

CLAVES CEEYPP — PANORAMA PARA LA DECISIÓN · N° 15

Prevención de ataques a infraestructuras críticas públicas y privadas en Ecuador: un modelo de protección activa en el contexto del conflicto armado interno

Michael Chong Pineda — IA Academy

Centro de Estudios en Estrategia y Políticas Públicas — Octubre de 2026

Resumen

La declaratoria de conflicto armado interno en Ecuador, formalizada mediante el Decreto Ejecutivo 111 de enero de 2024, trasladó parte de la confrontación entre el Estado y las organizaciones criminales al terreno de la infraestructura. Puentes, redes eléctricas, ductos, nodos de telecomunicaciones y corredores logísticos han pasado a ser, a la vez, objetivos de represalia, instrumentos de presión y variables de la gobernabilidad. Este ensayo sostiene que la prevención de ataques a infraestructuras críticas, públicas y privadas, exige abandonar el paradigma de la custodia estática y adoptar un modelo de protección activa, basado en riesgo, integrado entre sectores y sostenido por una gobernanza compartida. A partir de una revisión documental de fuentes normativas, periodísticas e institucionales del periodo 2024–2026, el texto analiza el patrón de amenaza, identifica las vulnerabilidades específicas de los sectores energético e hidrocarburífero, de telecomunicaciones y vial, y propone una arquitectura de cinco capas (conocimiento del riesgo, disuasión y protección física, detección tecnológica, respuesta interoperable y resiliencia operativa) acompañada de una hoja de ruta y de indicadores de desempeño. Se concluye que la ventaja del sabotaje asimétrico reside en la asimetría de costos y en la fragmentación institucional, y que ambas pueden reducirse mediante priorización rigurosa, interoperabilidad y cooperación público-privada con salvaguardas jurídicas explícitas.

Palabras clave: infraestructura crítica, sabotaje asimétrico, protección activa, resiliencia, colaboración público-privada, Ecuador

1. Introducción

Los Estados modernos se sostienen sobre redes que casi nunca se ven hasta que fallan. La electricidad que mueve bombas, hospitales y centros de datos; los ductos que llevan crudo y combustibles desde la Amazonía hasta la costa y las ciudades; los cables y torres por los que circulan las comunicaciones del comando civil y militar; los puentes que conectan puertos con zonas productivas y regiones enteras con el resto del país: todo ello constituye lo que la literatura de seguridad denomina infraestructura crítica. Su rasgo definitorio no es el valor del activo físico, sino el costo sistémico de su interrupción. Un transformador, un tramo de oleoducto o un pilar de puente pueden costar relativamente poco; el daño que su pérdida produce en cadena puede ser desproporcionadamente alto.

Ecuador ofrece hoy un caso particularmente instructivo. En enero de 2024, tras una oleada de ataques que incluyó la toma armada de un canal de televisión en Guayaquil, motines simultáneos en cárceles y atentados con explosivos en varias provincias, el presidente Daniel Noboa declaró la existencia de un conflicto armado interno y ordenó a las Fuerzas Armadas ejecutar operaciones militares para neutralizar a una veintena de organizaciones criminales (Vanguardia, 2024). Desde entonces, el Estado ha incrementado la presión operativa sobre estas estructuras, y estas han respondido con una combinación de violencia territorial, extorsión y acciones contra bienes de uso público. La lectura que realizan las propias autoridades es consistente: los atentados contra infraestructura son, con frecuencia, represalias por operaciones militares y policiales, como ocurrió en octubre de 2025, cuando un coche bomba en Guayaquil fue seguido, en menos de veinticuatro horas, por explosiones en dos puentes de las provincias de Guayas y Azuay (Reuters, 2025b; Noticias RCN, 2025).

Este patrón responde a una lógica doctrinal reconocible. Cuando un actor no estatal no puede igualar la capacidad de combate del Estado, desplaza el conflicto hacia terrenos donde el costo de atacar es bajo y el costo de defender es alto. La infraestructura es precisamente ese terreno: es extensa, está distribuida, con frecuencia carece de vigilancia permanente y su interrupción produce efectos políticos y económicos inmediatos. Además, obliga a dispersar fuerzas. Cada kilómetro de ducto, cada subestación y cada puente que debe custodiarse es un efectivo que no participa en operaciones ofensivas. La amenaza, por tanto, no es

solo el daño material, sino la distorsión que impone sobre la estrategia del Estado.

El problema de investigación que orienta este ensayo puede formularse así: ¿cómo prevenir, de manera eficaz y jurídicamente responsable, los ataques de grupos armados irregulares y organizaciones criminales contra infraestructuras críticas en Ecuador, considerando que gran parte de esos activos pertenece o es operada por el sector privado y que los recursos de seguridad del Estado son finitos? La tesis que se defiende es que la respuesta no reside en multiplicar guardias, sino en rediseñar la protección como un sistema activo y priorizado, que combine inteligencia, tecnología de detección, respuesta interoperable y resiliencia, y que se gobierne mediante acuerdos explícitos entre el sector público y el privado.

Por razones de responsabilidad, el texto permanece en el nivel doctrinal y de política pública: no describe métodos de ataque ni detalles operativos susceptibles de ser utilizados con fines hostiles.

2. Marco conceptual

Infraestructura crítica y sistemas de sistemas

La infraestructura crítica suele definirse como el conjunto de instalaciones, redes y servicios cuya destrucción o interrupción tendría un impacto grave sobre la salud, la seguridad, la economía o el funcionamiento del Estado. La Constitución ecuatoriana no emplea esa expresión, pero ofrece un equivalente funcional en la categoría de sectores estratégicos, entre los que figuran la energía en todas sus formas, las telecomunicaciones, el transporte y la refinación de hidrocarburos y los recursos naturales no renovables, cuya administración, regulación y control el Estado se reserva (Constitución de la República del Ecuador, 2008, art. 313). Esta equivalencia es útil, pero insuficiente: un puente concesionado o una red de fibra óptica de un operador privado pueden ser críticos para la continuidad nacional sin figurar en ninguna lista de sectores reservados.

El avance conceptual más influyente de las últimas décadas consiste en entender estas infraestructuras no como activos aislados, sino como un sistema de sistemas interdependientes. Rinaldi, Peerenboom y Kelly (2001) mostraron que las infraestructuras se acoplan de manera física, cibernética, geográfica y lógica, de modo que una falla en un sector puede propagarse a otros con rapidez y de formas difíciles de anticipar. La electricidad alimenta el bombeo de crudo y las estaciones de telecomunicaciones; las telecomunicaciones coordinan el despacho eléctrico y el control de ductos; las vías permiten el acceso de las cuadrillas que reparan ambos. Perrow (1984), desde la sociología de las organizaciones, advirtió que los sistemas estrechamente acoplados y complejos tienden a producir accidentes que no son anomalías, sino propiedades normales de su diseño. Para la seguridad, el corolario es incómodo: un adversario no necesita comprender toda la red; le basta identificar los pocos nodos cuya falla se transmite con mayor fuerza.

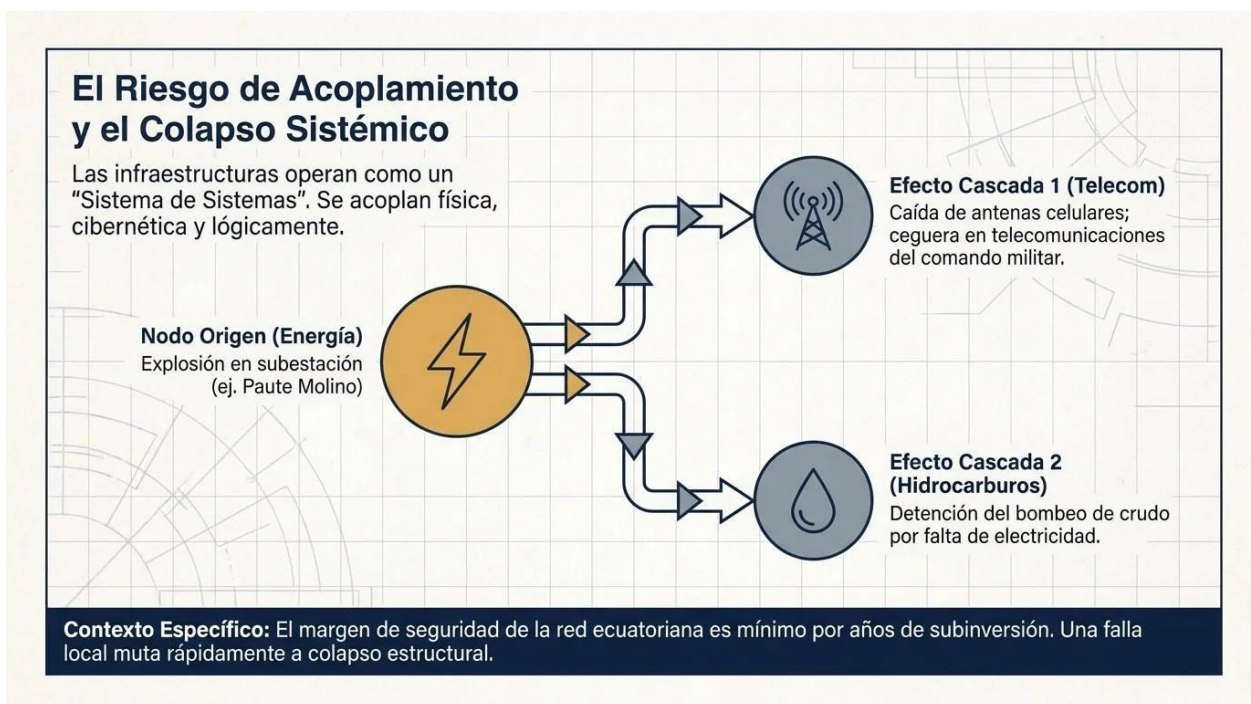
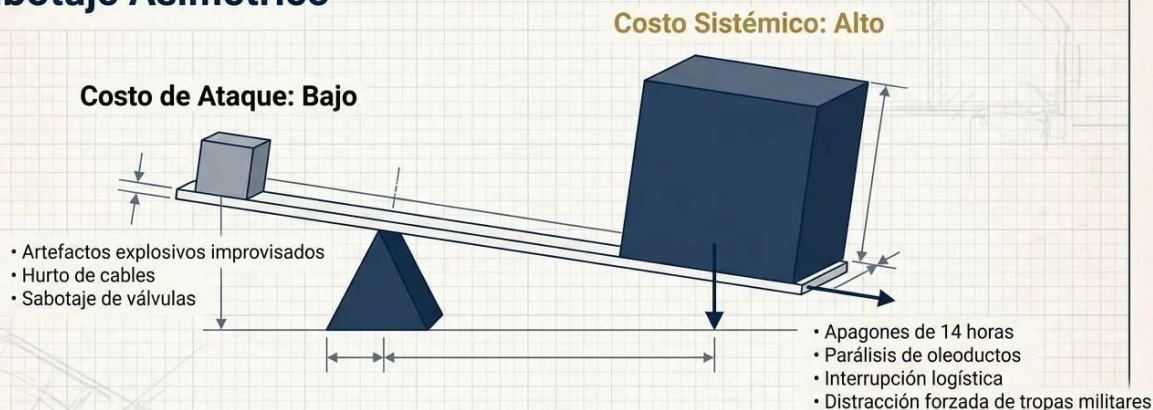


Figura 1. Efecto cascada por acoplamiento entre sistemas de infraestructura. Nota. Elaboración propia.

Sabotaje asimétrico y lógica de la agresión

El sabotaje asimétrico puede entenderse como el uso de medios de bajo costo y alta selectividad para producir efectos estratégicos desproporcionados sobre un adversario más fuerte. Su eficacia descansa en tres condiciones: la extensión territorial de lo que se debe proteger, la visibilidad y vulnerabilidad de ciertos nodos, y la capacidad de producir un efecto político, sea de intimidación, de presión negociadora o de distracción de fuerzas. Esta lógica no es nueva en América Latina. Los ataques recurrentes contra oleoductos en otros países de la región, las perforaciones ilegales para la sustracción de combustible y los bloqueos de ejes viales como instrumento de presión han formado parte de repertorios de acción de actores armados y criminales durante décadas. Lo que cambia en el caso ecuatoriano es la combinación de una criminalidad transnacional con capacidad financiera, acceso a explosivos y control territorial parcial, con un Estado que ha elevado deliberadamente el nivel de confrontación.

La Ecuación del Sabotaje Asimétrico



El rasgo definitorio de la infraestructura crítica no es el *valor físico del activo*, sino el *costo de su interrupción*.

Figura 2. Asimetría de costos en el sabotaje a infraestructura crítica. Nota. Elaboración propia.

Defensa en profundidad, protección activa y resiliencia

La literatura de protección física ofrece una síntesis operativa clara: un sistema de protección eficaz debe detectar la intrusión, retrasarla el tiempo suficiente y permitir una respuesta que llegue antes de que el adversario complete su objetivo (García, 2007). Esa secuencia de detección, retardo y respuesta implica que ninguna barrera, por sólida que sea, protege por sí sola; lo que protege es la relación entre el tiempo que el adversario necesita y el tiempo que la respuesta tarda en llegar. Una cerca perimetral sin detección ni respuesta es solo un retraso gratuito. Una cámara sin nadie que pueda actuar sobre su alerta es un archivo de evidencia.

La protección activa, que es el concepto central de este ensayo, extiende esa lógica con tres rasgos. Primero, la vigilancia es continua y automatizada en lo rutinario, de modo que la atención humana se reserve para lo anómalo. Segundo, la información fluye entre operadores y fuerzas de seguridad en tiempo real, no mediante informes diferidos. Tercero, la respuesta es proporcionada y escalonada: no toda alerta exige una intervención armada, y diferenciar una falsa alarma de una incursión es en sí mismo un objetivo de diseño.

El Fracaso del Status Quo vs. El Modelo Activo		
	Status Quo: Custodia Estática	La Solución: Protección Activa
Enfoque Estratégico	Cubrir territorio ciegamente (kilómetros de ductos, todos los puentes).	Proteger las consecuencias (nodos críticos donde la falla genera colapso).
Dependencia	Altamente dependiente del recurso humano (guardias, tropas estacionarias).	Analítica automatizada e inteligencia distribuida.
Mecanismo de Reacción	Aislada y tardía.	Respuesta interoperable, graduada y en tiempo real.
Sostenibilidad	Agota financieramente al Estado y debilita operaciones ofensivas.	Escalable, económica y de gobernanza compartida.

Figura 3. Custodia estática frente a protección activa. Nota. Elaboración propia.

Finalmente, la protección debe complementarse con resiliencia, entendida como la capacidad de resistir, absorber, recuperarse y adaptarse ante un evento adverso (U.S. Department of Homeland Security, 2013). La razón es simple: ninguna estrategia de protección alcanza el riesgo cero. Si se acepta que algunos ataques ocurrirán, la pregunta decisiva es cuánto tarda el sistema en restablecer el servicio y qué redundancias permiten que la interrupción no se convierta en colapso. Esta orientación es la que inspira marcos como el de la Unión Europea, que combina obligaciones de resiliencia para entidades críticas con requisitos de seguridad de redes y sistemas de información (Directiva (UE) 2022/2557; Directiva (UE) 2022/2555).

3. El patrón de amenaza en Ecuador, 2024–2026

Del estallido de 2024 a la escalada de 2025

La evidencia pública permite reconstruir una secuencia de tres momentos. En el primero, enero de 2024, la declaratoria del conflicto interno ocurrió tras ataques simultáneos de alto impacto simbólico. Las Fuerzas Armadas aseguraron puntos críticos y estratégicos del país con el propósito explícito de evitar ataques que comprometieran la estabilidad nacional (Eje Central, 2024). Durante los primeros seis días el Gobierno informó de 1.534 detenidos, 158 de ellos por presunto terrorismo, y reportó trece atentados contra infraestructuras públicas y privadas (Primicias, 2024a). Al cabo de veintiséis días, la cifra de atentados contra infraestructura que el Gobierno comunicaba seguía siendo de trece, mientras los detenidos superaban los 5.900 (Primicias, 2024b). Este dato, tomado con la cautela que merecen las cifras oficiales, sugiere que la fase inicial combinó una reacción masiva del Estado con un número relativamente acotado de ataques contra infraestructura, lo que apunta a un efecto disuasivo temporal del despliegue.

El segundo momento corresponde al deterioro sostenido de la seguridad durante 2025. Según cifras oficiales, hasta octubre de ese año el país contabilizaba 7.553 asesinatos, por encima de los 7.063 registrados en todo 2024, y una organización internacional de monitoreo de conflictos incluyó a Ecuador en su lista de seguimiento para 2026 por el riesgo de nuevas escaladas (Vistazo, 2025a). Es decir, la presión militar no redujo, por sí sola, la capacidad de daño de las organizaciones criminales, que compiten por el control de economías ilícitas como la extorsión, el narcotráfico y la minería ilegal.

El tercer momento es la mutación táctica hacia la infraestructura. En marzo de 2025, dos artefactos explosivos en Machala, uno de ellos contra un puente de la circunvalación norte, dañaron líneas y equipos de media tensión y dejaron sin electricidad varios sectores de la ciudad (El Mercurio, 2025). En octubre de 2025, el coche bomba de Guayaquil y las explosiones en los puentes de Churute, en Guayas, y de la vía que conecta Azuay con El Oro fueron atribuidos por el ministro del Interior a una represalia por las operaciones contra la minería ilegal en Imbabura, con presunta responsabilidad de Los Lobos, organización designada como terrorista por Estados Unidos (Reuters, 2025a; Primicias, 2025a). El ministro de Infraestructura señaló que el propósito de las explosiones en los puentes era interrumpir el tránsito (Reuters, 2025b). Estados Unidos condenó los hechos y los describió como ataques dirigidos contra infraestructura clave (Primicias, 2025a). Un informe internacional de seguimiento de la democracia señaló, para ese mes, al menos veintisiete muertos en una serie de atentados que evidencian un uso creciente de tácticas terroristas por parte de grupos criminales (International IDEA, 2025).

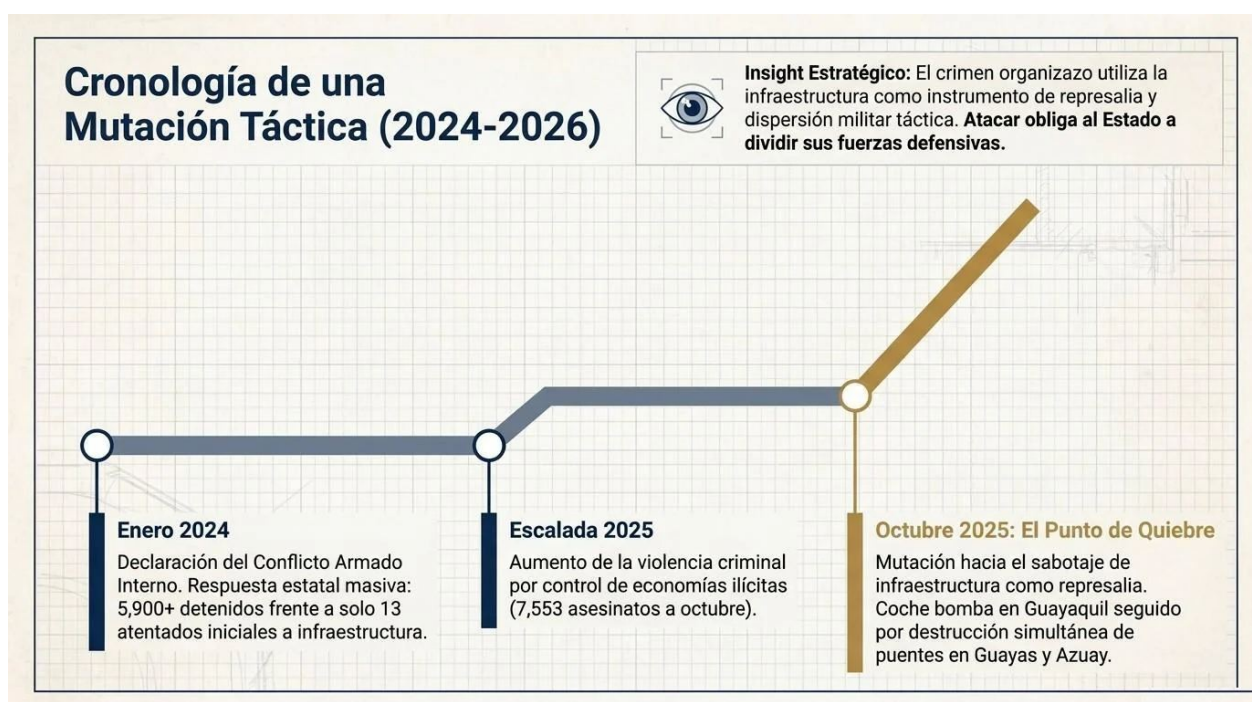


Figura 4. Cronología de la mutación táctica hacia la infraestructura, 2024–2026. Nota. Elaboración propia.

Lectura estratégica del patrón

De esta secuencia se desprenden cuatro observaciones relevantes para la prevención. La primera es la correlación entre presión estatal y respuesta sobre infraestructura: los atentados no son aleatorios, sino que siguen a operaciones concretas. Esto abre una ventana de anticipación, pues el calendario operativo del Estado es también un indicador de riesgo para los activos del entorno. La segunda es la selección de nodos de impacto vial. Los puentes tienen la ventaja, para el agresor, de ser localizables, de concentrar la función de conectividad en un punto y de exigir reparaciones lentas y costosas. La tercera es la dimensión multisectorial: un mismo evento puede afectar vías, energía y comunicaciones, como ocurrió en Machala. La cuarta es la convergencia con delitos de oportunidad, como el hurto de cables y combustible, que degradan los mismos activos con motivaciones distintas, pero que, al ser tolerados, normalizan la presencia de actores ilegales en torno a la infraestructura.

A este panorama se suma una vulnerabilidad que no es obra de ningún adversario: la fragilidad estructural de varios sistemas. Entre 2024 y 2026, Ecuador experimentó racionamientos eléctricos de hasta catorce horas diarias (Vistazo, 2025b), apagones nacionales no programados y una advertencia explícita del operador del

sistema sobre su estado degradado por años de subinversión (Primicias, s. f.). La implicación es que el margen de seguridad frente a un acto hostil es menor que en un sistema robusto: un daño que otra red absorbería con normalidad puede aquí producir un colapso. La prevención de ataques y la mejora de la confiabilidad técnica no son, por tanto, agendas separadas.

4. Análisis sectorial de vulnerabilidades

La Tabla 1 resume, de forma comparada, los tres bloques de infraestructura que el análisis identifica como de mayor exposición, junto con sus principales factores de vulnerabilidad y las líneas de prevención que se desarrollan a continuación.

Tabla 1. Exposición sectorial y líneas de prevención.

Sector	Activos críticos	Principales vulnerabilidades	Líneas de prevención
Energía e hidrocarburos	SOTE, OCP y poliducto Shushufindi–Quito; subestaciones de transmisión; centrales hidroeléctricas	Corredores compartidos en la Amazonía; extensión lineal de difícil vigilancia; perforaciones clandestinas; sistema eléctrico degradado y con baja redundancia; demoras en el cierre de válvulas	Priorizar los tramos compartidos; vigilancia aérea con sensores térmicos; integrar alarmas técnicas y de seguridad; cierre automático de válvulas; repuestos críticos y variantes de trazado
Telecomunicaciones y nodos de datos	Torres, fibra óptica, centros de datos y estaciones de cable submarino	Hurto de cobre y vandalismo; acceso físico a los sitios; dependencia de energía y de rutas únicas; riesgo para las comunicaciones de mando y control	Control de acceso y alarmas de apertura; anillos y rutas redundantes; respaldo energético; reporte en tiempo real a las fuerzas de seguridad; cumplimiento de la ley de ciberseguridad
Infraestructura vial y logística	Puentes principales, ejes troncales y nodos intermodales	Estructuras localizables y de reparación lenta; pocos corredores alternativos; uso como instrumento de aislamiento táctico	Caracterizar la criticidad de los puentes; vigilar los nodos prioritarios; planificar desvíos y puentes provisionales; canal directo entre concesionaria y fuerza pública

Nota. Elaboración propia con base en las fuentes citadas en el texto.

Energía e hidrocarburos

El sector energético concentra los activos de mayor valor sistémico. En materia de hidrocarburos, el Sistema de Oleoducto Transecuatoriano (SOTE), de propiedad estatal, transporta aproximadamente el 59 % del crudo extraído en el país, mientras que el 41 % restante circula por el oleoducto privado OCP (Primicias, 2025b). Ambos comparten parcialmente su corredor, y el poliducto Shushufindi–Quito discurre en la misma región amazónica. Esa concentración geográfica es una vulnerabilidad en sí misma: un evento localizado puede afectar simultáneamente varias líneas. La experiencia reciente lo ilustra con claridad, aunque en un registro no hostil. A comienzos de julio de 2025, la erosión regresiva del río Loco, en Napo, obligó a suspender el bombeo en el OCP el 1 de julio y provocó roturas y derrames en el SOTE, con paralizaciones de varias semanas y la necesidad de construir variantes de trazado (Primicias, 2025b; El Universo, s. f.). Si una causa natural logró detener simultáneamente los dos ductos principales, un acto deliberado en un tramo equivalente tendría un efecto comparable.

Esta lección es doble. Por un lado, la planificación de protección debe identificar los tramos de corredor compartido como zonas de máxima prioridad. Por otro, la capacidad de respuesta técnica importa tanto como la de seguridad: tras una rotura ocurrida en Quinindé en marzo de 2025, el propio gerente de Petroecuador reconoció que la empresa demoró casi media hora en cerrar válvulas y confirmar el evento (Primicias, 2025c). En un escenario hostil, esos minutos significan volumen derramado, daño ambiental y presión social. A ello se suma un fenómeno de baja intensidad pero alta frecuencia: las perforaciones clandestinas en el SOTE, que Petroecuador ha confirmado como causa de derrames y que combinan delito de oportunidad con riesgo ambiental (Primicias, 2025d).

En el subsector eléctrico, la vulnerabilidad se concentra en las subestaciones de transmisión, las líneas troncales y los grandes complejos hidroeléctricos. En septiembre de 2024, tras un apagón atribuido a una falla humana, el presidente ordenó al Bloque de Seguridad operar y reforzar la seguridad de las hidroeléctricas más importantes, e incluso capacitar a personal policial y militar para apoyar la operación de las centrales; el Gobierno recordó que los atentados contra infraestructura de sectores estratégicos tienen pena de siete a diez años de prisión (Primicias, 2024c). El 30 de junio de 2026, una explosión reportada en la subestación Paute Molino a las 02:07 provocó la salida del complejo hidroeléctrico Paute y obligó a desconexiones programadas en varias provincias, mientras Celec y el operador del sistema activaban protocolos de protección (El Diario, 2026). Las fuentes consultadas no establecen la causa del evento, y este ensayo no la atribuye; pero el episodio demuestra que un único nodo puede dejar fuera a la mayor central del país y que la distancia entre una falla técnica y un ataque, desde el punto de vista del impacto, es mínima. Por eso la protección debe diseñarse para la consecuencia, no para la causa.

Telecomunicaciones y nodos de datos

En telecomunicaciones, la amenaza más frecuente no proviene de grupos armados, sino del hurto de cobre y del vandalismo. Un estudio regional del Centro de Estudios de Telecomunicaciones de América Latina concluyó que el robo y el vandalismo de infraestructura son un problema estructural en catorce países; entre el 40 % y el 65 % de los casos revisados involucraban cables de cobre o hurtos de cable sin especificar, y para Ecuador se documentaron pérdidas cercanas a 1,7 millones de dólares en la provincia de Pichincha (Torres Alcocer y Carrasco Muro, 2026). Los autores observan, además, que muchos incidentes se producen porque los ladrones confunden fibra óptica con cobre. Para la seguridad nacional, la relevancia de este fenómeno no radica en el monto, sino en que revela la facilidad de acceso físico a nodos de la red y la existencia de mercados secundarios que absorben los materiales sustraídos.

El riesgo hostil es cualitativamente distinto y más grave. Los episodios de vandalismo comunitario, como el ocurrido en diciembre de 2021 en Cotopaxi, que dejó sin servicio a más de dieciocho mil usuarios durante varios días y cuya reparación se demoró porque no se permitió el ingreso de los técnicos (DPL News, 2021), muestran que la dimensión social del acceso al territorio es decisiva: un nodo físicamente intacto es inútil si el personal que debe repararlo no puede llegar. Más allá de las torres y la fibra terrestre, los centros de datos y las estaciones de aterrizaje de cable submarino constituyen la primera milla de la conectividad internacional. Ecuador cuenta con cuatro sistemas de cable submarino en operación (Expreso, s. f.), y América Latina está conectada por más de ochenta, cuya protección los autores citados consideran una cuestión estratégica creciente (Torres Alcocer y Carrasco Muro, 2026). Un ataque exitoso a estos puntos afectaría no solo a la población civil, sino a las comunicaciones de mando, control, inteligencia y alerta temprana de las propias fuerzas de seguridad.

Infraestructura vial y logística

La infraestructura vial es, hasta ahora, el sector donde el patrón hostil resulta más visible. Los puentes concentran la función de conectividad en estructuras localizables, de reparación lenta y con alternativas limitadas de desvío. Los atentados de octubre de 2025 contra puentes en Guayas y en la conexión entre Azuay y El Oro causaron daños en la base de sus pilares y obligaron a suspender el tránsito (Uno TV, 2025; Noticias RCN, 2025). La concesionaria de la vía calificó uno de los hechos como un presunto atentado terrorista y cerró el tramo mientras se realizaban inspecciones técnicas (Primicias, 2025e). La lección es que la protección del sector no puede recaer solo en el Estado: el operador privado fue el primero en detectar, comunicar y gestionar el evento.

5. Un modelo de protección activa en cinco capas

La evidencia revisada sugiere que la protección de infraestructura crítica en Ecuador enfrenta un problema de diseño antes que de cantidad. Custodiar todo es imposible; custodiar sin criterio es ineficiente. El modelo que se propone organiza la prevención en cinco capas encadenadas, cada una de las cuales reduce la probabilidad o el impacto de un ataque y se apoya en las demás. Su lógica es la de la defensa en profundidad: ninguna capa es suficiente, pero su combinación eleva el costo y el riesgo para el agresor y reduce el tiempo disponible para que complete su objetivo.

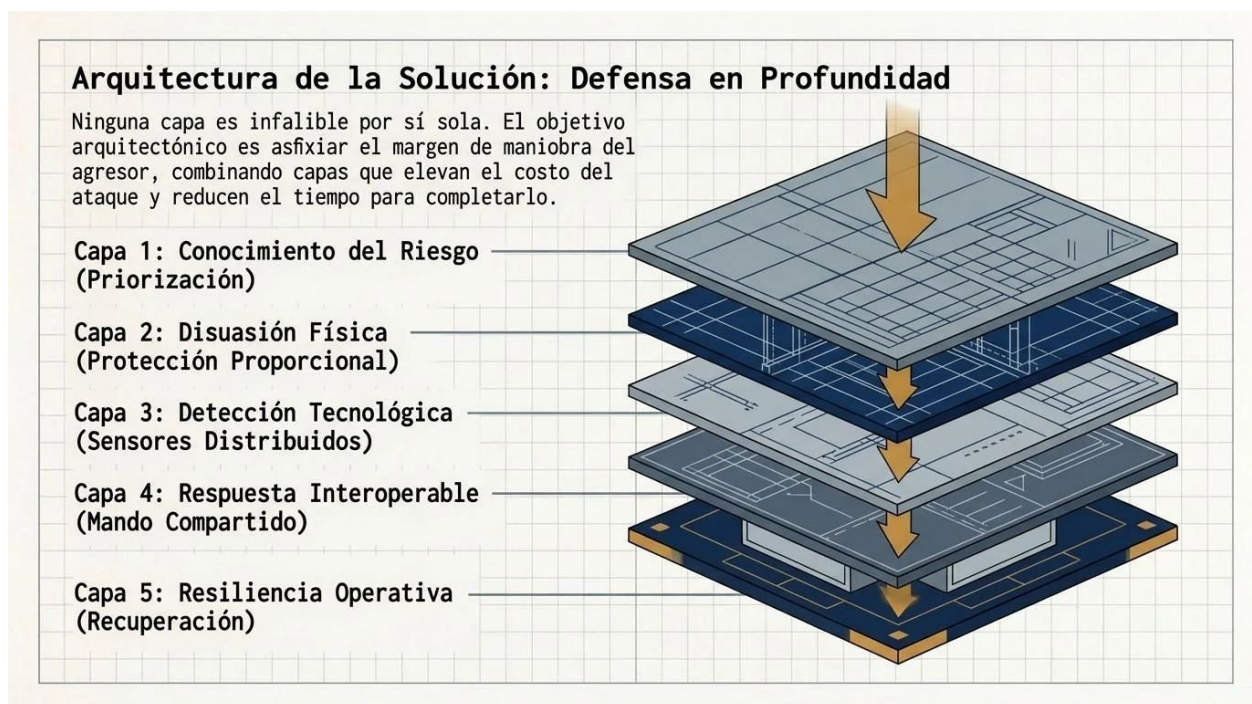


Figura 5. Arquitectura de defensa en profundidad en cinco capas. Nota. Elaboración propia.

Primera capa: conocimiento del riesgo y priorización

Toda estrategia de protección comienza por saber qué proteger primero. Ello exige un inventario nacional de activos críticos, público-privado, clasificado por criticidad sistémica y no solo por propiedad o valor contable. La metodología recomendable combina tres variables: la consecuencia de la pérdida del activo (población afectada, duración, efecto en cascada sobre otros sectores), su vulnerabilidad (exposición, accesibilidad, redundancia disponible) y la amenaza (actores presentes, historial de incidentes, correlación con operaciones estatales). El resultado debería ser un número reducido de nodos de máxima prioridad, para los cuales se justifica una protección reforzada, y un conjunto más amplio de activos de segunda y tercera categoría, con medidas proporcionadas.

Esta capa tiene un componente de inteligencia que merece ser subrayado. Dado que los ataques recientes han seguido a operaciones estatales concretas, la planificación operativa de las Fuerzas Armadas y la Policía debería incorporar, como práctica estándar, una evaluación de riesgo de represalia sobre la infraestructura del área de influencia, antes de ejecutar operaciones de gran escala. Ello equivale a tratar las infraestructuras vecinas como parte del teatro de operaciones, y a anticipar refuerzos temporales de vigilancia y de capacidad de reparación. Marcos internacionales de gestión de riesgo, como la norma ISO 31000, ofrecen una estructura metodológica adecuada para formalizar este proceso (International Organization for Standardization [ISO], 2018).

Segunda capa: disuasión y protección física proporcionada

La segunda capa busca elevar el costo del ataque y reducir su atractivo. Incluye el endurecimiento de los puntos de acceso, el control de perímetros en los nodos de máxima prioridad, la protección de estructuras

singulares como pilares, apoyos y cámaras de válvulas, y la gestión del entorno inmediato, que con frecuencia es más decisivo que la infraestructura misma. A diferencia de los enfoques que buscan blindar todo, aquí el principio es la proporcionalidad: un puente secundario en una ruta con alternativas no justifica la misma inversión que un tramo de corredor compartido entre dos oleoductos o una subestación de la que depende un complejo hidroeléctrico.



Figura 6. Capas 1 y 2: conocimiento del riesgo y disuasión física proporcionada. Nota. Elaboración propia.

Tercera capa: detección tecnológica distribuida

La tercera capa es la que mejor ilustra el tránsito hacia la protección activa. Su objetivo es sustituir la vigilancia humana permanente, que no es escalable, por una red de sensores y analítica que detecte anomalías y las traduzca en alertas útiles. En la práctica, se trata de combinar tres familias de tecnología. La primera es la vigilancia perimetral automatizada: cámaras con analítica de video, sensores de movimiento o vibración, barreras y alarmas de acceso en sitios fijos como subestaciones, estaciones de bombeo y estaciones de telecomunicaciones. La segunda son los sistemas aéreos no tripulados de patrullaje, equipados con sensores térmicos y capacidad de procesamiento en el borde, es decir, algoritmos de inteligencia artificial que corren en el propio dispositivo o en una estación local y que permiten reconocer patrones anómalos sin depender de un enlace permanente con un centro de datos. Estos medios resultan especialmente útiles en corredores lineales extensos y de difícil acceso, como los ductos amazónicos, donde la vigilancia terrestre continua es inviable. La tercera es el monitoreo técnico de la propia infraestructura: caídas de presión en ductos, variaciones de carga en subestaciones, apertura de gabinetes y pérdida de enlaces en redes de telecomunicaciones. Estos indicadores operativos, que ya existen en la mayoría de los sistemas de control, suelen estar desvinculados de la función de seguridad. Integrarlos permite detectar un evento por sus efectos aunque el agresor haya eludido los sensores perimetrales.

Dos advertencias son pertinentes. La primera es de eficacia: un sistema de detección que genera un exceso de falsas alarmas se desacredita y es ignorado. La calidad de la analítica y la calibración con el entorno local importan más que la cantidad de sensores. La segunda es de seguridad: los sistemas de detección son a su vez objetivos. Si controlan o alertan sobre infraestructura crítica, deben protegerse con los mismos estándares que se exigen a los sistemas industriales, como las series de normas IEC 62443 para seguridad de sistemas de

automatización y control, y con criterios de ciberseguridad alineados con marcos como el Cybersecurity Framework del NIST (International Electrotechnical Commission [IEC], 2018; National Institute of Standards and Technology [NIST], 2024). Un dron sin cifrado o una cámara con credenciales de fábrica son una puerta de entrada para el adversario, no una barrera.

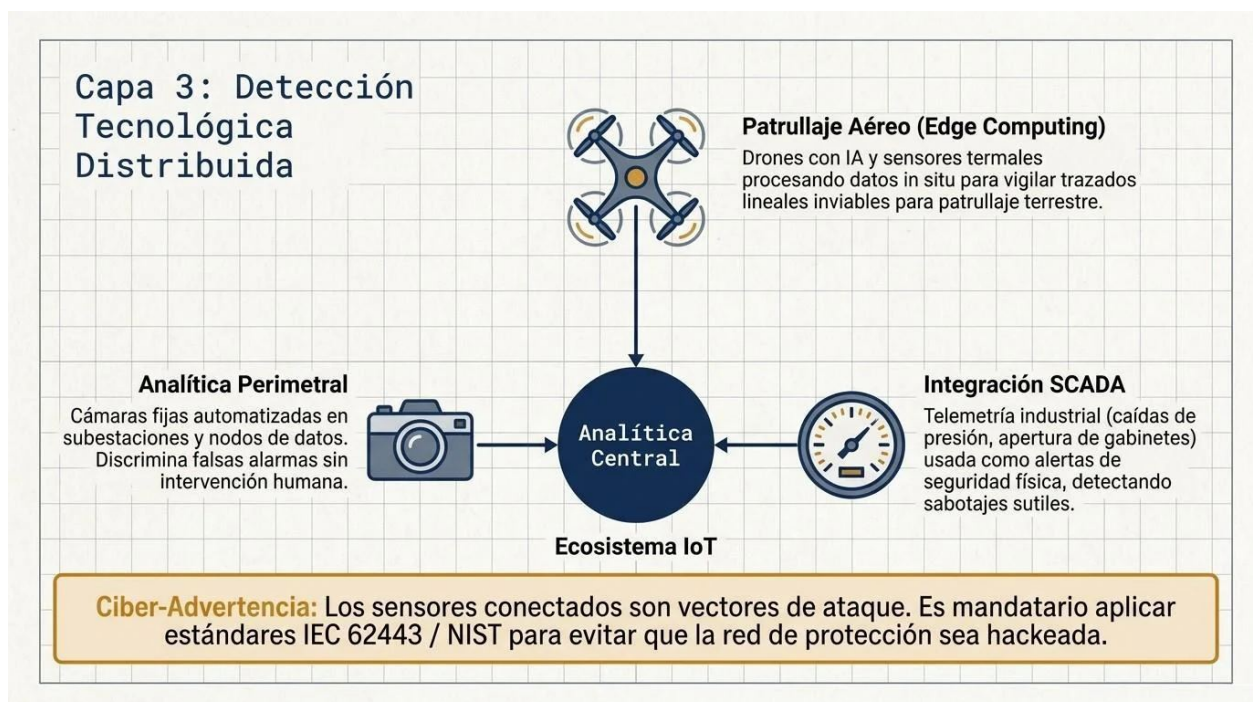


Figura 7. Capa 3: ecosistema de detección tecnológica distribuida. Nota. Elaboración propia.

Cuarta capa: respuesta interoperable y mando táctico compartido

La detección solo tiene valor si desemboca en una respuesta oportuna. La cuarta capa se ocupa de que la información llegue a quien puede actuar, en el formato correcto y con el menor retardo posible. El principal obstáculo en este punto no suele ser tecnológico, sino organizativo: operadores públicos y privados, Fuerzas Armadas, Policía, concesionarias viales, empresas eléctricas y gobiernos locales manejan sistemas, protocolos y lenguajes distintos, de modo que un evento detectado por un operador tarda en convertirse en una acción coordinada. El caso del puente de Churute, donde fue la concesionaria privada quien informó primero y cerró el tránsito mientras se realizaban inspecciones (Primicias, 2025e), muestra que el sector privado ya cumple funciones de primera respuesta sin contar necesariamente con canales formales hacia el sistema de seguridad.

Para resolverlo, la doctrina contemporánea recomienda plataformas de conciencia situacional compartida e interoperable. Sistemas de mando táctico como el Team Awareness Kit y sus variantes (ATAK, WinTAK) permiten que distintos actores visualicen en un mismo mapa la posición de unidades, sensores, alertas e incidentes, intercambien mensajes y coordinen la respuesta con mínimos tiempos de transmisión. Su valor para la protección de infraestructura radica en que reducen la fricción de coordinación entre organizaciones heterogéneas: un operador privado de oleoducto, una brigada militar y una unidad policial pueden trabajar sobre la misma imagen operativa sin integrar sus sistemas internos. Para que ello funcione se requieren tres condiciones: acuerdos previos sobre qué información se comparte y con qué restricciones, protocolos de activación escalonada que distingan entre alerta, verificación y respuesta, y ejercicios periódicos conjuntos que pongan a prueba la cadena completa.

La respuesta debe ser, además, graduada. No toda alerta exige una intervención armada. Un diseño bien concebido distingue al menos tres niveles: verificación remota (mediante un dron o una cámara), respuesta

de proximidad (cuadrillas técnicas, seguridad privada o patrullas policiales) y respuesta de fuerza, reservada a incidentes confirmados de amenaza. Esta gradación protege a las comunidades, reduce el riesgo de incidentes por error y preserva la legitimidad de la fuerza pública.

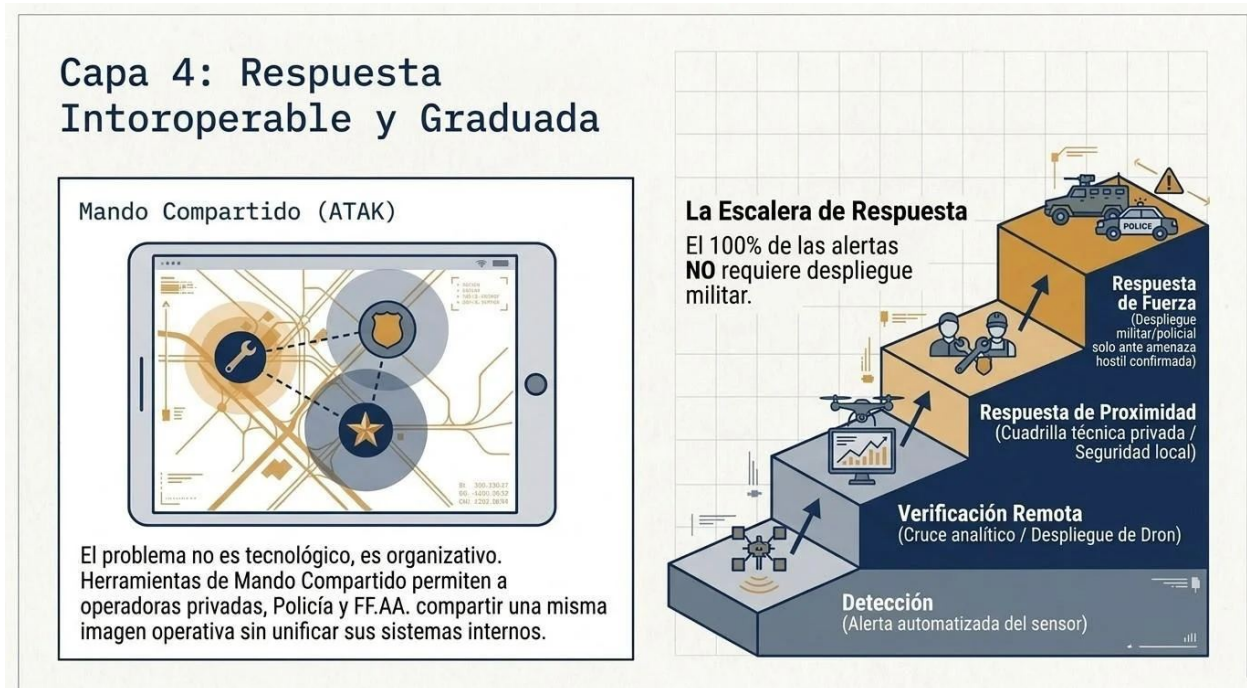


Figura 8. Capa 4: mando compartido y escalera de respuesta graduada. Nota. Elaboración propia.

Quinta capa: resiliencia operativa y recuperación

La última capa asume que algunos ataques tendrán éxito y se propone que no se conviertan en crisis sistémicas. Comprende la redundancia de rutas y suministros, los planes de continuidad operativa, los inventarios estratégicos de repuestos críticos, la capacidad de reparación rápida y los protocolos de comunicación pública. La norma ISO 22301 sobre continuidad del negocio ofrece un marco adecuado para formalizar estos planes en el nivel de la organización (ISO, 2019), mientras que el enfoque de resiliencia de infraestructura crítica del Departamento de Seguridad Nacional de Estados Unidos aporta un marco para el nivel sectorial (U.S. Department of Homeland Security, 2013).

En el contexto ecuatoriano, esta capa tiene aplicaciones concretas. En energía e hidrocarburos, implica contar con variantes de trazado o rutas alternativas, válvulas de cierre automático y respuesta documentada a derrames, cuyo retraso, como mostró el caso de la rotura de Quinindé, multiplica el daño (Primicias, 2025c). En telecomunicaciones, supone anillos de fibra redundantes, diversidad de rutas internacionales y energía de respaldo en los nodos críticos. En el sector vial, requiere identificar con antelación puentes provisionales, desvíos y capacidades de reparación para los nodos de mayor criticidad. En todos los casos, el indicador que importa no es cuántos ataques se evitaron, sino cuánto tarda el servicio esencial en restablecerse.

Capa 5: Resiliencia Operativa y Recuperación

El Cambio de Métrica: El indicador de éxito no es cuántos ataques se evitan, sino cuánto tiempo tarda el restablecimiento del servicio esencial.



Figura 9. Capa 5: curva de resiliencia operativa. Nota. Elaboración propia.

6. Gobernanza y marco normativo

Una arquitectura institucional fragmentada

La principal fuente de vulnerabilidad de la protección de infraestructura crítica en Ecuador no es la falta de normas, sino su dispersión. El país cuenta con un esquema constitucional que reserva los sectores estratégicos al Estado (Constitución de la República del Ecuador, 2008, art. 313), con una Ley de Seguridad Pública y del Estado que faculta al ministro de Defensa a disponer que las Fuerzas Armadas protejan las instalaciones de los sectores estratégicos ante circunstancias críticas (Ley de Seguridad Pública y del Estado, 2009, art. 42; Primicias, 2022), y con un régimen penal que sanciona los atentados contra infraestructura de sectores estratégicos con penas privativas de libertad de siete a diez años (Primicias, 2024c). Sin embargo, la protección concreta se reparte entre ministerios sectoriales, operadores estatales, concesionarias privadas, gobiernos autónomos descentralizados y fuerzas de seguridad, sin un marco único de priorización ni un sistema integrado de intercambio de información.

La Constitución es clara respecto del reparto de funciones: la protección interna y el mantenimiento del orden público corresponden primariamente a la Policía Nacional, mientras que las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial (Constitución de la República del Ecuador, 2008, art. 158). El conflicto armado interno ha modificado en la práctica este equilibrio al habilitar un empleo más amplio de las Fuerzas Armadas, pero una gobernanza sostenible de la protección de infraestructura no puede depender indefinidamente de un régimen excepcional. La protección ordinaria debe descansar en capacidades policiales, privadas y técnicas permanentes, y reservar el componente militar para los nodos y los periodos de mayor riesgo.

La Ley Orgánica para el Fortalecimiento de la Ciberseguridad como precedente

Un avance reciente, aunque centrado en la dimensión digital, ofrece un modelo útil. La Ley Orgánica para el Fortalecimiento de la Ciberseguridad, aprobada por la Asamblea Nacional con 82 votos afirmativos (Teleamazonas, 2026) y vigente desde el 22 de mayo de 2026, establece un marco para proteger la infraestructura crítica digital y garantizar la continuidad de los servicios esenciales (DPL News, 2026). Su

rasgo más relevante para este ensayo es el principio de responsabilidad compartida: la ley distribuye obligaciones entre entidades públicas que administran servicios esenciales, prestadores de servicios digitales y organizaciones privadas cuya actividad impacta de manera directa la continuidad de servicios estratégicos, y excluye, como regla general, a las personas naturales y a los operadores no calificados como críticos (NMS Law, 2026). Establece también obligaciones de gestión de riesgos, medidas técnicas de seguridad y respuesta ante incidentes, y otorga el rol rector al Ministerio de Telecomunicaciones y de la Sociedad de la Información (Defonline, 2026).

La lección que cabe extraer es doble. En lo positivo, el país ha demostrado capacidad de construir un marco de responsabilidad compartida con obligaciones diferenciadas para el sector privado, lo que constituye un precedente transferible a la dimensión física. En lo problemático, el marco cubre la infraestructura digital pero no existe un instrumento equivalente de rango legal para la protección física integrada de la infraestructura crítica, que continúa regulada por disposiciones sectoriales dispersas. Dado que, como se ha visto, los eventos más relevantes combinan daño físico y efectos digitales y viceversa, mantener dos regímenes separados es una fuente de brechas.

Hacia un esquema de colaboración público-privada

Gran parte de los activos críticos pertenece o es operada por empresas privadas o por concesionarias: un oleoducto de capital privado, concesiones viales, operadores de telecomunicaciones, generadoras y distribuidoras mixtas. Esto implica que el Estado no puede proteger lo que no controla ni conoce. Un esquema eficaz de colaboración debería descansar en cinco componentes.

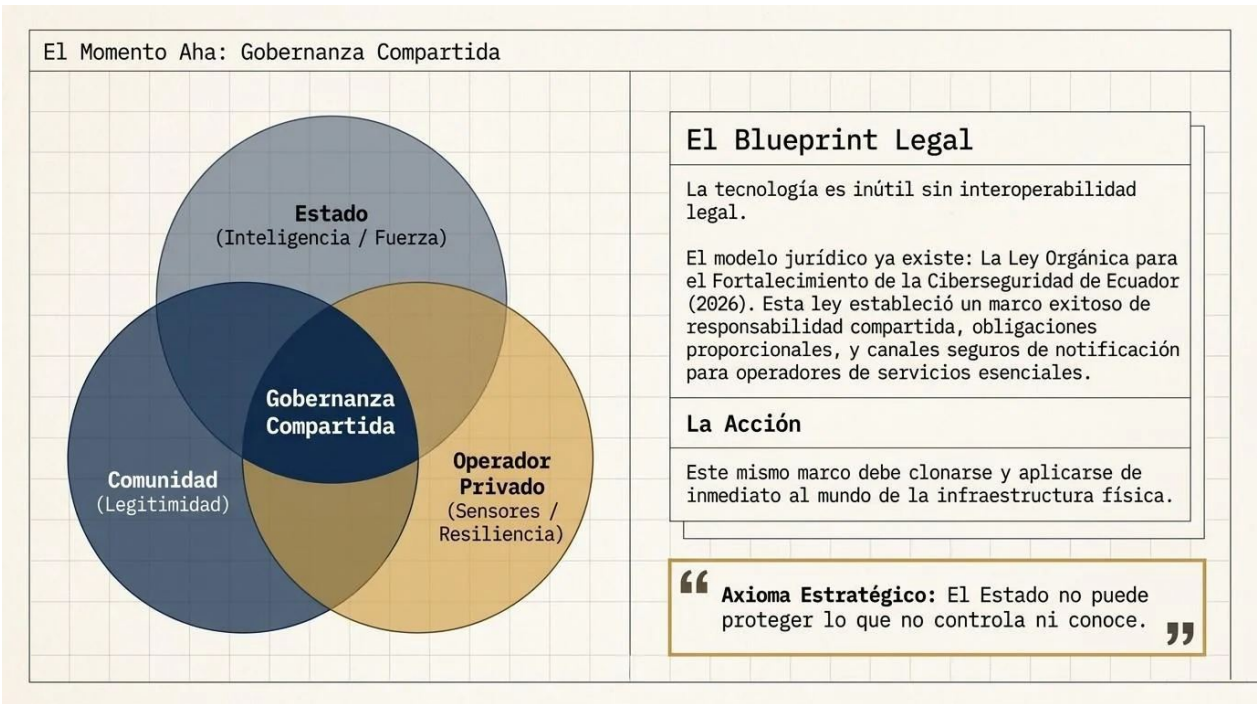


Figura 10. Gobernanza compartida entre Estado, operador privado y comunidad. Nota. Elaboración propia.

El primero es la designación formal de operadores críticos, con criterios transparentes y obligaciones proporcionales, en la línea de lo que ya hace la ley de ciberseguridad para el ámbito digital. El segundo es un régimen de obligaciones mínimas de seguridad física y continuidad, graduadas por criticidad, que incluya planes de protección, ejercicios y notificación obligatoria de incidentes. El tercero es un canal único y seguro de intercambio de información, que permita al sector privado compartir alertas sin temor a sanciones reputacionales o a la filtración de información comercial sensible, y recibir a cambio inteligencia de amenaza procesada por el Estado. El cuarto es un sistema de incentivos: seguros, beneficios fiscales o prioridad de

apoyo estatal para quienes cumplan los estándares. El quinto es un mecanismo de coordinación local, que involucre a gobiernos autónomos descentralizados y a las comunidades del entorno, pues, como evidencia el caso de Cotopaxi, la relación con el territorio determina si los técnicos pueden acceder a reparar lo dañado (DPL News, 2021).

Este último componente subraya una dimensión que los enfoques centrados en la fuerza tienden a subestimar: la legitimidad social de la infraestructura. Los activos que se perciben como ajenos o como fuente de daño ambiental y de exclusión de beneficios son más vulnerables, porque las comunidades del entorno no actúan como aliadas de la protección. Una política preventiva eficaz incluye, por ello, mecanismos de diálogo, empleo local en tareas de vigilancia y mantenimiento, y canales de denuncia confiables, incluyendo protección para quienes los utilicen en contextos de presión criminal.

7. Hoja de ruta e indicadores de desempeño

La implementación del modelo exige secuenciar. Intentar desplegarlo todo de forma simultánea consumiría recursos sin producir resultados visibles. Se propone un horizonte de treinta y seis meses organizado en tres fases, cuyos principales hitos e indicadores se resumen en la Tabla 2.

Tabla 2. Hoja de ruta de implementación a treinta y seis meses.

Fase	Horizonte	Hitos principales	Indicadores de desempeño
1	0–12 meses	Inventario y clasificación de activos críticos; designación de operadores críticos; instancia de coordinación público-privada; pilotos de detección y mando compartido; protocolos de intercambio de información	Porcentaje de activos clasificados; número de operadores designados; ejercicios conjuntos realizados
2	12–24 meses	Ampliación de la cobertura a corredores de segunda prioridad; interoperabilidad entre plataformas; obligaciones mínimas formalizadas; programas de formación	Tiempo medio entre detección y primera respuesta; tasa de falsas alarmas por sensor; porcentaje de operadores que cumplen los estándares
3	24–36 meses	Evaluación independiente; ajuste de la priorización; cooperación internacional; transición hacia capacidades permanentes policiales y privadas	Tiempo medio de restablecimiento del servicio; proporción de comunidades con diálogo activo; reducción de incidentes con afectación del servicio

Nota. Elaboración propia. Los indicadores miden resultados y no actividad.

En la primera fase, de cero a doce meses, el esfuerzo se concentra en la base de conocimiento y en el diseño institucional: inventario nacional y clasificación de activos críticos, designación de operadores críticos, creación o fortalecimiento de una instancia de coordinación interinstitucional con participación privada, y despliegue piloto de detección y mando compartido en un número reducido de nodos de máxima prioridad. Esta fase debe producir, además, protocolos básicos de intercambio de información y los primeros ejercicios conjuntos.

En las fases siguientes, de doce a treinta y seis meses, se amplía la cobertura tecnológica a los corredores de segunda prioridad, se institucionaliza la interoperabilidad entre plataformas, se formalizan las obligaciones mínimas de los operadores críticos y se desarrollan programas de formación de personal técnico y de seguridad, una brecha que el Banco Interamericano de Desarrollo identifica como persistente en materia de ciberseguridad (El Diario, 2025). Hacia el final del horizonte, el énfasis pasa de la instalación a la mejora continua: evaluación independiente, ajuste de la priorización con base en la evidencia y transición gradual de funciones de protección desde el esfuerzo militar excepcional hacia capacidades permanentes policiales y privadas.

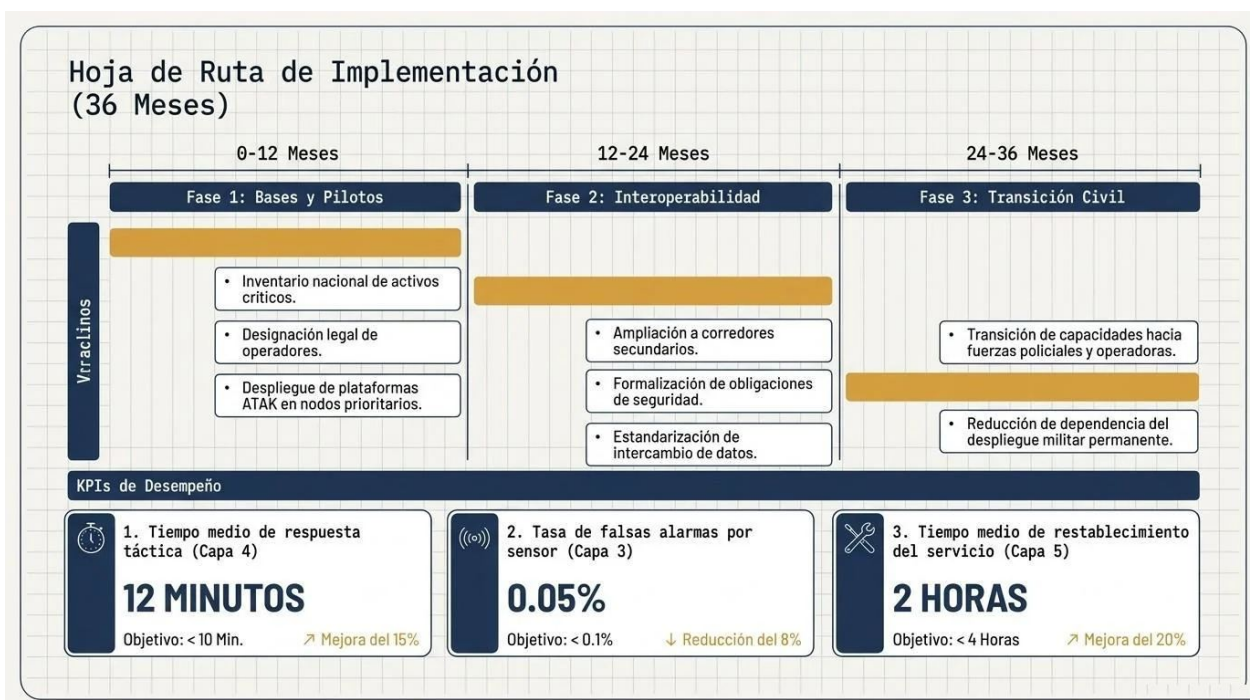


Figura 11. Hoja de ruta de implementación e indicadores de desempeño. Nota. Elaboración propia.

Los indicadores deben medir resultados, no actividad. Cuatro métricas resultan especialmente informativas: el tiempo medio entre detección y llegada de la primera respuesta a nodos de máxima prioridad, la tasa de falsas alarmas por sensor, el tiempo medio de restablecimiento del servicio tras un incidente y la proporción de operadores críticos que cumplen los estándares mínimos y participan en ejercicios conjuntos. A ellas se suma una métrica de legitimidad, como el porcentaje de comunidades del entorno con mecanismos activos de diálogo. La publicación periódica, con las reservas de seguridad necesarias, de un resumen agregado de estos indicadores contribuiría a la rendición de cuentas y a la confianza del sector privado.

PROTECCIÓN ACTIVA DE INFRAESTRUCTURAS CRÍTICAS EN ECUADOR

Ante el conflicto armado interno, Ecuador transita hacia un modelo de protección activa basado en riesgo, detección tecnológica e interoperabilidad público-privada.

LAS 5 CAPAS DE LA PROTECCIÓN ACTIVA



HOJA DE RUTA DE IMPLEMENTACIÓN (36 MESES)

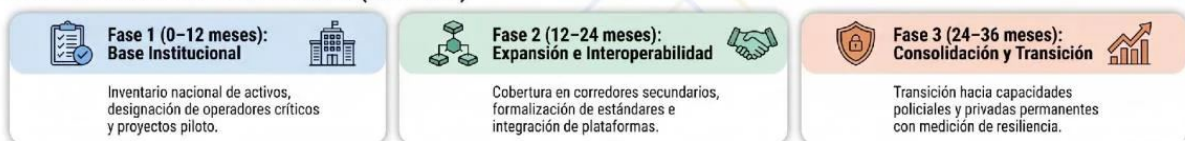


Figura 12. Síntesis visual del modelo de protección activa. Nota. Elaboración propia.

8. Salvaguardas éticas y jurídicas

Un modelo de protección activa que amplía la vigilancia, el uso de sensores y el empleo de la fuerza en el entorno de infraestructuras sensibles plantea riesgos que deben gestionarse desde el diseño. Tres cuestiones merecen atención.



Figura 13. Salvaguardas jurídicas y éticas del modelo. Nota. Elaboración propia.

La primera es la protección de datos personales. Las cámaras con analítica y los drones con sensores capturan imágenes de personas, vehículos y comunidades. La Ley Orgánica de Protección de Datos Personales de 2021 exige principios de finalidad, proporcionalidad y minimización, de modo que los sistemas deben configurarse para limitar la captura y la retención de datos a lo estrictamente necesario, con reglas claras de acceso y plazos de conservación, y con evaluaciones de impacto cuando corresponda. La vigilancia de infraestructura no puede convertirse en un instrumento de vigilancia generalizada de poblaciones.

La segunda es el empleo proporcionado de la fuerza. La conceptualización del conflicto interno como un conflicto armado activa el marco del derecho internacional humanitario, pero no suspende el derecho internacional de los derechos humanos ni los límites constitucionales. La distinción entre combatientes y población civil, los principios de necesidad, proporcionalidad y precaución y el uso progresivo de la fuerza deben traducirse en reglas de enfrentamiento claras para el personal que protege infraestructura, incluidas las empresas de seguridad privada, cuyo entrenamiento y supervisión requieren estándares específicos. La graduación de la respuesta descrita en la cuarta capa es, entre otras cosas, una salvaguarda de este tipo.

La tercera es la seguridad de los propios sistemas. Un dron, una plataforma de mando compartido o una red de sensores comprometidos pueden convertirse en un vector de ataque, de espionaje o de manipulación de la imagen operativa. Todo despliegue debe acompañarse de evaluación de riesgos cibernéticos, cifrado, control de acceso, gestión de proveedores y cadena de suministro confiable, así como de un régimen claro de responsabilidad para operadores públicos y privados. Esta es una dimensión en la que la nueva ley de ciberseguridad ofrece un punto de apoyo normativo (NMS Law, 2026).

Conclusiones

Este ensayo ha sostenido que la prevención de ataques a infraestructuras críticas en Ecuador exige un cambio de paradigma: pasar de la custodia estática y reactiva a un modelo de protección activa, basado en el riesgo, integrado entre sectores y gobernado de forma compartida entre el Estado y el sector privado.

En primer lugar, la evidencia de 2024 a 2026 muestra un patrón de amenaza reconocible. La infraestructura se ha convertido en terreno de represalia y presión; los ataques contra puentes, la afectación de redes eléctricas en contextos de violencia criminal y la persistencia de delitos de oportunidad en telecomunicaciones e hidrocarburos configuran una amenaza real y creciente. A ello se suma una fragilidad estructural, particularmente en el sistema eléctrico, que reduce el margen de seguridad frente a cualquier choque, sea hostil o accidental.

En segundo lugar, la asimetría de costos explica la persistencia de la amenaza, pero también señala las vías para reducirla. Si atacar es barato y defender es caro, la respuesta no es defender todo con el mismo esfuerzo, sino priorizar con rigor, detectar a bajo costo mediante sensores y analítica distribuida, responder de forma graduada e interoperable y asumir la resiliencia como objetivo explícito. El modelo de cinco capas propuesto traduce estas ideas en una arquitectura operativa y en una hoja de ruta con indicadores de resultado.

En tercer lugar, la gobernanza es el factor decisivo. La ley de ciberseguridad de 2026 demuestra que el país puede construir marcos de responsabilidad compartida con obligaciones diferenciadas para el sector privado. El desafío es extender esa lógica a la protección física, mediante la designación de operadores críticos, estándares mínimos, canales seguros de intercambio de información, incentivos y coordinación local con las comunidades. Sin ello, las mejores tecnologías serán islas desconectadas.

Finalmente, la eficacia debe equilibrarse con la legitimidad. Una política de protección que vulnere la privacidad, abuse de la fuerza o naturalice el empleo permanente de las Fuerzas Armadas en tareas civiles erosiona la confianza social de la que depende, en última instancia, la seguridad de la infraestructura. Las salvaguardas de protección de datos, uso proporcionado de la fuerza y seguridad de los propios sistemas no son un costo adicional, sino una condición de sostenibilidad.

La seguridad de la infraestructura crítica será, cada vez más, una medida de la capacidad del Estado para proteger la vida cotidiana de su población sin sacrificar los derechos que justifican su existencia.

Referencias

- Constitución de la República del Ecuador. (2008). *Registro Oficial 449*, 20 de octubre de 2008.
- Defonline. (2026). *La Ley de Ciberseguridad de Ecuador, ¿un ejemplo para Argentina?* <https://defonline.com.ar/seguridad/la-ley-de-ciberseguridad-de-ecuador-un-ejemplo-para-argentina/>
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. *Diario Oficial de la Unión Europea*, L 333.
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas. *Diario Oficial de la Unión Europea*, L 333.
- DPL News. (2021). *Vandalismo a infraestructura telecom deja sin servicio a miles de usuarios en Ecuador*. <https://dplnews.com/?p=128490>
- DPL News. (2026). *Entra en vigor Ley de Ciberseguridad en Ecuador para blindar infraestructura crítica y datos personales*. <https://dplnews.com/?p=317624>
- Eje Central. (2024). *En alerta Centro y Sudamérica por conflicto en Ecuador*. <https://www.ejecentral.com.mx/en-alerta-centro-y-sudamerica-por-conflicto-en-ecuador>
- El Diario. (2025, 19 de diciembre). *Ciberseguridad en Ecuador enfrenta amenazas crecientes según BID*. <https://www.eldiario.ec/ecuador/ciberseguridad-en-ecuador-enfrenta-amenazas-crecientes-segun-bid-19122025/>
- El Diario. (2026, 30 de junio). *Cortes de luz en Ecuador: razones de los apagones*. <https://eldiario.ec/ecuador/cortes-de-luz-ecuador-razones-apagones-30062026/>
- El Mercurio. (2025). *Machala sufre dos ataques explosivos y se queda sin energía eléctrica*. <https://elmercurio.com.ec/?p=1184042>

- El Universo. (s. f.). *SOTE* [Página temática]. <https://www.eluniverso.com/temas/sote/>
- Expreso. (s. f.). *Internet en Ecuador: ¿hay riesgo tras la decisión de Arcotel sobre Cable Andino?* <https://www.expreso.ec/actualidad/economia/internet-ecuador-riesgo-problema-cable-andino-expertos-221421.html>
- Garcia, M. L. (2007). *Design and evaluation of physical protection systems* (2.^a ed.). Butterworth-Heinemann.
- International Electrotechnical Commission. (2018). *IEC 62443: Security for industrial automation and control systems* [Serie de normas]. IEC.
- International IDEA. (2025). *Ecuador – October 2025* [Democracy Tracker]. <https://www.idea.int/democracytracker/report/ecuador/october-2025>
- International Organization for Standardization. (2018). *ISO 31000:2018. Risk management — Guidelines*. ISO.
- International Organization for Standardization. (2019). *ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements*. ISO.
- Ley de Seguridad Pública y del Estado. (2009). *Registro Oficial Suplemento* 35, 28 de septiembre de 2009.
- Ley Orgánica de Protección de Datos Personales. (2021). *Registro Oficial Quinto Suplemento* 459, 26 de mayo de 2021.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- NMS Law. (2026, 1 de junio). *Ecuador: Ley Orgánica para el Fortalecimiento de la Ciberseguridad*. <https://nmslaw.com.ec/blog/2026/06/01/ecuador-ley-organica-fortalecimiento-ciberseguridad/>
- Noticias RCN. (2025, 15 de octubre). *Nuevo ataque con explosivos dejó dos puentes destruidos en Ecuador*. <https://www.noticiasrcn.com/internacional/ataque-con-explosivos-en-ecuador-947860>
- Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.
- Primicias. (s. f.). *Al menos cinco apagones nacionales y otros cortes imprevistos ha vivido Ecuador en el último año*. <https://primicias.ec/economia/apagones-recurrentes-noboa2024-cortes-luz-crisis-86045>
- Primicias. (2022). *Ejecutivo plantea que militares ingresen a las cárceles en casos críticos*. <https://primicias.ec/noticias/politica/ejecutivo-plantea-militares-ingresen-carceles>
- Primicias. (2024a). *Este es el balance de detenidos y atentados en seis días de “conflicto armado interno”*. <https://primicias.ec/noticias/sucesos/conflicto-armado-detenidos-atentados-ecuador>
- Primicias. (2024b). *Terrorismo, el motivo del 4 % de las detenciones durante el conflicto armado interno*. <https://www.primicias.ec/noticias/seguridad/terrorismo-detenidos-ecuador-gobierno-conflicto-armado-interno>
- Primicias. (2024c). *Fuerzas Armadas y Policía operarán y reforzarán seguridad de hidroeléctricas en Ecuador*. <https://primicias.ec/economia/gobierno-militares-operaciones-centrales-electricas-cortes-luz-ecuador-78330>
- Primicias. (2025a). *Estados Unidos condena atentado en Guayaquil con coche bomba y explosiones provocadas en dos puentes*. <https://www.primicias.ec/seguridad/estados-unidos-condena-atentado-guayaquil-coche-bomba-puentes-explosion-107343/>
- Primicias. (2025b). *Rotura del oleoducto estatal SOTE genera nuevo derrame de petróleo entre Cuyuja y Papallacta, en Napo*. <https://www.primicias.ec/economia/derrame-petroleo-cuyuja-papallacta-napo-99856/>
- Primicias. (2025c). *Petroecuador demoró casi media hora en cerrar válvulas y confirmar la rotura del SOTE, según su gerente*. <https://www.primicias.ec/tag/oleoducto/>
- Primicias. (2025d). *Perforación clandestina en el SOTE produce nuevo derrame de petróleo*. <https://www.primicias.ec/economia/perforacion-clandestina-sote-derrame-petroleo-ecuador-102528/>
- Primicias. (2025e). *Alerta por explosión en el puente Churute, vía Puerto Inca–Naranjal*. <https://www.primicias.ec/sucesos/alerta-explosion-puente-churute-prefectura-guayas-atentado-via-naranjal-ecuador-107287/>
- Reuters. (2025a). *Explosions hit Ecuador bridges days after illegal mining crackdown*. <https://mcac.maryland.gov/?p=9855>
- Reuters. (2025b). *Explosions reported on two bridges along Ecuador coast*. <https://www.yahoo.com/news/articles/explosions-reported-two-bridges-along-144336487.html>
- Rinaldi, S. M., Peerenboom, J. P., y Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25. <https://doi.org/10.1109/37.969131>
- Teleamazonas. (2026). *Ley para el fortalecimiento de la ciberseguridad en Ecuador fue aprobada por el Pleno Legislativo*. <https://www.teleamazonas.com/actualidad/noticias/politica/asamblea-aprueba-ley-fortalecimiento-ciberseguridad-110582/>
- Torres Alcocer, L. M., y Carrasco Muro, C. D. (2026). *Robo de cables y vandalismo de infraestructura de telecomunicaciones en América Latina*. cet.la / ASIET. <https://isoclave.substack.com/p/latam-cable-theft>
- U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. DHS.
- Uno TV. (2025). *Atentados con explosivos dañan dos puentes en Ecuador*. <https://www.unotv.com/internacional/atentados-con-explosivos-danan-dos-puentes-en-ecuador/>

- Vanguardia. (2024, 9 de enero). *Gobierno de Ecuador autoriza a Fuerzas Armadas a ejecutar acciones militares: firmó decreto de conflicto armado interno*. <https://www.vanguardia.com/mundo/gobierno-de-ecuador-autoriza-a-fuerzas-armadas-a-ejecutar-acciones-militares-firmo-decreto-de-conflicto-armado-interno-JG8383874>
- Vistazo. (2025a, 12 de diciembre). *Ola de violencia en Ecuador rompe su propio récord: informe advierte que seguirá en aumento en 2026*. <https://www.vistazo.com/amp/actualidad/nacional/2025-12-12-ola-violencia-ecuador-record-no-cede-crezca-2026-NB10553718>
- Vistazo. (2025b, 10 de marzo). *CELEC anuncia cortes de luz este martes 11 de marzo en Guayas para realizar labores en subestación*. <https://www.vistazo.com/actualidad/nacional/2025-03-10-celec-cortes-de-luz-martes-11-de-marzo-guayas-BL8940416>