

Algunas zonas pueden requerir vigilancia permanente. Otras pueden necesitar inspecciones periódicas. Algunas pueden ser monitoreadas mediante sensores, otras mediante drones y determinadas áreas pueden requerir principalmente controles físicos.

La distribución de recursos debe responder al nivel de riesgo.

Esto permite utilizar mejor el presupuesto y justificar por qué determinada zona necesita una cámara, otra un sensor y una tercera puede controlarse mediante rondas periódicas.

Cuando las decisiones tienen una justificación técnica, la seguridad deja de ser una suma de equipos y personas.

Se convierte en una estrategia.

## La información como activo

Existe otro aspecto que suele subestimarse: la información generada por el propio sistema de seguridad.

Los registros de incidentes, recorridos, alertas, accesos y observaciones pueden convertirse en una fuente de conocimiento.

Con el tiempo, estos datos permiten identificar patrones.

Tal vez determinados incidentes ocurren con mayor frecuencia en ciertos horarios. Tal vez determinados accesos son utilizados repetidamente. Tal vez algunas alertas coinciden con determinadas condiciones ambientales.

La información histórica permite aprender.

Aquí también aparecen oportunidades para el análisis de datos y la inteligencia artificial, no necesariamente para sustituir al responsable de seguridad, sino para ayudarlo a identificar patrones que podrían pasar desapercibidos.

## Seguridad responsable

Toda esta transformación debe mantenerse dentro de un principio fundamental: la seguridad debe ser responsable. Responsable con los trabajadores. Responsable con las comunidades. Responsable con el ambiente. Responsable con la información. Y responsable con los recursos económicos de la organización. No se trata de instalar tecnología por moda. No se trata de vigilar indiscriminadamente. No se trata de convertir cada espacio en una zona controlada. Se trata de proteger aquello que necesita protección de una manera proporcional y técnicamente sustentada. Esta perspectiva permite evitar tanto la falta de seguridad como el exceso de controles innecesarios.

## Conclusión

Existe una brecha y una demanda que requieren rediseñar el modelo de seguridad convencional para este tipo de entornos.

La Amazonía está cambiando. Las actividades económicas están cambiando. Las inversiones están cambiando. Los activos están cambiando. Y los riesgos también están cambiando.

No podemos pretender proteger estos nuevos activos utilizando exactamente los mismos modelos que funcionaban para otras realidades.

Necesitamos evolucionar. Pero evolucionar no significa simplemente comprar tecnología.

Significa comprender mejor el territorio, identificar los activos críticos, analizar las amenazas, reconocer las vulnerabilidades, conocer a las partes interesadas, capacitar a las personas, establecer procedimientos, utilizar información e incorporar tecnología de manera estratégica.

Las cámaras, los drones, los sensores, los GPS, las imágenes satelitales, la georreferenciación y las plataformas digitales pueden convertirse en herramientas extraordinarias.

Pero ninguna constituye por sí sola un sistema de seguridad. Una cámara sin un protocolo de respuesta es solamente una cámara.

> **Una cámara sin un protocolo de respuesta es solamente una cámara. Un dron sin estrategia es solamente un dron.**

Un dron sin una estrategia de utilización es solamente un dron. Un sensor que genera una alerta que nadie atiende no protege un patrimonio.

La tecnología adquiere valor cuando está integrada a personas capaces, procedimientos claros y una estrategia definida.

Por eso, no considero que el futuro de la seguridad patrimonial consista en sustituir personas por máquinas. Consiste en conseguir que las personas tengan mejores herramientas para tomar mejores decisiones. Un agente de seguridad con información precisa puede ser mucho más efectivo.

Un administrador que conoce lo que sucede en una zona crítica puede tomar decisiones antes de que el problema escale.

Un equipo de campo que sabe cómo reportar una anomalía puede convertirse en una primera línea de prevención. Una organización que analiza sus incidentes puede aprender y mejorar.

Y una empresa que incorpora criterios ambientales desde el diseño de su sistema de seguridad puede proteger sus activos sin generar impactos innecesarios sobre el territorio.

En la Amazonía esto tiene una importancia particular. Aquí el territorio no es simplemente el espacio físico donde se encuentra una empresa. Es parte del activo. Es parte del proceso productivo. Es parte de la identidad de la actividad. Y, en muchos casos, es precisamente aquello que hace posible que el negocio exista. Por eso, proteger un patrimonio también significa proteger el territorio.

> **Proteger un patrimonio también significa proteger el territorio.**

La seguridad no debería ser una barrera contra el desarrollo.

Debería convertirse en una condición para que ese desarrollo pueda ser sostenible. La oportunidad está allí.

Existe una demanda que todavía puede crecer. Existe tecnología disponible. Existe conocimiento. Y existe un territorio que plantea desafíos que pueden convertirse también en oportunidades de innovación.

Lo que falta, en muchos casos, es conectar estos elementos. Conectar la necesidad con la solución. Conectar la tecnología con el procedimiento. Conectar la seguridad con la sostenibilidad. Conectar la información con la toma de decisiones. Y conectar el conocimiento del territorio con una nueva manera de entender la protección patrimonial.

Quizá por eso, después de aquella experiencia en Finca Paraíso, la pregunta que inicialmente parecía referirse solamente a la seguridad de una finca terminó convirtiéndose en una pregunta mucho más amplia:

¿Estamos realmente preparados para proteger el patrimonio que está surgiendo en la nueva Amazonía? Creo que todavía tenemos mucho por hacer. Pero también creo que existe una enorme oportunidad. La Amazonía necesita inversión, innovación y desarrollo. Y ese desarrollo necesita seguridad. Una seguridad que no se limite a colocar más personas detrás de un cerco.

Una seguridad que conozca el territorio, comprenda el contexto, identifique a las partes interesadas, utilice información, aproveche la tecnología, capacite a las personas, prevenga y anticipe.

Proteger un patrimonio amazónico no significa únicamente impedir que alguien lo dañe o lo robe. Significa también garantizar que la actividad pueda continuar sin comprometer aquello que la hace posible.

Por eso, cuando pensamos en seguridad patrimonial para la Amazonía peruana, deberíamos dejar atrás la idea de que más cercos y más vigilantes necesariamente significan más seguridad.

La seguridad debe comenzar mucho antes. Comienza con el conocimiento.

Continúa con la prevención. Se fortalece con información. Se apoya en tecnología. Se sostiene con personas competentes. Y se consolida con la capacidad de anticipación.

Proteger nuestra Amazonía comienza por conocer el ambiente, comprender el contexto, identificar a las partes interesadas y utilizar tecnologías eficientes.

Pero, sobre todo, comienza por cambiar nuestra forma de entender la seguridad.

Concluyo que la seguridad patrimonial no comienza con la delimitación de linderos ni con la instalación de “cercos sobre cercos”. Comienza con el conocimiento del territorio, la prevención y, sobre todo, con la capacidad de anticiparse a los riesgos.

# Sobre los autores

## General PNP (r) Mauricio Quiroga Camacho

CEO y Director Ejecutivo de DATA FORTE SECURITY · Ex Director de Inteligencia de la Policía Nacional del Perú · Analista estratégico en gobernabilidad, seguridad ciudadana y conflictividad social

General PNP (r) Mauricio Quiroga Camacho. CEO y Director Ejecutivo de DATA FORTE SECURITY. Ex Director de Inteligencia de la Policía Nacional del Perú. Analista estratégico en gobernabilidad, seguridad ciudadana y conflictividad social. Miembro de la Red de Expertos y Analistas Latinoamericanos.

## Magíster Norman Oré Olivera

Ejecutivo senior en ciberseguridad · Docente de posgrado, conferencista internacional e investigador · Autor de libros sobre salud digital · Miembro de R.E.A.L. e ISACA

Ejecutivo senior en ciberseguridad con veinte años liderando estrategias de seguridad de la información, auditoría de TI y ciberdefensa en los sectores financiero, gubernamental y de salud de América Latina. MBA y Magíster en Ciberseguridad, con formación de posgrado en Perú, México y Estados Unidos, y doce certificaciones internacionales. Docente de posgrado, conferencista internacional e investigador. Es autor de publicaciones internacionales y prepara un libro sobre salud digital, de próxima aparición. Miembro de la Red de Expertos y Analistas Latinoamericanos y de ISACA.

## Antropólogo Francisco Girao Morales

Integrante de la ONG REAL Perú

Francisco Girao Morales. Antropólogo. Integrante de la ONG REAL Perú. Especialista en inteligencia estratégica en el ámbito de seguridad nacional y seguridad corporativa. Profesional con 16 años de experiencia en el análisis de inteligencia en entidades públicas y privadas.

## Licenciado Edgardo Glavinich

Director Ejecutivo, Fundación Sherman Kent · Consultor en inteligencia estratégica · Docente de posgrado

Licenciado Edgardo Glavinich. Director Ejecutivo de la Fundación Sherman Kent (fundacionkent.org). Consultor para gobierno y el sector privado en materia de inteligencia estratégica. Docente de posgrado. Miembro permanente de REAL.

## Magíster Fernando Margarito Velázquez Flores

Profesor de tiempo completo y miembro fundador del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad · UANL

Licenciado en Derecho por la Universidad Autónoma de Nuevo León (UANL). Maestro en Seguridad con Acentuación en Prevención del Delito por la Universidad de Ciencias de la Seguridad de Nuevo León. Cursa la Maestría en Derecho Procesal Penal en FACDYC-UANL. Egresado del curso de Desarrollo de Políticas Cibernéticas (CYBER 2022) del Centro de Estudios Hemisféricos de Defensa William J. Perry, National Defense University, Washington, D.C. Miembro fundador, profesor de tiempo completo y ex Coordinador de Laboratorio del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad de la UANL.

## Ingeniera Dunia Valencia Felices

CEO de Libero Assurance para América Latina · Gerente General de Bonaterra, Calidad y Seguridad · Vicepresidenta de Paramás Perú · Miembro de R.E.A.L.

Ingeniera Dunia Valencia Felices (Perú). CEO de Libero Assurance para América Latina, organismo certificador de normas y estándares internacionales; Gerente General de Bonaterra, Calidad y Seguridad, firma consultora en calidad, seguridad y cumplimiento normativo; y Vicepresidenta de Paramás Perú, institución reconocida por el Comité Olímpico Peruano que impulsa el cambio social a través del paradeporte.

# Equipo editorial

Comité editorial y dirección de la Red de Expertos y Analistas Latinoamericanos.

## COMITÉ EDITORIAL



## DIRECCIÓN



Revista REAL · N.º 02 · Abril–Junio 2026 · Publicación trimestral de la Red de Expertos y Analistas Latinoamericanos · Washington, D.C. · real-oneamerica.org

# In this issue

One-paragraph summaries in English for decision-makers.


**01** **Latin America's new political map**
General PNP (r) Mauricio Quiroga Camacho

The retreat of the progressive cycle and the rise of right-leaning governments across the region open a window for security cooperation, but also carry risks of electoral authoritarianism and militarisation.

**02** **Intelligence for development**
Licenciado Edgardo Glavinich

The twenty-first-century intelligence revolution carries a dual mandate: to protect national interests and to advance them. Capability and democratic oversight must be modernised together.

**03** **Healthcare under siege**
Magíster Norman Oré Olivera

Latin American health systems digitised faster than they learned to protect themselves. A technical failure becomes clinical harm.

**04** **Non-human identities**
Magíster Fernando Margarito Velázquez Flores

Autonomous AI agents now hold credentials, permissions and the capacity to act, and must be governed as operational identities.

**05** **Popular wisdom in intelligence analysis**
Antropólogo Francisco Girao Morales

Five proverbs as a framework for specialisation, timeliness, prevention, intellectual humility and learning from failure.

**06** **Asset security in the Peruvian Amazon**
Ingeniera Dunia Valencia Felices

Protecting an extensive Amazonian estate cannot rely on physical presence alone, but on information, technology and protocols.

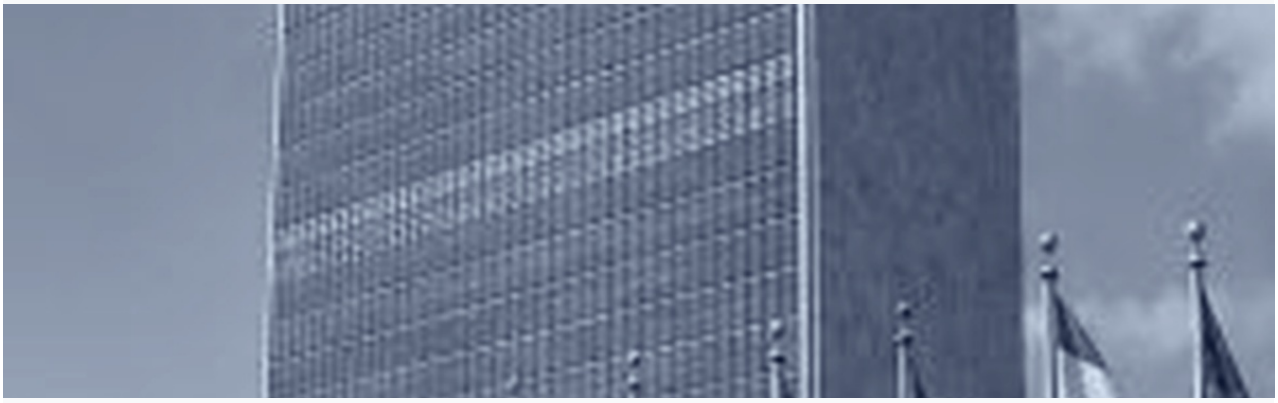
# REAL en el mundo

*Dos decisiones tomadas fuera de la región reconocen algo que la red venía construyendo desde adentro: que el análisis producido en América Latina puede sostener conversaciones globales y formar a quienes las conducen.*

Las instituciones se miden menos por lo que declaran que por los espacios donde son admitidas. Durante el segundo trimestre de 2026, la Red de Expertos y Analistas Latinoamericanos cruzó dos umbrales de naturaleza distinta pero de significado convergente: uno en el sistema multilateral, otro en el ámbito académico europeo.

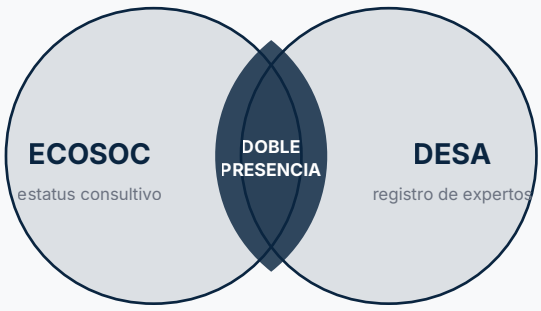
## 01 JULIO 2026 · NACIONES UNIDAS

## Doble presencia ante el sistema multilateral



Sede de las Naciones Unidas, Nueva York.

REAL fue aceptada en la base de datos de organizaciones con estatus consultivo del Departamento de Asuntos Económicos y Sociales de las Naciones Unidas —DESA, por sus siglas en inglés—, en su sección de Sociedad Civil e Inclusión Social. El registro se suma al estatus consultivo que la red ya mantenía ante el Consejo Económico y Social, el ECOSOC.




Dos vías institucionales ante el sistema de Naciones Unidas

La consecuencia práctica es una doble presencia institucional. Cada vía habilita canales distintos: el estatus ante el ECOSOC otorga voz en el órgano que coordina la labor económica y social del sistema, mientras que la inscripción ante DESA sitúa a la red en el circuito operativo donde se preparan consultas, se convocan expertos y se elaboran los insumos técnicos que después alimentan las decisiones intergubernamentales.

LO QUE CAMBIA

*La red pasa de comentar la agenda multilateral a poder intervenir en su formulación.*

## 02 AGOSTO 2026 · COOPERACIÓN ACADÉMICA

# Una maestría propia en inteligencia electoral


Convenio Específico de Cooperación Académica entre REAL y el Instituto Europeo Campus Stellae.

REAL suscribió un Convenio Específico de Cooperación Académica con el Instituto Europeo Campus Stellae para el desarrollo conjunto de la Maestría en Inteligencia Electoral, un programa internacional dictado íntegramente en línea.

**REAL APORTA**
Diseño académico integral · Plan de estudios · Contenidos · Selección y coordinación del claustro docente · Gestión académica y operativa

**CAMPUS STELLAE APORTA**
Aval académico institucional · Verificación de estándares de calidad · Aprobación formal del programa · Expedición de diplomas, certificados y títulos propios

REAL no adapta un programa ajeno ni presta su nombre a una oferta preexistente: define qué se enseña, cómo se enseña y quién lo enseña. Campus Stellae certifica que ese diseño cumple estándares europeos.

LO QUE CAMBIA

*La red deja de ser únicamente productora de análisis para convertirse también en formadora de quienes lo producirán.*

Una organización de análisis solo tiene dos formas de aumentar su impacto: llevar su conocimiento a los espacios donde se decide, o transmitirlo a quienes decidirán después. La presencia ante Naciones Unidas atiende lo primero. La maestría con Campus Stellae atiende lo segundo.

| 13 | 1 | 1 |
| --- | --- | --- |
| países | sistema multilateral | aval académico europeo |

# La inteligencia es conocimiento, y conocimiento para la acción.

Sherman Kent, Strategic Intelligence for American World Policy, 1949

Esta edición reunió seis análisis sobre geopolítica, inteligencia estratégica, ciberseguridad, salud digital y seguridad patrimonial, firmados por expertos de la red REAL en Argentina, México y Perú. El próximo número continuará explorando cómo la región produce, protege y aplica el conocimiento estratégico en un entorno global en recomposición.

N.º 03 · JULIO–SEPTIEMBRE 2026

REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

# Revista para profesionales de la Defensa, Seguridad, Desarrollo y Democracia

Publicado el 21 de agosto de 2026
Editado en Washington, D.C.
real-oneamerica.org

N.º 02 · ABRIL–JUNIO 2026