PROGRAMA **JUNIOR FELLOWSHIP** 2025

# ROBO DE CABLES Y VANDALISMO DE INFRAESTRUCTURA DE TELECOMUNICACIONES EN AMÉRICA LATINA

**Luis Mauricio Torres Alcocer,**
**Coordinador del cet.la**
**Carlos David Carrasco Muro,**
**Junior Fellow 2025**

cet.la
Centro de Estudios de Telecomunicaciones de América Latina

**Este proyecto de investigación fue desarrollado en el marco del programa de becas Junior Fellowship 2025 y coordinado por el Centro de Estudios de Telecomunicaciones de América Latina (cet.la).**

El **Centro de Estudios de Telecomunicaciones de América Latina** (cet.la) ha elaborado un ejercicio integral de diagnóstico, análisis y generación de propuestas sobre el problema del robo de cables y vandalismo de las telecomunicaciones.

En esta investigación se recopila una serie de propuestas centradas en políticas de prevención, disuasión, seguridad de instalaciones, detección, atención y seguimiento de incidentes, así como mecanismos de coordinación público-privada, mitigación y combate a mercados ilegales, como una agenda regional contra el vandalismo de las telecomunicaciones.

Desde el cet.la, se busca que este análisis contribuya al debate sobre la problemática y promover el impulso de acciones concretas en los países de América Latina afectados por este fenómeno.

estudios@tel.lat
cet.la

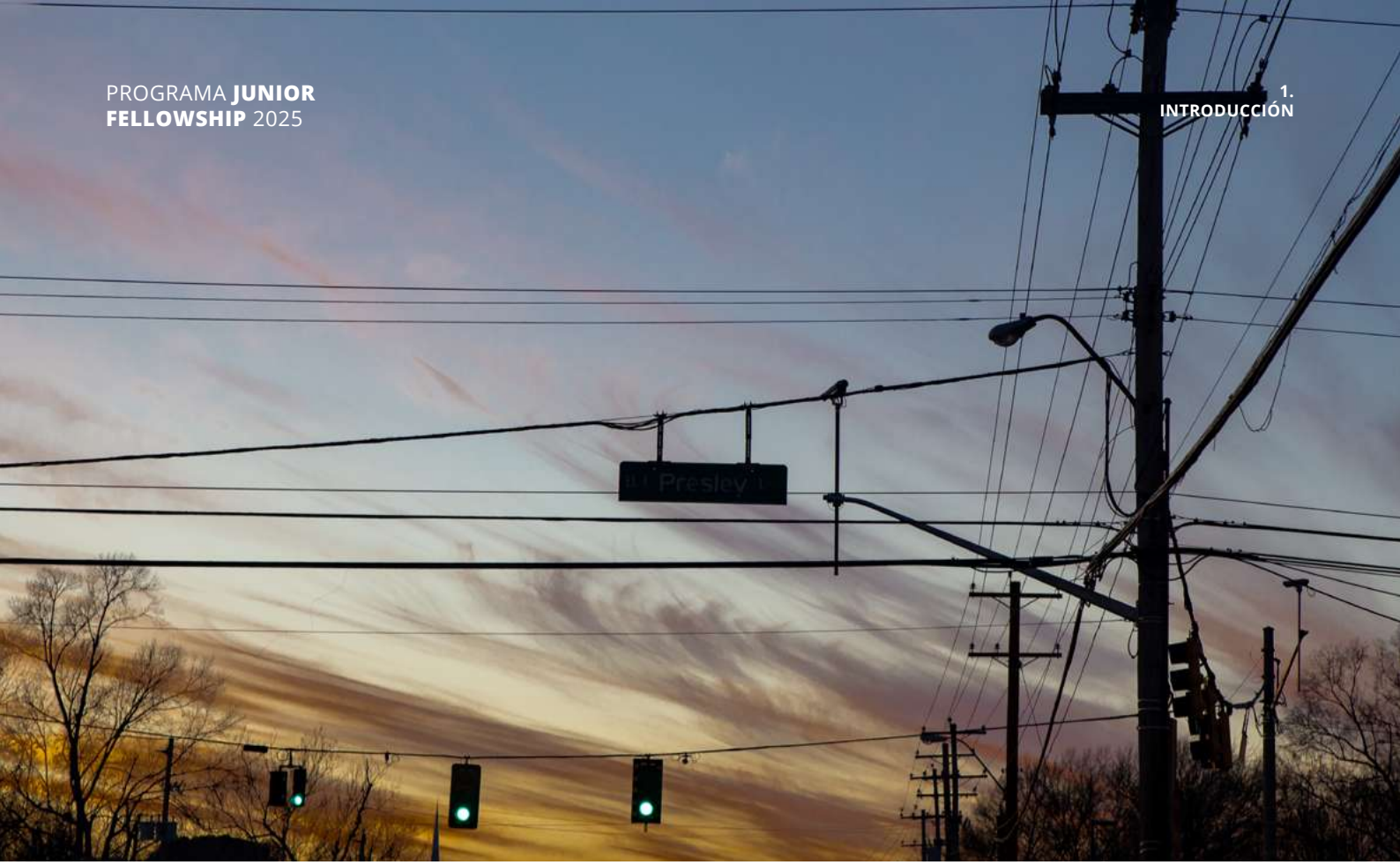
**Luis Mauricio Torres Alcocer**
Coordinador del Centro de Estudios de Telecomunicaciones de América Latina (cet.la) y Editor Asociado de la Revista Latinoamericana de Economía y Sociedad Digital (RLESD). Economista por la Universidad de las Américas Puebla, México (UDLAP), y maestro en regulación por la London School of Economics and Political Science (LSE). Es consultor especialista en gestión y desarrollo de investigación aplicada para asuntos y políticas públicas. Ha trabajado con diversos centros de investigación y think tanks enfocados al análisis económico y regulatorio de sectores y mercados en la región.

**Carlos David Carrasco Muro**
Licenciado en Comunicación Social (2016) por la Universidad Católica Andrés Bello, Venezuela. Magister en Transformación Digital e Industria 4.0 por la Universidad Isabel I (2021), becado por la OEA. Cuenta con trayectoria profesional, en organismos internacionales liderando áreas de investigación e incidencia en migración, interseccionalidad, derechos humanos y democracia. Ha sido migrante en Chile. Actualmente es profesor de la Universidad Central de Venezuela y en la Universidad Católica Andrés Bello. También es estudiante del Doctorado en Sociedad Política y Cultura de la Universidad del País Vasco (España).

Rambla República de México 6125, CP 11400, Montevideo, Uruguay.
Calle Príncipe de Vergara 109, 2° planta, CP 28802, Madrid España.

Fecha de publicación: Abril, 2026

# Contenido



# 1. Introducción:

En América Latina y el Caribe existe un problema estructural de la infraestructura de telecomunicaciones relacionado con el robo de cables y el vandalismo de instalaciones. De forma frecuente se observan denuncias en la prensa por parte de operadores de telecomunicaciones y usuarios en diversos países de la región señalando el robo de cables y otros componentes de infraestructura con afectaciones a las señales de telefonía móvil, fija y de televisión. Una consulta a operadores de telecomunicaciones en 14 países de la región[1] muestra que **63%** de ellos percibe un aumento significativo o moderado en el número de incidentes de robo o afectaciones a su infraestructura en los últimos 5 años. En contraste, algunos operadores observan avances importantes en la reducción de incidencias en países como Chile y Colombia.

Estas prácticas delictivas tienen implicaciones tanto para la conectividad de millones de personas cada año como impactos económicos para los operadores de telecomunicaciones.

Sus efectos más adversos se manifiestan en falta de acceso confiable de servicios de telecomunicaciones en economías locales y retraso en el desarrollo digital de las comunidades afectadas ante este tipo de vandalismo. Las empresas de infraestructura digital así como los prestadores de servicios de telecomunicaciones observan un reto operativo para llevar servicios a zonas con alta prevalencia de ataques a instalaciones y los usuarios experimentan un acceso incierto y deteriorado

**1.** Ver cuadro de Metodología y análisis de datos

a servicios de conectividad. Además de los retos operativos y los costos directos relacionados con el daño a instalaciones y la reposición de materiales y equipos, existen costos ocultos e indirectos para los operadores de telecomunicaciones: interrupción de la conectividad que genera reclamos y menor satisfacción del cliente, así como costos regulatorios y sanciones por incumplimientos de metas de calidad en el servicio.

La naturaleza del fenómeno no se limita a incidentes aislados. Una buena parte del vandalismo se encuentra liderado por estructuras criminales que buscan cables de cobre, baterías y otros componentes tecnológicos para venderlos en mercados negros y exportarlos fuera de los países de la región. Esto influenciado y agravado por una debilidad institucional y de seguridad en muchos países de América Latina. Adicionalmente, el vandalismo de infraestructura tiene implicaciones financieras adversas para el desempeño de la industria de las telecomunicaciones que tiene ya dificultades derivadas del contexto macroeconómico y de los mercados en la región.

### Metodología de recopilación y análisis de datos

Para la elaboración de este reporte, además de la revisión de literatura y fuentes de información secundaria, se realizaron dos análisis de datos relevantes para entender el fenómeno del robo de cables y le vandalismo en el sector de las telecomunicaciones en América Latina:

**Análisis de notas periodísticas.** Se recopilaron y revisaron más de 100 notas de prensa sobre 19 países publicadas en medios nacionales y regionales entre 2020 y 2025 que abordan diversos casos e incidentes de robo y vandalismo que afectan a la infraestructura de conectividad. Esta muestra no es representativa del fenómeno a nivel nacional o regional para un análisis cuantitativo y estadístico profundo del fenómeno, debido a que la disponibilidad de datos no es homogénea y la falta de agregación nacional de casos. Además el seguimiento de la prensa se centra en incidentes con alto impacto mediático, reportes y denuncias de la industria y no necesariamente en un seguimiento estructurado del fenómeno a través del tiempo. Sin embargo, la revisión de estos casos ofrece información cualitativa valiosa para comprender el fenómeno en dimensiones relacionadas con el modus operandi y tipología de incidentes relacionados al tema.

**Encuesta sondeo a operadores locales de telecomunicaciones.** En el marco de esta investigación se tuvo también la oportunidad de consultar a una muestra no representativa de operadores locales que operan en 14 países de América Latina con el objetivo de conocer con mayor profundidad su percepción sobre la problemática. Si bien los datos de este sondeo no son representativos cuantitativamente de la realidad de los países o de la región, es posible reconocer algunas tendencias relevantes para el entendimiento y diagnóstico del problema. Su valor se centra en capturar las opiniones y reportes de manera balanceada para los países incluidos.

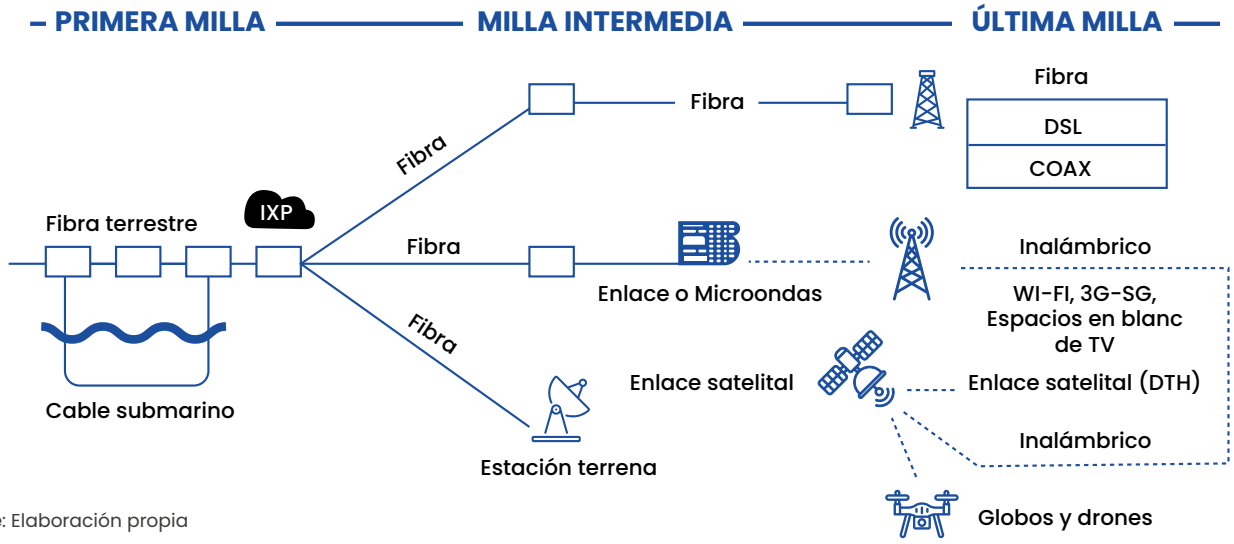
# 2. Robo y vandalismo de infraestructura en la cadena de valor de las telecomunicaciones

El robo y vandalismo de infraestructura de telecomunicaciones puede definirse como el proceso de sustracción, daño o interferencia no autorizada de componentes o equipos de infraestructura física que forma parte de las redes de telecomunicaciones utilizadas por operadores para la transferencia de datos y la provisión de servicios de conectividad[2345].

Para entender mejor este fenómeno delictivo es importante situarlo dentro de la cadena de valor de la infraestructura de telecomunicaciones[6]. Si bien los distintos tramos de infraestructura son vulnerables a múltiples fuentes de disrupción (climática, de seguridad nacional, accidentes o desastres), el robo y vandalismo se observa primordialmente en la última milla de la cadena de valor.

**2.** Fiscalía General del Estado de Ecuador. (s. f.). Formulario en línea para el registro de presuntos delitos de robo y hurto. Fiscalía General del Estado.
**3.** Fiscalía Nacional de Chile. (2024, noviembre). Crimen organizado en Chile. Insight Crime.
**4.** East African Communications Organisation, EACO (2018). Curbing the communications infrastructure vandalism vice in the East African Community.
**5.** Ministerio Público Federal de Brasil
**6.** Banco Mundial. (2024). Resilient telecommunications infrastructure. Open Knowledge World Bank.

**Gráfico 1**




Fuente: Elaboración propia

# Primera milla

Se trata de la parte inicial del sistema de telecomunicaciones. Son el punto de entrada de datos de las redes internacionales, donde se pueden ubicar componentes como los cables submarinos, estaciones de amarre (CLS), conexiones terrestres y satelitales, centros de datos, nodos internacionales o puntos de intercambio de tráfico (IXP). La función de estos componentes es conectar las redes nacionales con proveedores globales o fuentes de contenido, transportando datos hacia las redes troncales de los países.

En el caso de los cables submarinos, suelen estar compuestos por fibra óptica y capas de vaselina, polietileno, alambres de acero trenzado, barreras de aluminio resistente al agua, policarbonato, tubos de cobre o aluminio. De igual manera, en el caso de estaciones de amarre (CLS) y los centros de datos están compuestos por servidores que pueden variar en tamaño en función de las necesidades o del espacio físico. También, se utilizan sistemas de alimentación ininterrumpida (SAI) que funcionan con baterías compuestas por elementos como el plomo, cobalto, litio o níquel.

Normalmente, los componentes de esta primera milla no suelen ser un foco de vandalismo, ya que se encuentran en lugares remotos o de difícil acceso. Además, se encuentran con vigilancia privada permanente y cuentan con apoyo de organismos de seguridad y defensa al tratarse de infraestructura crítica para los países. Recientemente ante ataques a cables submarinos a nivel global existe una renovada atención por estos componentes.

## Milla intermedia

Comprende aquellos componentes que unen a la primera milla con las redes locales, ya sea a nivel de internet, televisión, radiodifusión, telefonía móvil y telefonía fija. Esta infraestructura transporta datos dentro de las demarcaciones geográficas de los países y pueden incluir estaciones terrestres de satélites, enlaces de microondas, centrales locales (DSLAM), puntos de intercambio de tráfico (IXP), cables de cobre o de fibra óptica.

En el caso de las estaciones terrestres de satélites, entre los materiales claves de estas estructuras se pueden mencionar las antenas parabólicas, transceptores y sistemas de soporte que incluyen paneles solares o baterías. De igual manera, en las DSLAM, se encuentran sistemas de refrigeración y fuentes de alimentación eléctrica.

Algunos de los materiales que componen esta milla intermedia pueden resultar atractivos para grupos delictivos. Igualmente pueden estar expuestos a fenómenos naturales o climáticos. Además, no toda la infraestructura en esta milla cuenta con seguridad por parte de las empresas operadoras o el Estado.

## Última milla

Se refiere a la parte final que conecta la red del sistema de telecomunicaciones con los usuarios finales. Esta conexión puede ser mediante fibra óptica, cables de cobre o redes inalámbricas a través de antenas, torres de telecomunicaciones, drones y globos.

Esta infraestructura suele tener un mayor grado de vulnerabilidad, ya que se encuentran en amplias zonas del espacio público, cuyo monitoreo y vigilancia puede ser más difícil en zonas menos pobladas. Además, para los grupos delictivos, resulta atractivo el robo de cables, baterías o antenas al encontrarse de fácil acceso para su manipulación.

La revisión de notas de prensa sobre el tema en la región muestra que es en la última milla donde se reportan con más frecuencia incidentes y casos de robo de cable y vandalismo[7]. Además, existe una concentración en cierto tipo de componentes de la infraestructura.

**7.** En el análisis de prensa se descartaron modalidades de daño y sustracción de materiales de infraestructura de telecomunicaciones de las primeras millas o millas intermedias debido a que se concentran en aspectos como operaciones de guerra, terrorismo o sabotaje de infraestructuras críticas que responden a fenómenos distintos al robo o vandalismo común.

**Una de las razones principales que impulsa el robo de cables compuestos de metales como el cobre es que tienen un incentivo económico. El cobre como metal se trata de uno de los materiales más buscados para su posterior reventa en el mercado negro.**

## Robo de cables de cobre

Se focaliza en la sustracción de cables y materiales que se encuentran en el espacio público y cuyo interés se centra en la extracción del metal para su posterior tráfico o comercialización. Este tipo de delito es el más común reportado en los casos de vandalismos identificados. Entre el **40%** y **65%** de las notas de prensa analizadas mencionan o implican a los cables de cobre (o cables sin especificar) como el principal material objeto de robo en la región.

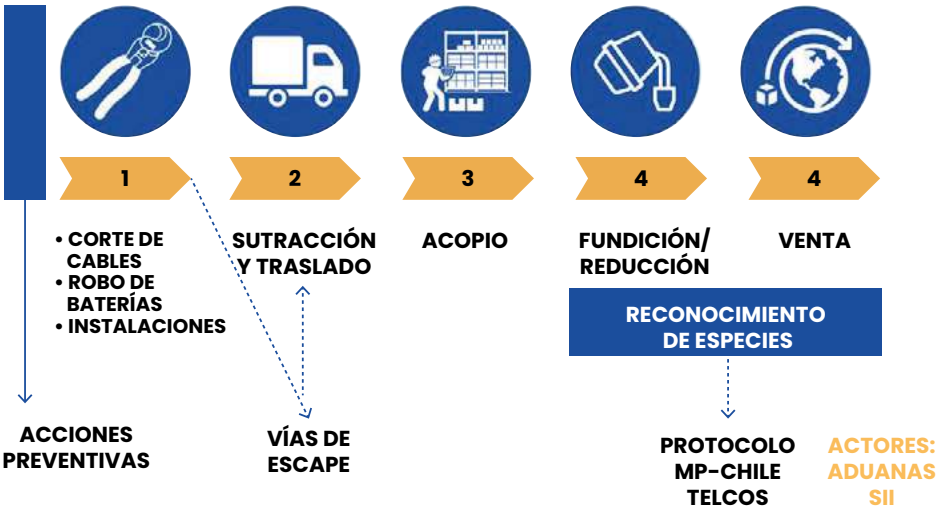
En casos básicos, el robo se presenta a través del corte de cableado. No obstante, existen modalidades de robo sistemáticas que requieren de la utilización de vehículos para arrastrar el cableado y facilitar su extracción.

Una de las razones principales que impulsa el robo de cables compuestos de metales como el cobre es que tienen un incentivo económico. El cobre como metal se trata de uno de los materiales más buscados para su posterior reventa en el mercado negro. El alza en los precios del cobre impulsa las actividades de sustracción ilegal y genera rentabilidad en las organizaciones internacionales de tráfico del mismo.

El daño o robo de estos cables podría deberse, en casos excepcionales, a intenciones de sabotaje o vandalismo con objetivos distintos a la comercialización de metales.

**Gráfico 2**

### ROBO DE CABLES DE COBRE: MERCADO




Fuente: Servicios de Impuesto Internos de Chile

**Existe una demanda creciente de robo de otros dispositivos de infraestructura como baterías y componentes de las estaciones, torres y fuentes de poder en instalaciones de telecomunicaciones.**

## Extracción de cables de fibra óptica

En conjunto con el robo de cables de cobre, aunque en menor medida, se reporta el robo de cable de fibra óptica. Sin embargo, este material no puede ser utilizado, comercializado o monetizado de manera directa luego de su extracción y daño. Por esa razón, se presume, como se observa en algunas de las notas de prensa analizadas, que el vandalismo hacia los cables de fibra óptica se debe a la búsqueda fallida de cobre por parte de delincuentes al no poder diferenciar entre distintos tipos de cables.

En menos del **30%** de las notas de prensa evaluadas se mencionan incidentes donde el cable de fibra óptica fue objeto de robo o daño (incluyendo en esta clasificación a las notas que no especifican el material robado - cerca del **16%**).

Es posible también plantear la hipótesis de que en una minoría de casos el objetivo es la desconexión intencional o la interferencia del servicio con objetivos distintos al robo (por ejemplo en casos de sabotaje o control/interferencia territorial de las comunicaciones por parte de grupos criminales o terroristas).

## Robo de baterías y otros componentes de las instalaciones

Los reportes periodísticos revisados muestran que, aunque en menor medida, existe una demanda creciente de robo de otros dispositivos de infraestructura como baterías y componentes de las estaciones, torres y fuentes de poder en instalaciones de telecomunicaciones.

Se trata del segundo delito más común reportado en los casos de vandalismos analizados. Las baterías son buscadas también para su reventa en el mercado negro. La sustracción de las baterías en antenas o subestaciones también requiere de la utilización de vehículos que sean capaces de movilizar dichas baterías, ya que pueden tener un peso cercano a los 30 kg en algunos casos. Si bien, las baterías tradicionales siguen siendo buscadas, existe una tendencia en aumento por el robo de baterías de litio cuya duración es mayor.

# 3. Daño a infraestructuras de conectividad: perfil criminal y modus operandi

El fenómeno del vandalismo de infraestructura puede ser analizado desde la perspectiva de los agentes perpetradores, sus motivaciones y métodos. Se ha identificado una segmentación de dos tipos de actores que incurren en el robo de cables y en vandalismo.

## Ladrones ocasionales con intencionalidad oportunista

Este tipo de actores criminales recurren a instancias de robo y afectaciones a infraestructura ocasionales y no sistemáticas realizadas por personas o grupos no organizados como un medio de subsistencia inmediata. En esta clasificación se encuentran personas o grupos que logran vulnerar las instalaciones físicas para la obtención de materiales, pero sin un método determinado de sustracción, ni una red

organizada para la movilización y monetización de materiales o equipos. Es decir, se refiere bandas criminales oportunistas circunscritas a comunidades locales, ladrones comunes de vivienda, comercio o autos experimentando otras modalidades de robo, e incluso personas en situación de calle o con problemas de adicciones en busca de oportunidades para la reventa de material sustraído.

- **Reventa en mercados ilegales locales de menor alcance.** Dentro del análisis de los casos identificados, sobresale un ejemplo de Tucumán, Argentina[8] donde los grupos que roban baterías, no se encuentran insertados en una cadena delincuencial internacional, sino que las baterías son revendidas para alimentar los equipos de audio que se instalan en los autos o para paneles solares. Un caso similar, sucede en Bolivia[9], donde la policía ubicó una cantidad de baterías robadas de una operadora, que se encontraban siendo ofertadas en redes sociales.

También, se puede mencionar el caso de Colombia[10], donde la Fiscalía General de la Nación desarticuló a una banda dedicada al hurto de baterías de plomo y de litio de antenas de telefonía celular; así como también lograron la captura de compradores locales de estas baterías robadas.

Según un comunicado oficial de la Policía Nacional de Colombia, en el municipio de Aguadas (Caldas) se frustró el hurto de 29 baterías de antenas de telecomunicaciones, importantes para mantener servicios de internet móvil, telefonía y televisión durante cortes eléctricos; gracias a la denuncia de la comunidad, las autoridades capturaron en flagrancia a un hombre joven que había ingresado violentamente al sitio, encontrándole además elementos utilizados para el hurto y una camioneta utilizada para movilizar los bienes robados[11].

En Uruguay[12] por ejemplo, las investigaciones policiales han determinado que una buena parte de los autores de los hurtos de cables son delincuentes menores e incluso personas en situación de calle y vulnerables por adicciones que venden los cables en distintos depósitos y chatarrerías. En un caso concreto, se indicaba cómo el cobre robado era enviado a Porto Alegre, Brasil donde atravesaba un proceso de reindustrialización. También el caso de Ecuador[13], donde las empresas de telecomunicación locales han señalado que algunos de los responsables de los robos de cables son habitantes en situación de calle, quienes aprovechan la noche para sustraer los cables y después venderlos a terceros.

## Estructuras criminales organizadas

Estas redes tienen capacidad sistemática, no solo para la extracción cable y otros componentes, sino también para el transporte, fundición, transformación, desmantelamiento, comercialización y exportación a mercados internacionales. Estas capacidades permiten clasificar a estas redes como grupos de crimen organizado bajo la definición de la Convención de Palermo de Naciones Unidas[14] al cumplir con los principales criterios y características para ser clasificados de esta manera:

**8.** Tucumán Despierta. (2023, septiembre 4). Roban baterías de las antenas de Personal y Claro.
**9.** EJU.tv. (2021, 11 de agosto). Capturan a cinco personas vinculadas al robo de baterías de una antena de Entel.
**10.** Alcaldía de Bogotá. (2022, agosto 3). Por hurto de baterías de antenas telefónicas cayeron 5 de 'Los Bodegueros'.
**11.** Policía Nacional de Colombia. (2023). En una rápida acción policial se logró frustrar el hurto de 29 baterías para antenas de telecomunicaciones.
**12.** Leal, C. M. (2022). Los cables de cobre en Uruguay: un robo que deja vidas en el camino y ataca a la sociedad. Montevideo Portal.
**13.** Redacción Ecuavisa. (2025). Quito | Los habitantes de calle han robado cerca de USD 70 000 en cables de telefonía fija en el primer mes de 2025. Ecuavisa.
**14.** United Nations Office on Drugs and Crime. (2004). United Nations Convention against Transnational Organized Crime (UNTOC) e-book. ONUDC.

**De entre las notas de prensa analizadas en las que es posible distinguir el perfil criminal de los actores involucrados, casi el 85% de los reportes refieren a robo y vandalismo por parte de grupos organizados y solo un 15% a robos oportunistas.**

- El involucramiento de 3 o más personas de forma consensuada.
- La existencia de una vocación y gestión en el tiempo en función de los delitos cometidos.
- El objetivo principal es un beneficio económico, político o social y no un daño aislado.

De entre las notas de prensa analizadas en las que es posible distinguir el perfil criminal de los actores involucrados, casi el 85% de los reportes refieren a robo y vandalismo por parte de grupos organizados y solo un 15% a robos oportunistas.

## Modus operandi de los grupos organizados de robo y vandalismo de infraestructura

Las actividades delictivas de las organizaciones implican una cadena operativa compleja (aunque a distintas a escalas de operación) que conecta los actos en instalaciones con redes internacionales de tráfico de componentes y materiales:

- **Robo y vandalismo de cables y otros componentes físicos en instalaciones de telecomunicaciones.** Normalmente, estos grupos utilizan técnicas avanzadas de sustracción con planificación y gestión profesional, uso de vehículos y herramientas para el desmantelamiento de infraestructura y redes organizacionales logísticas para la captura de valor económico derivado de sus actividades delictivas.

- **Vinculación con redes criminales especializadas.** Las organizaciones que cometen estos delitos se encuentran estrechamente vinculados con otros grupos delincuenciales rubros complementarios en la cadena criminal para la comercialización de materiales y equipos que podrían no estar limitadas a las relacionadas con telecomunicaciones sino con otras infraestructuras críticas como las redes eléctricas, por ejemplo. Además, existe un ecosistema que promueve la venta de cable de cobre y otros componentes, a través de la vinculación con recicladoras de chatarra, fundidoras de metales e inclusive empresas de exportación de metales:

    - Transporte, almacenamiento y manejo logístico de componentes sustraídos.
    - Fundición, reducción, transformación o reconfiguración de cables, equipos, componentes y materiales sustraídos.
    - Tráfico, comercialización y exportación de componentes y materiales.

Dentro de los reportes de prensa consultados en la región, es posible definir algunas modalidades y características recurrentes de los grupos criminales que operan en el robo y vandalismo de las telecomunicaciones.

- **Fingen pertenecer a operadoras o abusan de su capacidad de acceso a instalaciones.** Se destacan casos como el de Curitiba, Brasil[15] donde se capturó a un hombre que fingía ser operador de una empresa de telecomunicaciones para robar baterías de una antena. De igual manera, en el estado de Minas

**15.** Banda B. (2024, 11 de octubre). Trío es preso por furtar y triturar cables telefónicos en Campina Grande do Sul.

Gerais[16], dos hombres fueron detenidos *in fraganti* por robar baterías en una estación de una empresa de telecomunicaciones, ambos eran empleados subcontratados del sector y tenían acceso a las instalaciones de más de un proveedor.

En el caso de Plata, Argentina[17], también se puede ubicar el caso de 9 sospechosos detenidos que fingían ser empleados de empresas de telefonía y contaban con uniformes de trabajo, un camión y credenciales falsas. De igual manera, en Perú[18] se presentó el caso de una banda que fue hallada robando baterías y contaban con chalecos y cascos de seguridad para pasar como personal de alguna operadora. Un caso similar se puede ubicar en Paraguay[19], donde un grupo fingía ser trabajadores técnicos y lograban apoderarse de baterías en diferentes departamentos de ese país. En México se conoce de casos en donde, para pasar desapercibidos, personas se caracterizan de técnicos de operadores locales para cortar y sustraer cable de cobre, en ocasiones dañando fibra óptica de proveedores de telecomunicaciones.

Igualmente en Paraguay[20], la operadora estatal ha señalado situaciones de vandalismo donde técnicos de la compañía se han visto involucrados. Asimismo, el Ministerio de Seguridad de Costa Rica[21] ha señalado la existencia de grupos que simulan ser cuadrillas de trabajo para tener acceso al cable sin despertar sospechas y usan indumentaria, cascos e incluso rotulación falsa en vehículos.

- **Conexión permanente con actores en mercado negros internacionales de cobre.** Se identificaron notas de prensa en países como Bolivia[22], donde se menciona que el robo de cables de cobre suele aumentar cuando se presenta un incremento en la valorización de este metal. Otro ejemplo, se puede ubicar en Brasil[23] en 2024, donde los propietarios de un depósito de chatarra fueron arrestados por recibir placas de retransmisión de señal utilizadas por las antenas de telefonía. Igualmente en Brasil[24] durante 2025, la Policía Civil de la División de Robos y Hurtos (DRF) realizaron un operativo para desmantelar una banda dedicada al hurto y robo de cables de cobre y fibra óptica. Se afirmaba que este grupo es sofisticado y está involucrado en el lavado de dinero y tiene vínculos con el Comando Vermelho (CV), la segunda banda más grande de Brasil. De igual manera, en México[25] se atribuye al crimen organizado el robo de cables de cobre del sistema de transporte Metro, la empresa estatal de electricidad y operadoras de telefonía fija para su venta.

A nivel global, se pueden ubicar estudios que coinciden con esta caracterización. Por ejemplo, en la Universidad Walter Sisulu en Sudáfrica analizaron el impacto socioeconómico del robo de cobre en Sudáfrica y Zimbabue (2020-2023)26, cuyos hallazgos sugieren la operación de bandas criminales altamente organizadas vinculadas a mercados ilegales asiáticos y europeos, donde se pueden blanquear hasta 3.000 toneladas anuales de metal robado de infraestructuras eléctricas y telecomunicaciones, causando pérdidas de USD 46.000.000 al año e interrupciones críticas de servicios (apagones, caídas de redes móviles). Este estudio también

**16.** Teletime News. (2024, 1 de diciembre). Roubo de equipamentos de telecom se multiplica para além dos cabos de cobre. Teletime.
**17.** Infobae. (2025, 5 de mayo). Simulaban ser técnicos de una empresa para robar cables en La Plata: hay 9 detenidos.
**18.** El Muro. (2023, 20 de agosto). Los "Telemáticos" caen robando cables de telefonía en el cerro San Cristóbal.
**19.** ÚH. (2025, 12 de mayo). Detienen a miembro de una banda dedicada al robo de baterías de alto valor para empresas telefónicas. Última Hora.
**20.** La Nación. (2024). Copaco investiga a técnicos por robo de 1.800 metros de cables en San Vicente.
**21.** Columbia (2024). Cifras de robo de cable bajan, pero perjuicio económico sigue siendo alto.
**22.** Unitel Bolivia. (2024, 24 de octubre). La venta de cobre en el mercado negro, una de las razones que vecinos apuntan como causa para el robo de cables.
**23.** Teletime News. (2024, 1 de diciembre). Roubo de equipamentos de telecom se multiplica para além dos cabos de cobre. Teletime.
**24.** Interlira Reports. (2025). Copper cable theft: Gangs connected to organized crime.
**25.** Barragán, A. (2023). El robo de cables del Metro, CFE, Telmex y más servicios se dispara 306% en 5 años.
**26.** Mugari, I., & Obioha, E. E. (2024). Socio-economic development impacts, attendant challenges and mitigation measures of infrastructure vandalism in Southern Africa. Development Southern Africa, 41(3), 570–587.

destaca que la demanda china de cobre (60% de las exportaciones ilegales sudafricanas) y la corrupción en puertos que facilita este crimen, mientras que la vulnerabilidad física (cercas débiles, falta de sensores) y pobreza local (reclutamiento en comunidades marginadas) son factores que perpetúan esta situación.

Una alternativa para identificar, desde los datos macroeconómicos de comercio internacional, patrones de actividades de exportaciones ilegales de cobre podría ser el análisis de discrepancias entre la producción minera de los países y los datos de exportación. Estas podrían indicar países donde el tamaño de las exportaciones de cobre no es congruente con el tamaño de la actividad minera, lo cual podría explicarse al menos parcialmente por el comercio de cobre ilegal y robado.

- **Competencia desleal.** Operadores de la región mencionan también casos de competencia desleal en las cuales proveedores de servicios de telecomunicaciones pequeños o informales compran y utilizan materiales como cobre o baterías robadas para la provisión de servicios con el objetivo de ahorrar costos de inversión en equipos nuevos y legales.

- **Vandalismo de telecomunicaciones como estrategia de control.** En México[27] se afirma que el vandalismo de las telecomunicaciones puede tener objetivos más allá de la reventa de cierto material. Se señala que los grupos de crimen organizado buscan establecer su propio control y dominio sobre las áreas donde tienen mayor presencia. De igual manera, en Colombia[28], se puede identificar como grupos guerrilleros han atacado infraestructura de telecomunicaciones, dejando incomunicados a usuarios e instituciones públicas. Bajo esa lógica, la destrucción de la infraestructura de las telecomunicaciones forma parte de la estrategia para lograrlo. También, se alerta que la desconexión dificulta la respuesta de las autoridades, aumenta la impunidad y el poder de las organizaciones criminales cuando ocurren operativos para combatir o capturar a jefes criminales.

**27.** Bravo, Jorge. (2023, 25 de agosto). Crimen organizado ataca infraestructura de telecomunicaciones. Proceso.
**28.** Diario La Libertad. (2020, 16 de febrero). Con explosivos guerrilla intentó derribar torre de antenas en Río de Oro-Ocaña (Norte de Santander). Diario La Libertad.

# 4. Consecuencias del robo de cables y vandalismo de las telecomunicaciones

El robo de cables y vandalismo a infraestructuras de telecomunicaciones tiene impactos y consecuencias directas e indirectas para todos los involucrados en la cadena de valor de los servicios de conectividad: usuarios, operadores, gobiernos y comunidades en las cuales se desarrollan los incidentes.

## Afectaciones directas a usuarios, comunidades y sectores productivos

Un sondeo a operadores en diversos países de la región muestra que **58%** de ellos registran un aumento significativo o moderado en los usuarios afectados por robo y otras interferencias con su infraestructura. Por otro lado, se observan avances en países como Argentina, Uruguay y Paraguay donde existe una disminución moderada de los usuarios impactados o Chile con una reducción significativa.

**Un sondeo a operadores en diversos países de la región muestra que 58% de ellos registran un aumento significativo o moderado en los usuarios afectados por robo y otras interferencias con su infraestructura.**

Los incidentes de robo y vandalismo en instalaciones de operadores de conectividad detonan una serie de consecuencias inmediatas para las comunidades donde se encuentran.

## Inseguridad contextual

La ocurrencia de incidentes de robo y vandalismo es en sí mismo un indicador de la vulnerabilidad e inseguridad comunitaria que hace atractivo a ciertos puntos de infraestructura para ser atacados por grupos criminales que operan y proliferan en la zona. Algunos mecanismos de prevención y fortalecimiento de la seguridad comunitaria tendrían externalidades positivas inmediatas no solo para la protección de instalaciones, sino también para la seguridad del entorno inmediato.

## Vulneración de las instalaciones y riesgo físico para las inmediaciones

La interferencia y daño de cables, postes, perímetros de seguridad, instalaciones eléctricas, antenas y otros componentes y equipos inducen el riesgo de funcionamiento defectuoso que podría desembocar en desastres como incendios, desplomes, descargas eléctricas y otro tipo de incidentes que vulneran la seguridad física en el perímetro de las instalaciones.

## Interrupción de los servicios de conectividad y telecomunicaciones

Las afectaciones a las instalaciones derivan usualmente en algún tipo de discontinuidad o variabilidad de calidad en la provisión de servicios tanto de telefonía, internet fijo, móvil y satelital, así como servicios de televisión. La interrupción de servicios implica una incapacidad para utilizar los recursos tecnológicos y redes para actividades cotidianas como la comunicación, consumo de información, así como uso para temas educativos, laborales, comerciales y productivos.

Adicionalmente, la consulta con empresas de telecomunicaciones señala que el tiempo promedio de disrupción, entre el incidente y la reparación de las afectaciones puede ir de **3 a 12 horas** dependiendo de las dificultades geográficas, técnicas y propias de las comunidades. Sin embargo, en algunos casos estas afectaciones se pueden extender por entre **1 y 3 días**, especialmente cuando el daño se realiza en otros equipos como baterías y componentes eléctricos. Algunos operadores mencionan obstáculos adicionales para la atención a incidentes por falta de acceso oportuno a materiales importados debido a restricciones a la importación, así como la imposibilidad de reposición de componentes por obsolescencia de la tecnología.

### Desconfianza, incertidumbre y baja valoración de los servicios

Los usuarios que observan falta de continuidad o calidad en los servicios de telecomunicaciones podrían experimentar una baja en la confianza y certidumbre sobre los servicios contratados, así como una pérdida de valor recibido como consumidores. Por ejemplo, **9 de cada 10** operadores locales de telecomunicaciones encuestados mencionan a los daños reputacionales a las empresas como un impacto de los ataques a sus instalaciones e infraestructuras, y **7 de cada 10** ubican a la inconformidad de los usuarios como una consecuencia directa en materia de servicio al cliente. Adicionalmente, **63%** de los encuestados dicen que el impacto negativo en la reputación de la empresa es alto o muy alto frente a este tipo de incidentes.

## Impactos y costos económicos para operadores de telecomunicaciones

De acuerdo con la consulta a operadores locales de telecomunicaciones, un **47%** señala haber registrado un aumento significativo en los costos relacionados con incidentes de robo y afectaciones a infraestructura en los últimos 5 años, mientras un **13%** adicional indica un aumento moderado en estos gastos[29].

En **Brasil**, durante 2023 se robaron más de 5,4 millones de metros de cables de telecomunicaciones afectando a más de 7,6 millones de usuarios[30]. En el caso de **Colombia**, entre 2023 y 2024, Movistar[31] registró cerca de 13.500 casos de hurto con afectaciones para más de 300 mil usuarios y tan solo en 2023 reflejando pérdidas por 1,8 millones de dólares[32]; en 2022 Tigo[33] reportó 2.000 instancias de robo que representaron 27.000 horas de desconexión para más de 293.000 hogares afectados; tan solo en Bogotá los costos por este crimen sumaron 3.5 millones de dólares[34]. Telecom y Telefónica en **Argentina**[35] calculaban afectaciones económicas por entre 7 y 8 millones de dólares por vandalismo de infraestructura en 2020.

**29.** Una brecha identificada durante el desarrollo de este estudio se encuentra en la falta de datos agregados suficientes sobre el robo de cables y vandalismo en los países de América Latina para realizar estimaciones regionales y ejercicios de comparación efectivos. Esto es una barrera que impide conocer con mayor exactitud la magnitud de este fenómeno y su impacto en la región.
**30.** Conexis Brasil Digital. (2024). Mais de 5,4 milhões de metros de cabos de telecom foram roubados em 2023.
**31.** Telefónica Movistar Colombia. (2024). Movistar presenta campaña "La ruta del cable perdido".
**32.** Telefónica Movistar Colombia. (2024). 270 mil clientes de Movistar se vieron afectados por el hurto de infraestructura en el 2023.
**33.** Mi Oriente. (2024). Robo de cable en Colombia afectó a 293.000 hogares y negocios durante 2023.
**34.** Concejo de Bogotá. (2024). En el 2023 en Bogotá se hurtaron en cobre el total de kilómetros equivalente a la distancia entre Bogotá y Cartagena.
**35.** Rodríguez, J. M. (2020). Robo de cables: un delito con miles de damnificados y perjuicios millonarios. La Nación.

**El 81% de las operadoras encuestadas tienen la percepción de que la demora en la resolución de casos e incidentes impone retos e impacta directamente en la gestión administrativa y operativa de las empresas de telecomunicaciones.**

Durante 2022 en **Perú** se reportaron casos de hurto que afectaron a más de 95.000 personas[36] pero en otros años la cifra ha llegado a más de 350.000 usuarios[37]. Para el caso de **Chile**, Claro informó en una consulta costos en 2024 por 860 millones de dólares en afectaciones a infraestructura; Chile Telcos[38] informa de 60.000 eventos de robo entre 2020 y 2023 con 725.000 kilos de cables robados en 2022; además en 2020 Movistar registró 30.000 casos de vandalismo dejando sin conectividad a 1,5 millones de hogares así como[39]. En **Ecuador**[40], según un reporte del canal de televisión Ecuavisa, solamente en la provincia de Pichincha, provincia que incluye a la capital Quito se denunciaron pérdidas por USD 1.700.000 ante el vandalismo y el robo de cables. Por otro lado, en el año 2024, solamente la compañía del Grupo ICE en **Costa Rica**[41] denunció la pérdida de USD 1.600.000 por el vandalismo a su infraestructura.

## Daño a instalaciones y pérdida de materiales y equipos

El primer impacto directo del robo y vandalismo de infraestructura son las pérdidas (y los costos de reparación y recuperación) relacionadas con la sustracción forzada de materiales como cobre o fibra óptica, así como de equipos como baterías y componentes eléctricos. Más de la mitad (**56%**) de los operadores sondeados señala a la dificultad para recuperar las pérdidas por incidentes de este tipo como un impacto importante para sus empresas.

## Atención y resolución de incidentes

Una vez ocurridos e identificados los actos de robo y vandalismo es necesario para las empresas proveedoras de servicios de conectividad iniciar un proceso que implica la atención y resolución de los incidentes. Por un lado, es necesario gestionar un protocolo para atender técnica y físicamente los problemas de reparación del daño o sustracción, el funcionamiento de las redes y, en última instancia, de la entrega del servicio para los usuarios afectados. Por otro lado, existe la necesidad de dar seguimiento al caso legal y de seguridad de los casos, lo cual también implica destinar recursos humanos y financieros al seguimiento administrativo de los incidentes.

El **81%** de las operadoras encuestadas tienen la percepción de que la demora en la resolución de casos e incidentes impone retos e impacta directamente en la gestión administrativa y operativa de las empresas de telecomunicaciones.

## Mayores costos de operación e inversión en seguridad

Los dos tipos de impactos abordados anteriormente abonan a un incremento en los gastos necesarios para operar y gestionar servicios, así como en los costos de mantenimiento de sus redes e instalaciones. Además de los costos operativos, las empresas de telecomunicaciones deben invertir más en esquemas de seguridad para prevenir incidentes de robo y vandalismo en sus instalaciones.

El **100%** de los operadores consultados indican que los mayores costos de operación e inversión en seguridad son el principal impacto para las empresas proveedoras de servicios de conectividad.

**36.** Perú 21. (2024). Callao: 5 años de prisión efectiva a delincuente por robo de cables de telecomunicaciones.
**37.** IP Noticias. (2024). El robo de cables: un delito que crece y afecta a miles de usuarios.
**38.** Chile Telcos. (2024). Comisión Investigadora de la Cámara analiza redes delictuales y consecuencias del robo de cables.
**39.** Telesemana. (2022). En Chile se robaron más de 725.000 kilos de cables de telecomunicaciones en lo que va del año.
**40.** Redacción y Televistazo. (2025, 7 de febrero). Quito | Los habitantes de calle han robado cerca de USD 70 000 en cables de telefonía fija en el primer mes de 2025. Ecuavisa.
**41.** Arley, A. (2024, 17 de noviembre). Cifras de robo de cable bajan pero perjuicio económico sigue siendo alto. Radio Columbia.

### Seguros y costos financieros

Dentro de la muestra de operadores sondeados, **6 de cada 10** menciona que la prevalencia y recurrencia de incidentes de robo y vandalismo de infraestructura impone mayores primas de seguro para proteger su infraestructura, un costo financiero que va más allá de la atención inicial y los gastos operativos de las empresas.

### Multas, sanciones y riesgos de incumplimiento regulatorio

Las interrupciones y falta de continuidad en el servicio, así como la variabilidad en calidad y experiencia de usuarios suele imponer riesgos de cumplimiento regulatorio en algunos países. La falta de seguridad y garantías de protección de infraestructura de conectividad deteriora los indicadores de provisión y calidad de los servicios y abre posibilidades para que las empresas de telecomunicaciones sean señaladas y sancionadas. Lo anterior agrava las asimetrías regulatorias y de contributivas que existen entre las empresas de telecomunicaciones y las plataformas digitales convergentes que no tienen obligaciones ni sanciones frente a fallas, interrupciones y otras afectaciones a la calidad de servicios equiparables.

El **50%** de las operaciones locales encuestadas para esta investigación ponen al riesgo de recibir multas y penalizaciones, por aparentes incumplimientos de estándares de seguridad o continuidad y calidad en el servicio, como un impacto importante para los corporativos.

## Efectos del robo y vandalismo de telecomunicaciones para el cierre de brechas de conectividad, la transformación digital y la seguridad nacional relacionada con infraestructuras críticas

Los ataques a las instalaciones de telecomunicaciones ralentizan el desarrollo y despliegue de redes necesarias para reducir las brechas de cobertura y el aprovechamiento de la conectividad para la transformación digital regional. Esto es especialmente importante en zonas rurales y periurbanas donde la distancia a centros poblados y las dificultades de acceso favorecen el hurto de componentes y equipos de telecomunicaciones[42]. Este efecto se puede materializar en tres momentos. Primero, un efecto directo en zonas de alta la recurrencia de robo de cables y vandalismo es que los proyectos ejecutados de despliegue de infraestructura pierden rentabilidad de largo plazo al enfrentar mayores costos de operación: mantenimiento preventivo y correctivo, reparaciones, reinstalación de materiales y componentes, logística, gastos en seguridad, seguros, costos legales, compensaciones a usuarios afectados, así como multas por baja calidad o interrupción de servicio.

Segundo, el efecto indirecto sobre las decisiones de negocio respecto a la expansión de las redes en zonas conflictivas. Por un lado, mayores costos operativos por

**42.** El Morichal. (2024). La Policía recuperó baterías hurtadas a antenas de telefonía celular en Puerto Carreño. El Morichal.

**El impacto del robo y vandalismo de infraestructura abona a los problemas generales de sostenibilidad de la inversión e impone una carga financiera que se suma a otras complejidades del sector de telecomunicaciones**

mantenimiento y seguridad de las redes reducen la disponibilidad de recursos para inversión en cobertura, calidad y nuevas generaciones de tecnología. Es decir, el impacto del robo y vandalismo de infraestructura abona a los problemas generales de sostenibilidad de la inversión e impone una carga financiera que se suma a otras complejidades del sector de telecomunicaciones como costo de espectro, altas cargas regulatorias y dinámicas de mercado en detrimento de la rentabilidad necesaria para la expansión de la conectividad.

Por otro lado, una menor rentabilidad esperada desincentiva la inversión en infraestructura en ciertas zonas. De acuerdo con el sondeo realizado a operaciones locales de telecomunicaciones para esta investigación, **38%** de los operadores identifican una concentración de incidentes en los ámbitos urbanos especialmente en países como Brasil, Chile, Colombia, Costa Rica y República Dominicana. Casi **20%** indica que el problema es más intenso en zonas periurbanas con casos como Argentina, Uruguay y Paraguay. Un **26%** observa una carga de incidentes en zonas rurales particularmente en Ecuador y Guatemala (aunque también en los límites territoriales cercanos a la periferia urbana), mientras que **19%** parece observar una incidencia proporcional tanto en ámbitos urbanos, rurales y periurbanos (por ejemplo, en El Salvador, Honduras y Nicaragua).

En tercer lugar, incluso en aquellas zonas de alta incidencia de robo y vandalismo donde es posible desplegar infraestructura y cerrar brechas de cobertura, se puede reducir significativamente su impacto en términos de la calidad y continuidad del servicio, lo que limita la experiencia de usuarios, su capacidad de aprovechamiento productivo, comunitario y social, así como el ejercicio de derechos y el acceso a servicios digitales públicos y privados. Las interrupciones y la falta de confiabilidad en las redes de conectividad por este tipo de delitos dificultan el uso de tecnologías digitales para su uso y aprovechamiento productivo, lo cual se refleja en una falta de proliferación local de sectores y actividades económicas altamente digitalizadas o dependientes de la conectividad. Esto puede reducir el progreso social local y ampliar las desigualdades socioeconómicas regionales de aquellas zonas con bajo desarrollo digital frente a zonas con mayor seguridad de redes, urbanas y, en general, con mejores condiciones de acceso y uso de los servicios de conectividad.

Por último, es importante mencionar el tema de la seguridad relacionada con las infraestructuras críticas de los países. El robo de cables y vandalismo de infraestructuras de telecomunicaciones se trata de un asunto de seguridad nacional en la región ya que es considerada como parte de la infraestructura crítica de los países. La inacción por parte del Estado en este asunto podría tener impactos más allá del sector de las telecomunicaciones y la conectividad de los usuarios. Este crimen compromete servicios esenciales y vulnera la efectividad de infraestructura crítica para el desarrollo, la resiliencia y la defensa de las naciones.

### Una nota sobre la seguridad nacional y los cables submarinos

Los cables submarinos se encuentran en la primera milla dentro del sistema de las telecomunicaciones. Si bien, no se trata de un componente altamente susceptible al vandalismo del crimen organizado, en tiempos recientes se trata de una infraestructura que los países a nivel global comienzan a prestar atención a su protección.

En 2024, República Dominicana por medio del Instituto Dominicano de las Telecomunicaciones (Indotel) manifestó su apoyo a la Declaración Conjunta de Nueva York[43] sobre la seguridad y la resiliencia de los cables submarinos en un mundo globalmente digitalizado en el marco de la 79ª Asamblea General de las Naciones Unidas

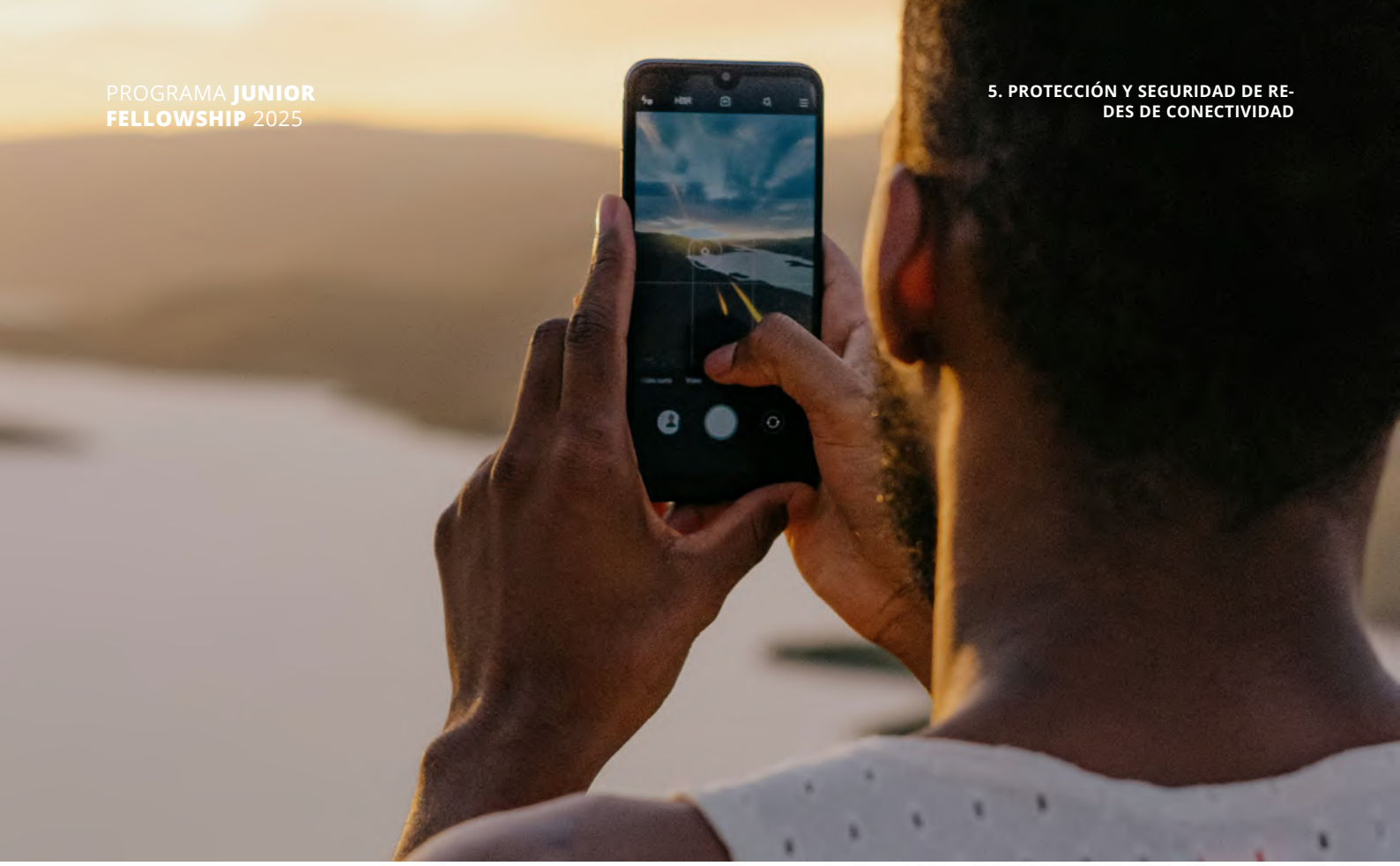
Por otro lado, durante 2022 en Argentina[44], se realizó el primer ejercicio conjunto de ciberdefensa y guerra electrónica para la protección de la infraestructuras críticas de las telecomunicaciones por parte de las Fuerzas Armadas de ese país. Este ensayo contó con la participación de 400 efectivos y se desarrolló en la población de Las Toninas, ya que en ese lugar se recibe cerca del 90% de tráfico de internet de Argentina mediante siete cables submarinos.

A nivel global, existen antecedentes recientes sobre la vulnerabilidad de los cables submarinos. En un informe publicado en julio de 2025 de la firma de ciberseguridad Recorded Future[45] alertó que los ataques deliberados a cables submarinos se encuentran como una nueva táctica de guerra híbrida. Entre los ejemplos más relevantes, se menciona el caso de noviembre 2024, donde los cables submarinos que conectan Lituania y Suecia fueron dañados. También, ocurrieron incidentes similares en otras regiones como el estrecho de Taiwán.

Ante esta realidad, resulta probable que más acciones vinculadas con la protección de los cables submarinos empiecen a tomar un mayor peso en la discusiones entre Estados, pero también entre los actores privados que administran dicha infraestructura.

En el caso de América Latina, según la firma Arizton en el informe *Latin America Data Center Construction Market – Industry Outlook & Market 2025-2030*, señalan que existen más de 80 cables submarinos que se conectan en la región. En conclusión, no se trata de un tema urgente de atención, pero si se trata de un asunto de primer orden cuando se evalúa y se implementa sistema de seguridad para el ecosistema de las telecomunicaciones.

**43.** Parra, R. (2024, 12 de noviembre). República Dominicana respalda declaración sobre protección de cables submarinos.
**44.** Unidiversidad. (2022, 17 de noviembre). Argentina se puso a prueba ante un escenario de "guerra electrónica".
**45.** Infobae. (2025, 20 de julio). Cables submarinos: la infraestructura crítica que sostiene al mundo en medio de constantes amenazas de sabotaje.



# 5. Protección y seguridad de redes de conectividad: retos y propuestas contra el robo de cables y el vandalismo de infraestructura de telecomunicaciones

Para construir una red segura frente al robo de cables y el vandalismo de las telecomunicaciones resulta necesario la conjunción de una serie de políticas enmarcadas en distintos segmentos de acción:

- Políticas de prevención y disuasión
- Políticas de protección de instalaciones y detección de incidentes
- Políticas de atención y seguimiento de incidentes

- Mecanismos coordinación con autoridades y comunidades contra el vandalismo de las telecomunicaciones
- Políticas de mitigación
- Políticas de combate a mercados ilegales adyacentes

A continuación, sobre la base de las experiencias identificadas en América Latina y el mundo se presentan una serie de retos y propuestas enmarcadas en estos seis conjuntos de políticas, cuya implementación debe ser coordinada para lograr resultados efectivos.

# Políticas de prevención y disuasión

## Tipificación del delito

Existe una diversidad de enfoques al momento de abordar el robo de cables y el vandalismo de las telecomunicaciones como delito. En diversas legislaciones la interpretación del acto está basada en los códigos penales y es considerado como un delito común. En la región, la tipificación de los crímenes relacionados con el robo y vandalismo de instalaciones de telecomunicaciones es un área donde se ha avanzado: solo **4 de cada 10** operadores encuestados señalan a la inadecuada definición de los delitos como un desafío legal relevante en sus países. Sin embargo, existen casos en los países de la región, donde se han modificado los códigos penales para especificar el delito de robo de cables y otras afectaciones a las instalaciones de telecomunicaciones como un delito grave.

En México ya desde el año 2015[46], se aprobó una modificación del Código Penal Federal, donde se calificaba al robo de cables de cobre como delito agravado y con mayores sanciones cuando provoque la interrupción de servicios públicos y básicos. A pesar de la aprobación en la Cámara de Diputados, esta propuesta no se llegó a concretar como Ley por parte del Senado. Sin embargo, se trata de un antecedente importante que se podría retomar en el futuro.

En el caso de Chile, durante el mes julio de 2025, se aprobó un proyecto de Ley[47] que endurece las sanciones para los delitos de robo, hurto y receptación de cables, incluyendo aquellos utilizados en las redes de telecomunicaciones. Entre las modificaciones más relevantes, se pueden identificar las modificaciones al Código Penal, donde se sustituye el concepto de "telefonía" por "telecomunicaciones". De acuerdo con la Cámara Chilena de Infraestructura Digital (IDICAM)[48] esta modificación permite incluir en el concepto las actuales redes digitales como la fibra óptica, torres, antenas y centros de datos.

En el caso de Brasil[49], también durante julio de 2025, se publicó la Ley N.º 15.181 que modifica el Código Penal para aumentar las sanciones aplicadas al robo, hurto y receptación de cables o equipos utilizados para la transferencia de datos, así como también cables de electricidad y cables de telefonía.

En Colombia[50], se incorpora adicionalmente este tipo de delito en el Código Penal, donde se estableció el concepto de defraudación de fluidos que incluye aquellas

**46.** Noroeste. (2025, 10 de septiembre). "Será delito grave robo de cable de cobre".
**47.** Cámara de Diputados de Chile. (2024). Informe para proyecto de ley sobre robo y vandalismo contra infraestructura de telecomunicaciones [Documento de comisión]. Cámara de Diputados de Chile.
**48.** IDICAM. (2025, 6 de agosto). IDICAM valora aprobación de ley que endurece sanciones por robo de cables de telecomunicaciones. Diario Estrategia.
**49.** Brasil. Lei n.° 15.181, de 28 de julho de 2025. Altera o Decreto-Lei n.° 2.848, de 7 de dezembro de 1940 (Código Penal). Diário Oficial da União.
**50.** Organización de los Estados Americanos (OEA). Ley 599 de 2000. Código Penal de Colombia.

**8 de cada 10 empresas de telecomunicaciones consultadas indican que los castigos inadecuados o penas insuficientes para perpetradores son temas críticos para el combate al robo y vandalismo de infraestructura.**

acciones que atenten contra los sistemas de energía eléctrica, agua, gas natural, o señal de telecomunicaciones con penas de prisión de hasta 72 meses, así como multas.

> **Reconocimiento claro del robo de cables como delito grave.** Ante estos antecedentes, una de las principales recomendaciones a nivel de políticas de sanciones, se trata sobre el reconocimiento explícito en los códigos penales y reglamentos sobre el robo de cables de cobre y vandalismo de las telecomunicaciones para tener una base que permita establecer la tipificación del delito, penas, multas y reparaciones más específicas. Esto puede incidir en menos escenarios de impunidad.

## Penas, sanciones y multas

En contraste con el tema de la tipificación del delito, **8 de cada 10** empresas de telecomunicaciones consultadas indican que los castigos inadecuados o penas insuficientes para perpetradores son temas críticos para el combate al robo y vandalismo de infraestructura. Las penas aplicadas por este tipo de delitos pueden variar en función de las disposiciones establecidas en los códigos penales, así como también de aquellos factores que se pueden considerar agravantes. No obstante, hay dos formas generales para aplicar estas sanciones. Una forma es el tratamiento del robo de cables y vandalismo de las telecomunicaciones como un delito común. La otra forma es el tratamiento diferenciado y específico al delito del robo de cables como un ataque a infraestructura crítica.

Lo anterior pone de relieve la necesidad de ajustar la severidad y configuración de penas alrededor de estos delitos. Un antecedente importante en esta línea se puede ubicar en agosto de 2025, cuando las cuatro principales asociaciones de telecomunicaciones de Estados Unidos[51] enviaron una carta dirigida a la secretaria de Seguridad Nacional, Kristi Noem, y al director del FBI, Kash Patel, advirtiendo sobre las afectaciones por el robo de cable cobre y fibra óptica, así como de actos vandálicos. En dicha carta, se hace un llamado a la acción a través de leyes y sanciones más severas para que todos los ataques a redes privadas de telecomunicaciones sean considerados delitos federales.

Otro ejemplo es el caso de Indonesia[52], donde se propone una política para la seguridad de los activos críticos nacionales en el sector de las telecomunicaciones. Esta propuesta está basada en la creación de un reglamento que incluye mecanismos integrales que abarcan los procedimientos para la identificación, evaluación y gestión de la infraestructura de las telecomunicaciones. También señala algunas obligaciones que las operadoras deben cumplir como la adaptación de las instalaciones, infraestructura y operaciones a los estándares fijados por la policía nacional. Este reglamento se basa en un esfuerzo coordinado entre el Ministerio de Comunicaciones y Tecnologías de la Información, la Unidad de Gestión de Bienes Nacionales Estratégicos, la Policía Nacional de Indonesia y las Fuerzas Armadas de Indonesia (TNI).

En Paraguay, de acuerdo con una investigación de la Universidad Nacional de Itapúa[53], el Ministerio Público de ese país ha calificado el robo de cables como hurto

**51.** Red Fibra. (2025, 7 de agosto). Telecomunicaciones en EE. UU.: asociaciones exigen medidas federales contra ataques a la infraestructura.
**52.** Galih Ariprawira, Lessy Sutiyono Aji, Ade Wahyudin & Alfin Hikmaturokhman. (2023, diciembre). Policy Mechanism for Security of National Vital Objects in the Telecommunications Sector in Indonesia. Buletin Pos dan Telekomunikasi, 21(2), 57-73.
**53.** Caballero Ramírez, N. B. (2023). Hurto de cables. Un delito complejo 2021-2022. Ciencia Latina Revista Científica Multidisciplinar, 7(1), 9075-9094.

agravado que se encuentra tipificado en el código penal. En ese sentido, las penas por este tipo de delito pueden variar entre 6 meses y hasta 10 años de prisión. Sin embargo, se afirma que, por este tipo de delito, no suelen darse penas privativas de la libertad largas. Además, la inexistencia de una indicación penal específica que contemple el hurto de cables deriva en que se aplique el delito de hurto agravado sin considerar el hecho que este robo puede tener un impacto en la integridad de las telecomunicaciones y las repercusiones hacia posibles afectados. Este caso de Paraguay refleja una realidad a nivel legal observada también en otros países: brinda una aproximación sobre las limitaciones que impone el tratamiento legal en países donde no se ha tipificado de manera específica el robo de cables en los sistemas de telecomunicaciones.

En el caso de Paraguay, se puede observar que, se pone un límite al tipo de pena sobre la base al valor de la cosa objeto del hurto. Por ejemplo, cuando el robo de cables sea menor a 10 salarios mínimos diarios legales vigentes (aproximadamente USD 124), este robo será considerado como hurto simple. Además, según afirma la Universidad Nacional de Itapúa, cuando los autores de estos delitos son hallados en flagrancia, suelen recuperar inmediatamente su libertad, a través de la aplicación de medidas procesales vigentes en el Código Penal de ese país.

Por otro lado, considerando las legislaciones recientes de Brasil y Chile, donde sí hay una tipificación específica para el robo de cables de cobre y otros vandalismos de las telecomunicaciones (ver sección anterior), se pueden identificar las siguientes penas.

Según la Ley N.º 15.181 de Brasil, se indica que las penas por robos de cables son de 2 a 8 años de prisión, acompañadas de una multa. De igual manera, se establece que se aplican penas dobles, si el delito de robo de cables se comete con motivo de una calamidad pública. Se señala también en la Ley el establecimiento de penas de prisión de 6 a 12 años y multa, si la sustracción de cables se comete contra cualquier bien que comprometa el funcionamiento de los órganos del Estado brasileño o establecimientos privados que presten servicios públicos esenciales.

En el caso de Chile, se agregó una modificación al artículo 448 del Código Penal, agregando un apartado donde se indica que, el que robe o hurte cables de cobre, comete el delito de sustracción de cable de cobre y será sancionado con las penas, entre 3 y 5 años de prisión. Igualmente, se establece multas que pueden alcanzar las 400 Unidades Tributarias Mensuales (UTM), que equivale aproximadamente a más de USD 28.000. En dicho artículo se indica también una pena accesoria a quien robe y hurte cobre proveniente de cables destinados al uso de alumbrado público, conexiones de energía, fibra óptica o cualquier uso similar. En función de la cantidad de cobre robado, se establecen multas que pueden alcanzar 100 Unidades Tributarias Mensuales (aproximadamente USD 7.200).

> **Penas, sanciones y multas disuasivas.** Considerando los antecedentes de los países mencionados, una propuesta importante de aplicar se trata sobre el establecimiento de penas y sanciones efectivas por el robo de cables y el vandalismo de las telecomunicaciones. El tiempo de privación de libertad dependerá de la jurisprudencia de cada país. Sin embargo, la pena debería ser en un grado suficientemente largo como para disuadir de cometer delitos contra la infraestructura de telecomunicaciones.

**Categorizar agravantes del delito de acuerdo a su impacto comunitario y económico.** Adicionalmente, se puede sugerir la consideración de ciertos agravantes en función de las características del delito. Esto debería estar basado en la cantidad de material robado y por otros factores como si el delito tiene un daño perjudicial en terceros de forma directa y si fue vandalizado bienes públicos, privados o críticos.

### Sanciones al comercio ilícito de cobre, baterías y otros componentes de infraestructura

Cuando se aborda el problema del robo de cables y el vandalismo a la infraestructura de telecomunicaciones, resulta importante recordar que el delito forma parte de un ecosistema donde participan recicladoras, fundidoras y puertos. En ese sentido, se pueden ubicar apartados en ciertas legislaciones que buscan sancionar a otros actores que forman parte directa o indirecta de estas redes criminales.

En el caso de Chile, cuando se abordó la modificación del artículo 448 del Código Penal, también se establecieron multas para aquellas personas con tenencia de cobre proveniente de cables destinados a uso de alumbrado público. Estas multas también pueden alcanzar 100 Unidades Tributarias Mensuales (aproximadamente USD 7.200).

En el caso de Brasil con la Ley N.º 15.181, se impone una reclusión de 3 a 8 años, acompañada de multas para aquellos que adquieran, reciban, transporten, oculten o saquen provecho propio o ajeno de cables robados o equipos utilizados para la transmisión de telefonía y transferencia de datos. De igual manera, se indica que, aquellos operadores de telecomunicaciones que utilicen en sus actividades cables o equipos que sepan o deban saber que son producto de un delito estarán sujetos a sanciones determinadas en el Código Penal. También, se consideran clandestina las actividades de telecomunicaciones que usen cables o equipos que sean producto de algún delito.

**Sanciones a las cadenas de comercio ilícito de cobre y baterías.** Una propuesta necesaria se trata de la sanción efectiva para todos aquellos entes que forman parte de la cadena de mercado negro del cobre y batería, así como de otros componentes en la infraestructura de las telecomunicaciones. Esto debe apuntar con especial atención a fundidoras de metales y chatarrerías. De igual manera, los servicios de transportes, exportación y rastreos de estos materiales deben ser incluidos como actores susceptibles de penas y sanciones.

## Comunicación disuasoria y modernización de redes para desincentivar la demanda de cobre

### Señalización e identificación clara sobre cableado de fibra óptica

A diferencia del cable de cobre, el cable de fibra óptica no se puede reutilizar ni vender fácilmente. Por esta razón, una práctica básica y reiterada por parte de operadoras es la señalización de los cables de fibra óptica para evitar su hurto. La mitad de los

operadores consultados mencionan a la señalización como una de sus principales medidas de prevención contra el robo de cables.

La implementación de esta propuesta consiste en la instalación de carteles en postes o puertos de cableado que indiquen de forma clara y explícita que los cables instalados en determinadas zonas se tratan específicamente de cables de fibra óptica y no de cables de cobre. Esta medida parte de una suposición basada en la aceptación de la señalización por parte de los actores dedicados al vandalismo y busca reducir el incentivo de grupos criminales para robar un material que no podrá ser reutilizado ni vendido en el mercado negro.

Se pueden identificar prácticas de esta naturaleza sugeridas por actores como la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes de Bolivia, así como por parte de la Asociación Chilena de Telecomunicaciones.

Adicionalmente, es posible complementar estas señalizaciones con comunicación efectiva sobre las afectaciones comunitarias y las consecuencias legales de interferir con la infraestructura crítica de telecomunicaciones, así como hacer explícitas otras medidas de vigilancia, rastreo e investigación que podrían ser utilizadas en contra de los perpetradores.

> **Señalización e identificación clara sobre cableado de fibra óptica.** La colocación de señalizaciones sobre aquel cableado que sea de fibra óptica es necesaria para prevenir y disuadir cortes y daños con intención de robo. Sin embargo, esto no garantiza que los intentos de robo disminuyan automáticamente.

### Incentivos para la modernización del cableado de cobre a fibra óptica

La sustitución del cableado de cobre por fibra óptica también es una estrategia de prevención. La modernización y ampliación de las redes de fibra óptica[54] en sustitución del cableado de cobre[55] a nivel masivo permitirían reducir la efectividad de los grupos del crimen organizado en sus actividades de búsqueda y robo de cobre. Debido a que las redes de fibra óptica no son rentables para la delincuencia por su dificultad de monetización. Una menor disponibilidad de cobre en las redes disminuiría la probabilidad de éxito de los ataques, incrementa el costo de las actividades delictivas de búsqueda y reduce el atractivo económico del daño y robo de cableado.

El argumento de la protección de las redes sumado a la necesidad de ofrecer una mejor conectividad a comunidades podría ser una base para plantear una modernización del cableado de las telecomunicaciones en aquellas zonas más vulnerables.

> **Facilitación regulatoria y apoyo para la modernización del cableado de cobre a fibra óptica en zonas de alta incidencia de robo.** En ese sentido, el papel de los entes reguladores y las autoridades podría estar enmarcado en facilitar todas las gestiones administrativas y permisos para darle prioridad a la sustitución del cableado en aquellas zonas con mayor incidencia de robo. Esto podría estar acompañado con una publicidad en la zona que comunique dicha

**54.** CRHoy. (2024, 15 de septiembre). Ampliación de red de fibra óptica solucionaría problema del robo de cable.
**55.** También se puede plantear la opción de utilizar aluminio en lugar de cobre para el cableado.

sustitución para así desincentivar el corte de cables en la búsqueda de cobre. Adicionalmente, en aquellos mercados donde la presión financiera dificulte la inversión en fibra óptica es posible pensar en esquemas de incentivos y apoyos para la modernización de redes en comunidades vulnerables al delito en infraestructuras (por ejemplo, con uso de recursos de Servicio Universal u otros mecanismos de financiamiento público).

No obstante, estas recomendaciones podrían revalorizar y hacer más atractivo relativamente el focalizar los esfuerzos criminales en otros componentes como las baterías, equipos eléctricos y componentes valiosos de las instalaciones que seguirán enfrentando una alta vulnerabilidad. Adicionalmente, la modernización de cableado y su respectiva señalización podría facilitar la identificación de cables de fibra óptica para objetivos distintos al robo, como por ejemplo para vandalismo para sabotear las comunicaciones en comunidades para efectos de control, terrorismo o guerrilla.

# Políticas de protección de instalaciones y detección de incidentes

## Apoyo financiero para adopción de sistemas de monitoreo, seguridad física y nuevas tecnologías de apoyo

En el mercado de empresas especializadas en servicios de protección a infraestructura se pueden identificar algunas tendencias en materia de sistemas de seguridad para instalaciones de telecomunicaciones. Al menos **9 de cada 10** operadores encuestados indica que implementa medidas de seguridad como la vigilancia, monitoreo e inspección de sus instalaciones, así como servicios de seguridad, patrullaje y elementos de seguridad física (alarmas, cercas, etc.). De acuerdo con las empresas consultadas, un **75%** emplea tecnologías de monitoreo y análisis de datos para la vigilancia de sus instalaciones. Algunas empresas mencionan otras medidas como sistemas GPS para la localización de baterías o diversas medidas de protección física para componentes de su infraestructura (contratapas para cámaras de fibra óptica, soterramiento de baterías, jaulas, plataformas, instalaciones elevadas, etc.).

Es importante reconocer la inversión que realizan los operadores de telecomunicaciones en sistemas monitoreo y tecnologías para evitar y mitigar los crímenes en contra de su infraestructura. Ante la falta de seguridad pública, las empresas incurren en sobrecostos que impactan en la sostenibilidad financiera de la industria. Por ello, las autoridades y reguladores podrían implementar mecanismos de apoyo y financiamiento de medidas y sistemas de seguridad en las que incurran los operadores.

De acuerdo con las propias empresas, **25%** de ellas estiman como poco efectivas las medidas implementadas, especialmente en Centro América, mientras que **30%** observa una alta efectividad de sus medidas de protección, y el resto considera

que sus esfuerzos suelen ayudar a prevenir y reducir incidentes en sus instalaciones pero de manera moderada.

Algunas buenas prácticas podrían implementarse en América Latina. Por ejemplo, en Estados Unidos, algunos proveedores para instalaciones gubernamentales[56], en su oferta de servicios, proponen una serie de acciones para combatir el vandalismo de las telecomunicaciones como cercados electrificados, sistemas de monitoreo con drones, iluminación con detección de movimiento y regulación estricta en la compraventa de metales.

En Bogotá[57] se han implementado acciones preventivas como la marcación de tapas y cables para identificar que están libres de cobre, así como el sellado de tapas con diferentes métodos para dificultar el acceso de la delincuencia a las redes subterráneas. Esto se complementa con un aumento del personal de seguridad que monitorea zonas de la capital colombiana con la finalidad de prevenir la consolidación del delito. De igual manera, la empresa contratista del gobierno británico, Intelligence Fusion[58] propone soluciones ante las amenazas físicas para las telecomunicaciones y el robo organizado de cables de cobre bajo el uso de tecnologías de monitoreo en tiempo real con sensores IoT, colaboración con autoridades, reemplazo de cobre por fibra óptica y refuerzos físicos, a través de bloqueos de concreto y reubicación de torres en zonas menos accesibles.

La Universidad de Botswana[59] realizó una investigación acerca de propuestas de marcos de gestión de seguridad para las telecomunicaciones en África. En este análisis, se sugiere medidas para fortalecer la seguridad de la infraestructura de las telecomunicaciones basada en acciones cómo la implementación de sistemas de videovigilancia en ubicaciones estratégicas para el monitoreo de equipos. También, se sugiere la necesidad de realizar pruebas de seguridad periódicas para detectar vulnerabilidades. También se insiste en la capacitación del personal de las operadoras para desarrollar las habilidades necesarias para la prevención del vandalismo.

En un estudio de la Universidad de Energía Eléctrica del Norte de China[60] acerca de las auditorías de seguridad física para servicios públicos, se indica que, los modelos predictivos basados en SIG (Sistemas de Información Geográfica) y aprendizaje automático pueden ser una alternativa para combatir el robo de cable de cobre en infraestructuras críticas. El modelo propuesto tiene la capacidad de identificar áreas de alto riesgo para el robo de cables y vandalismos de la infraestructura de las telecomunicaciones, considerando factores como la proximidad a chatarrerías ilegales y la oscilación de precios del cobre como detonantes clave. De igual manera, sugieren estrategias geolocalizadas (patrullas inteligentes, sensores en puntos críticos) y políticas de regulación de mercados de metales.

También, se puede identificar una propuesta en Malasia realizada por la Universidad de Malasia Perlis[61], basada en un sistema de alerta en tiempo real para la detección de robos y cortes de cable, que utiliza un microcontrolador y tecnología GSM. A través de un dispositivo, se muestra la ubicación del corte de cable y se envía dicha información por SMS al teléfono móvil de las autoridades correspondientes y operadoras afectadas.

**56.** Gibson, K. (2023, 30 de junio). 9 Security Threats Facing Power Plants. AMAROK.
**57.** Ruíz Rojas, A. (2023, 3 de noviembre). ETB e Integración Social se unen para promover la denuncia de vandalismo contra redes de Internet. Secretaría Distrital de Integración Social de Bogotá.
**58.** Arends, A. (2023, 30 de junio). Protect your business: Unveiling the top physical security threats to the telecom industry. Intelligence Fusion.
**59.** Okike, E. U., & Seboko, B. E. (2022). A Security Management Framework for Telecommunications in Africa. Journal of Internet Technology and Secured Transactions, 10(1).
**60.** Mahato, N. K., Yang, J., Yang, J., Gong, G., & Hao, J. (2024). Physical Security Auditing for Utilities: A Guide to Resilient Substation. Safety, 10(3), 80.
**61.** Lim, E. K., Norizan, M. N., Mohamad, I. S., Yasin, M. N. M., Murad, S. A. Z., Baharum, N. A., & Jamalullail, N. (2017). Design of anti-theft/cable cut real time alert system for copper cable using microcontroller and GSM technology. AIP Conference Proceedings, 1885, Article 020287.

De igual manera, en el caso de Sri Lanka, se puede identificar una propuesta por parte de la Universidad de Wayamba[62], donde se señala que, las torres y estaciones base (BTS) requieren de instalación de sensores inteligentes y con alarmas que puedan transmitir la señal a los cuerpos policiales y los entes responsables de la seguridad por parte de las operadoras de telecomunicaciones. Por ejemplo, se menciona la detección de acciones delictivas a través de sistemas de alerta temprana, con apoyo de sensores de movimiento y videocámaras. Luego, se menciona la disuasión a través de vallas e iluminación de aquellos recintos susceptibles de robo. Además, se menciona que el uso de vallas puede retrasar o dificultar la sustracción de cables u otros materiales.

En el Reino Unido, también se pueden ubicar prácticas innovadoras, en este caso por parte de operadores y gestores de infraestructura. Un ejemplo es la empresa Openreach[63] que logró disminuir el robo de cables en 30% entre 2023 y 2024. Entre sus principales acciones para disminuir los robos se encuentra el recubrimiento de sus cables subterráneos con un líquido especial llamado SelectaDNA. Este líquido tiene un "ADN sintético" y brilla bajo luz ultravioleta. Cuando alguien toca los cables, este líquido invisible se queda en su piel, ropa o vehículo, dejando una marca única. Así, en caso de que la policía encuentre el material robado (o inspeccione a personas, vehículos e instalaciones sospechosas) sería posible facilitar la presentación de pruebas del delito y determinar el origen del robo.

Los sistemas de seguridad a implementar requieren de objetivos claros a nivel prevención para utilizar la tecnología más adecuada. En el caso de los sistemas de videovigilancia, existen múltiples tipos como cámaras de alta resolución, cámara con visión nocturna, cámaras panorámicas o cámaras con detección de movimiento. Cada una tiene sus ventajas y usos particulares en función de las necesidades de seguridad.

De igual manera, existen otros elementos que se deben considerar como los tipos de iluminación, así como los tipos de cerraduras o barreras físicas como pueden ser las cercas reforzadas, portones de seguridad o cerraduras electrónicas y biométricas. También, se menciona la importancia de considerar los tipos sistemas de monitoreo como aquellos de tiempo real, las alertas automáticas, las alarmas sonoras, visuales, silenciosas o con notificación remota.

Con el advenimiento de la Inteligencia Artificial (AI), existe la posibilidad de implementar sistemas que analizan patrones de comportamiento y anticiparse a robos y daños a la infraestructura. Sin embargo, para esto se requiere una gestión de datos y registro de la incidencia con suficiente detalle que permita realizar dichos análisis.

Existen sistemas de seguridad pensados para los operadores de infraestructuras de las telecomunicaciones basados en videovigilancia, sensores inteligentes, alertas en tiempo real e inclusive análisis predictivos con uso de AI. Pero es importante advertir que, estos esfuerzos pueden resultar insuficientes para la prevención del crimen, si no existe una interoperabilidad con los cuerpos de seguridad.

En ese sentido, resulta necesario plantear sistemas de seguridad que se puedan integrar con los cuerpos de seguridad. Sin embargo, ello plantearía el reto de que

**62.** Madugalla, M. S. N., & Kumarayapa, Y. A. A. (2014). Security system for protecting expensive copper cables from robbers at isolated telecommunication towers. Proceedings of the Annual Symposium on Research & Industrial Training, 1, 175–178. Department of Electronics, Wayamba University of Sri Lanka.
**63.** O'Halloran, J. (2024, 29 de abril). Openreach reaps benefit of invisible DNA marking with cable thefts down 30%. Computer Weekly.

las diversas tecnologías de seguridad de las operadoras sean compatibles con los sistemas de seguridad públicos.

**Sistemas de seguridad apoyados en tecnología.** Existen sistemas de seguridad basado en videovigilancia, sensores inteligentes, alertas en tiempo real e inclusive análisis predictivos con uso de AI. Sin embargo, estos esfuerzos pueden resultar insuficientes para la prevención del crimen, si no existe una interoperabilidad con los cuerpos de seguridad. En ese sentido, resulta necesario plantear sistemas de seguridad que se puedan integrar con los cuerpos de seguridad. Sin embargo, ello plantearía el reto de que las diversas tecnologías de seguridad de las operadoras sean compatibles con los sistemas de seguridad públicos.

Adicionalmente, se debe considerar los costos adicionales que deben enfrentar los operadores de infraestructura de telecomunicaciones en la protección, vigilancia y monitoreo de sus instalaciones. En un esfuerzo conjunto de las empresas de comunicaciones y las autoridades competentes es necesario incluir aspectos financieros como la coinversión en sistemas de protección de redes en donde la incidencia delictiva relacionada con la infraestructura no haya sido estabilizada, y la colaboración para la reducción de la inseguridad pública en ciertas zonas de cobertura.

# Políticas de atención y seguimiento de incidentes

## Respuesta y seguimiento de casos de robo y vandalismo

Uno de los aspectos más relevantes del fenómeno de vandalismo de instalaciones de infraestructura es el de la capacidad de las autoridades para atender los incidentes, investigar y dar seguimiento judicial a los casos. Dentro del sondeo a empresas de telecomunicaciones de la región se encuentra que poco más del **60%** de los operadores consultados observa una alta complejidad para reportar y dar seguimiento judicial a incidentes. Además, entre **70%** y **90%** de los operadores percibe una incapacidad de respuesta rápida y para realizar investigaciones efectivas por incidentes ocurridos. Y por último, **8 de cada 10** empresas registran complicaciones para llevar a juicio o castigar adecuadamente a los perpetradores. Lo anterior deriva en que **9 de cada 10** empresas de telecomunicaciones encuestadas en América Latina tenga la opinión de que la efectividad de respuesta y resolución de incidentes por parte de autoridades es baja.

Los operadores consultados consideran algunos retos y desafíos importantes que las autoridades necesitan enfrentar para mejorar la atención y resolución de casos de robo y vandalismo. Uno de ellos es que las autoridades y reguladores nacionales no suelen tener competencia local en el involucramiento de temas relacionados con incidentes sobre obra civil, instalaciones o cableados. Su colaboración podría ayudar especialmente en temas como registro de incidentes y reducción de riesgos de sanciones regulatorias por interrupción de servicio por daños a infraestructura.

**Las autoridades y reguladores nacionales no suelen tener competencia local en el involucramiento de temas relacionados con incidentes sobre obra civil, instalaciones o cableados.**

Por otra parte, el seguimiento policial y judicial de las denuncias por incidentes en instalaciones es competencia local lo cual deriva en complejidades propias de la fragmentación y falta de homologación legal y judicial: dispersión de autoridades, burocracia administrativa, procedimientos y protocolos poco efectivos para dar seguimiento a incidentes, sobrecarga laboral de casos en departamentos de policía, en fiscalías y en procesos judiciales, así como falta de capacidades presupuestarias y/o técnicas de funcionarios e instituciones involucradas en los casos delictivos.

La identificación, captura e imputación de responsables es complicada de llevar a cabo en la gran mayoría de los incidentes. En buena medida la falta de eficacia en estos procesos se debe a factores como la dificultad para integrar y tramitar informes y pruebas suficientes para las autoridades locales. Las denuncias policiales y las investigaciones de las fiscalías suelen tomar años para su resolución, con diversos factores penales que complejizan los procesos judiciales. Por ejemplo, en algunos países a pesar de existir un mandato legal para investigar delitos denunciados, el aporte de los indicios para identificar responsables y someterlo a procesos penales recae en los operadores de infraestructura. Esto dificulta la efectividad de las denuncias.

Por último, en algunos países no existen normativas que regulen procedimientos específicos de los delitos relacionados con el robo de cables o daños a infraestructura de telecomunicaciones. Tampoco se plantean instrumentos de coordinación entre operadores, gobiernos y policía.

**Fortalecimiento de respuesta y judicialización efectiva de incidentes.** De manera general las autoridades nacionales como locales deben generar políticas públicas que ayuden a las autoridades policiales, fiscalías e instituciones de procuración de justicia para tener mayores capacidades operativas para dar respuesta y atención a los casos de robo y vandalismo de infraestructura.

Los gobiernos locales pueden apoyar con cámaras y otros mecanismos de vigilancia como planes de patrullaje y alarmas comunitarias, sobre todo en zonas críticas y vulnerables a ataques.

# Mecanismos coordinación con autoridades y comunidades contra el vandalismo de las telecomunicaciones

## Coordinación con agencias gubernamentales para la seguridad de las telecomunicaciones

En términos de prevención del delito, los espacios de coordinación entre instituciones públicas, empresas y comunidades resultan clave. El **75%** de las empresas de telecomunicaciones sondeadas mantienen alguna especie de

programa de colaboración con autoridades para el combate a los ataques a instalaciones. Existen varios casos en la región y a nivel global, que se pueden analizar.

En España el abordaje para combatir este fenómeno ha partido de un modelo de gobernanza, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)[64], que facilita la cooperación público-privada para el intercambio de información y acciones conjuntas. Dentro de las áreas estratégicas consideradas como infraestructura crítica, se encuentran las Tecnologías de la Información y las Comunicaciones (TIC), donde se incluyen las redes de telecomunicaciones.

Durante 2024 en Venezuela, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) y la CANTV acordaron trabajar en conjunto para garantizar la seguridad de las redes de telecomunicaciones[65].

En el caso de Panamá durante el año 2025[66], la Autoridad Nacional de los Servicios Públicos (ASEP), así como las operadoras de telecomunicaciones y cuerpos seguridad se reunieron para reforzar el plan de mitigación contra el vandalismo y hurto de cables de telecomunicaciones; y así, garantizar que los usuarios no se vean afectados por estas prácticas.

Hay ejemplos globales con modelos de gobernanza para la colaboración entre las operadoras y las instituciones de seguridad pública. Por ejemplo, en Estados Unidos existe la America's Cyber Defense Agency[67] (Agencia de Defensa Cibernética de Estados Unidos) que ayuda al sector privado de las telecomunicaciones a predecir, anticipar y responder a las interrupciones de los servicios de conectividad. También, se encuentra el caso de la ciudad de Los Ángeles, donde el gobierno local estableció un Grupo de Trabajo de Alambre de Cobre en 2024, cuya gestión permitió el arresto de 82 personas y la recuperación de 2.000 libras de material robado[68].

También se puede observar como una tendencia creciente la promulgación de leyes para proteger la infraestructura de las telecomunicaciones. Por ejemplo, en Brasil[69] ya desde el año 2021, se publicó un reglamento de ciberseguridad aplicado al sector de las telecomunicaciones para promover la seguridad en las redes y servicios de telecomunicaciones bajo la supervisión de la Agencia Nacional de Telecomunicaciones (ANATEL). También, se puede mencionar el caso de Chile con la promulgación de la Ley Marco de Ciberseguridad de Chile[70], que incluyen las infraestructuras telecomunicaciones y las tecnologías de la información como servicios esenciales sujetos a la protección.

Algunas prácticas identificadas en la región y a nivel internacional sugieren el establecimiento de canales de coordinación entre operadores de las redes de telecomunicaciones y autoridades públicas para prevenir el robo de cable y el vandalismo. En algunos países estas instancias son comisiones temporales y en otros casos son espacios permanentes de coordinación.

**Instancias de coordinación público-privada contra el vandalismo de las telecomunicaciones.** Ante la magnitud de este crimen, resulta necesario

**64.** LISA Institute. (s. f.). Infraestructuras críticas: definición, planes, riesgos y amenazas.
**65.** Primicia. (2024, 27 de diciembre). CICPC y Cantv definen estrategias para evitar robo de cables.
**66.** DPL News. (2025, 14 de marzo). Panamá | Reforzarán acciones contra vandalismo de cables. DPL News.
**67.** Cybersecurity and Infrastructure Security Agency (CISA). (s. f.). Communications Sector. En Critical Infrastructure Security and Resilience.
**68.** NCTA – The Internet & Television Association. (2024, 20 de noviembre). Protecting networks: Battling the rise in copper theft and vandalism. NCTA.
**69.** Azevedo Sette Advogados. (2021, 8 de febrero). Telecommunications Cybersecurity: Recent Developments.
**70.** Law Library of Congress. (2025, 30 de enero). Chile: Framework law on cybersecurity comes into force.

apostar por la articulación de colaboración entre empresas y autoridades (e incluso entre privados), con la participación de comunidades, policías, cuerpos de defensa, fiscalías e instituciones ministeriales y de procuración de justicia. Las principales áreas de colaboración deberían ser el intercambio de información sobre patrones de robo, rutas de alta conflictividad, modus operandi, instalación de sistemas de seguridad, capacitación y equipamiento de autoridades y empleados, así como monitoreo, seguimiento y evaluación de incidentes y políticas de atención.

Estas instancias no pueden ser órganos en los que solo participen los entes públicos con competencia en la regulación de las telecomunicaciones, resulta necesario ampliar ese espectro de participación para que exista una respuesta integral. Estas instancias de coordinación podrían establecer convenios de colaboración para impulsar líneas de acción como concientización y educación comunitaria, vigilancia, identificación de zonas vulnerables a ataques, líneas de denuncia y contacto para el diagnóstico, prevención, detección y atención a incidentes.

La colaboración entre autoridades del sector de telecomunicaciones, gobiernos locales, policías, fiscalías e instituciones de procuración de justicia es fundamental para brindar una atención especializada a crímenes de seguridad de las redes y la infraestructura de telecomunicaciones.

La estrategia podría complementarse con los organismos de ciberseguridad que actualmente se están desarrollando para prevenir ataques informáticos. Esto implica también que el tema de seguridad de las redes críticas sea considerada parte de la capa física de ciberseguridad, es decir abordar el tema no solo desde la perspectiva de la clasificación del delito y sanciones, sino de considerar la protección de las redes un aspecto clave de las agendas nacionales de ciberseguridad. El hurto de materiales, daño a las instalaciones y el vandalismo de infraestructura no es un delito menor ya que tiene implicaciones de seguridad para infraestructuras críticas y estratégicas.

### Instancias de cooperación con las comunidades

Un factor fundamental en la prevención de incidentes y ataques contra la infraestructura es la participación de las comunidades beneficiarias de la redes y servicios de telecomunicaciones en la protección de las instalaciones. La colaboración entre las operadoras, las autoridades y los ciudadanos para disuadir, detectar y denunciar cualquier actividad sospechosa puede resultar clave para reducir la incidencia de casos. No obstante, para que se consolide esa confianza para la denuncia sea efectiva, resulta importante que las operadoras mantengan canales abiertos de comunicación y relacionamiento comunitario. Lo anterior implica un trabajo de reconocimiento, vinculación, atención y reciprocidad con usuarios, clientes y poblaciones en zonas vulnerables.

El sondeo realizado a empresas de telecomunicaciones de la región muestra que **8 de cada 10** cuentan con teléfonos de denuncia o reporte de incidentes, pero solo **40%** implementa o usa sistemas de vigilancia comunitaria o vecinal. Asimismo,

falta penetración de programas que ofrezcan recompensas a ciudadanos que proporcionen información útil para la captura de responsables en incidentes de robo o ataques a instalaciones.

La Universidad Militar Nueva Granada de Colombia[71], en una investigación sobre los factores del hurto de cobre en la infraestructura de las telecomunicaciones, se señala que resulta necesario un "trabajo de calle" por parte de las operadoras y autoridades, que consiste en la articulación de redes de protección compuesta por la vigilancia comunitaria, así como el apoyo del comercio nocturno, las estaciones de servicio y la ciudadanía en general. Para ello, se recomienda que las autoridades, empresas de seguridad y las operadoras establezca contacto con las comunidades y con quienes transitan por zonas críticas para la infraestructura, ya que, si se crean vínculos adecuados, estos grupos se pueden convertir en una valiosa fuente de información para la prevención y denuncia de robos o vandalismos.

Las empresas y autoridades podrían plantear algún tipo de apoyo social o incentivo económico que promueva la denuncia del robo de cables y otros componentes por parte de las comunidades. No existe un solo camino para ello. Una vía puede ser, a través de la responsabilidad social empresarial en los focos de mayor robo. Otra vía puede ser un reconocimiento a las comunidades que hayan denunciado robos o afectaciones antes de cometerse o aquellas que acompañen efectivamente la investigación de incidentes.

Adicionalmente debería existir también un trabajo concientización y educación por parte de las operadoras hacia sus clientes y la ciudadanía en general sobre el valor de la infraestructura para las comunidades y los riesgos en materia de servicio si se presenta un incidente.

### Canales de denuncia ciudadana ofrecidas por las operadoras y gobiernos locales

Existen operadoras que como estrategia de mitigación han facilitado canales la denuncia del robo de cable que puedan utilizar cualquier ciudadano. Sin embargo, las estrategias no son uniformes y pueden variar en cada país. Por ejemplo, en el caso de Telefónica Argentina[72] ofrece como canal de denuncia la App Mi Movistar. Mientras tanto, en el caso de Telefónica Chile[73] se ofrece un formulario en su sitio web.

Si bien los canales de denuncia se tratan de una buena práctica ampliamente implementada, resulta necesario brindar canales de acceso rápido. Por ejemplo, aquellos canales que requieran descargar una aplicación o llenar un formulario largo, no facilitan que la ciudadana o los clientes de esas mismas operadoras puedan denunciar de manera clara. También, resulta importante considerar la diversidad de las comunidades, ofrecer la denuncia a través de la omnicanalidad y en lenguas originarias puede resultar clave. Eso quiere decir, que se ofrezca recibir la denuncia por redes sociales, mensajes de texto, llamada, correo electrónico o inclusive a una sucursal física.

**71.** Montenegro Retamozo, A. J. (2021). Análisis de los factores del hurto de cobre en la infraestructura de telecomunicaciones [Ensayo académico, Universidad Militar Nueva Granada]. Repositorio UMNG.
**72.** Movistar Argentina. (s. f.). ¿Cómo denuncio el robo de cables en mi zona desde la app?
**73.** Movistar Chile. (s. f.). ¿Cómo denunciar el robo de cables del servicio de Movistar?

### Campañas de denuncia liderada por las operadoras y entes reguladores

Las campañas de denuncia promovidas de manera coordinada por operadores de telecomunicaciones, reguladores y hasta gobiernos locales, se trata de una buena práctica que se debe mantener o amplificar.

Existen antecedentes sobre colaboración entre operadores e instituciones públicas para mitigar otro tipo de robos, que podrían replicarse para abordar el problema del robo de cable y vandalismo en las telecomunicaciones. Por ejemplo, en 2016 en Honduras, Claro, Hondutel y Tigo suscribieron un acuerdo con la GSMA y la Comisión Nacional de Telecomunicaciones (Conatel)[74] como testigos para implementar la iniciativa "Nos Importa", enfocada en combatir el robo de dispositivos móviles e impulsar la inclusión digital en los centros educativos públicos.

Sin embargo, resulta importante mencionar que la transparencia de información sobre el impacto de estas campañas es clave para que sean sostenibles. Si quienes lideran las campañas comparten que gracias a las denuncias se ha recuperado material robado, se ha evitado algún tipo de crimen o se ha mantenido la continuidad y calidad en el servicio para las comunidades, se fomenta e incentiva la denuncia. Pero, si no se comunica el estatus de esas campañas de denuncia, podría no haber información que permita mantener la motivación a participar.

### Colaboración por parte de los operadores y organismos de seguridad para combatir el robo y vandalismo

De igual manera, la colaboración activa con instituciones de seguridad y defensa por parte de las operadoras, también se trata de una buena práctica implementada en la región, que se debe amplificar. Existe el caso de Colombia en 2024, donde la Gerencia de seguridad y riesgo de Claro[75] participó en un operativo en conjunto con la Policía de Santander, la Fiscalía 2 Seccional EDA y el Batallón Caldas de Bucaramanga para desmantelar la organización delincuencial "Los Satélite" dedicada al robo de infraestructura de telecomunicaciones en Santander.

También, en Colombia se puede mencionar la colaboración entre la Secretaría Distrital de Integración Social de Bogotá y la Empresa de Telecomunicaciones de Bogotá (ETB) para promover la denuncia de vandalismo contra redes de Internet. Durante 2023, se lograron 2.400 denuncias y la desarticulación de 17 bandas gracias a esta alianza.

Una buena práctica, donde existe oportunidad de innovación, se trata de la participación de las operadoras de telecomunicaciones en aquellas acciones por parte de los cuerpos de seguridad para evitar el robo de cables y baterías, así como también en acciones para su posible recuperación de materiales y equipos. Esto requiere de unas normas y delimitaciones claras, pero sería la oportunidad de sumar conocimientos técnicos que pueden presentar resultados más eficaces.

**74.** Krom, A. (2016, 1 de febrero). Honduras: Claro, Hondutel y Tigo acuerdan acciones contra el robo.
**75.** Beltrán, D. (2024, 23 de octubre). Claro se unió con las autoridades para desmantelar banda que había robado equipos de telecomunicaciones e infraestructura por $2 mil millones. Infobae.

# 6. Políticas de mitigación

Las políticas de mitigación resultan importantes de considerar como propuestas orientadas a reducir los impactos negativos del robo de cables y el vandalismo en las telecomunicaciones. Las líneas de acción más relevantes en este sentido son acceso y uso de seguros y garantías que protejan a las instalaciones y sus componentes ante robos y daños.

También es necesario diseñar esquemas de apoyos fiscales para la reparación de instalaciones y la atención inmediata de comunidades afectadas por interrupción de servicio. En este sentido, el plantear al robo y daño de infraestructura como una causa externa las empresas podría reducir el riesgo de multas por incumplimiento regulatorio en materia de calidad en el servicio.

## Políticas de combate a mercados ilegales adyacentes

### Seguimiento a las cadenas delincuenciales y la ruta del cobre y equipos robados

Si bien las propuestas mencionadas para mitigar el robo de cables resultantes pertinentes, como se mencionó anteriormente, existe una cadena de valor[76] que promueve el robo y la venta de cable de cobre[77] y otros componentes de las redes de telecomunicaciones que van más allá del alcance de la seguridad comunitaria, vigilancia de instalaciones y sistemas de denuncia.

**76.** Gutiérrez, A. L. (2023, 8 de febrero). México: El negocio del cobre robado que termina en el mercado negro. DPL News.
**77.** Lizana, P. (2025, 28 de junio). La ruta del cobre y de la droga. El Líbero.

> **Las políticas de mitigación resultan importantes de considerar como propuestas orientadas a reducir los impactos negativos del robo de cables y el vandalismo en las telecomunicaciones.**

Estas cadenas y redes delictivas están compuesta por las recicladoras de chatarra, fundidoras de metales e inclusive empresas de exportación de metales[78]. En ese sentido, existe una serie de propuestas dirigidas a estos sectores con la finalidad de disminuir el robo de cables de cobre y baterías, ya que estos actores son fundamentales para aquellos delincuentes dedicados a este negocio ilícito.

### Marcado de cobre

El marcado, registro y monitoreo del cobre es una de las propuestas más relevantes para el seguimiento de cadenas delictivas en mercados negros, considerando que el cobre se trata del material más demandado en los incidentes de robo y vandalismo de infraestructura.

Existen diferentes métodos de marcado como el marcado químico que utiliza sustancias invisibles que se pueden detectar con luz ultravioleta para marcar el cobre. También, existe el etiquetado RFID que permite rastrear en tiempo real el cobre. Finalmente, se encuentra el marcado físico, que consiste en el grabado de números de serie o códigos en el cobre para identificarlo.

> **Marcado de cobre.** Una de las propuestas que se identifican con mayor frecuencia, se trata del marcado de los cables de cobre[79]. Anteriormente los cables se enumeraban antes de su instalación en una zona visible. Sin embargo, en tiempos recientes, existen marcados basados en pinturas indelebles o con químicos sintéticos que permiten una identificación específica del cableado. Sin embargo, la implementación de estas tecnologías dependerá en gran medida de la capacidad económica y técnica de las operadoras y autoridades.

### Fiscalización de chatarrerías, centros de reciclaje y fundidoras

De igual manera, la Asociación Chilena de Telecomunicaciones (Chile Telcos)[80] señala que es clave abordar la cadena de reducción y transformación del cobre, a través de fiscalización por parte de las autoridades públicas hacia chatarrerías y centros de reciclaje, donde se exija la documentación de procedencia del material. Desde 2009, en Chile es obligación legal llevar un registro de los metales que compran los recicladores. También, resulta importante recordar que existe el acuerdo global (no vinculante) de *The Copper Mark*[81], que busca verificar de forma independiente las prácticas de producción responsables en la industria de metales y esto incluye las empresas recicladoras[82].

En la misma línea, el operador Tigo en Costa Rica menciona la importancia de regular la exportación del cobre, a través de procesos más complejos que permitan la validación de que dicho material no proviene del robo o el vandalismo. Para ello, también serían necesarias revisiones en compañías de chatarras y recicladoras.

> **Fiscalización de la cadena de valor del cobre.** Resulta necesario implementar una serie de fiscalizaciones frecuentes a chatarrerías, centros de reciclaje y fundidoras que podrían estar recibiendo materiales robados. Además, la información hallada en estas fiscalizaciones se debería compartir en formato de datos abiertos para ser reutilizada para políticas de mitigación.

**78.** Basso, C. (2023, 10 de enero). Far West en el Norte (N° 2): Perú y países asiáticos son el destino del cobre robado por mafias similares a los narcos. Ex-Ante.
**79.** O'Halloran, J. (2024, 29 de abril). Openreach reaps benefit of invisible DNA marking with cable thefts down 30%. Computer Weekly.
**80.** Chile Telcos. (2025, 3 de abril). Impacto del robo de cables en Chile.
**81.** The Copper Mark. (s.f.). Governance.
**82.** The Copper Mark y Responsible Minerals Initiative. (2023). Guía de criterios de la Evaluación de la preparación para el riesgo (RRA).

### Registro y trazabilidad de la comercialización del cobre

A nivel internacional se ha prestado también atención a la industria de la chatarra como parte de la cadena que hace posible el robo de cables de cobre. Por ejemplo, en el estado de Idaho en Estados Unidos, las autoridades han exigido a los vendedores que pueda presentar identificadores a los recicladores para mitigar el lavado de cobre robado.

En este aspecto surgen líneas de acción como las de Servicios de Impuestos Internos de Chile (SII)[83], en las cuales se identifica una serie de delitos tributarios que podrían vincularse con la sustracción de cables como declaraciones falsas, comercio irregular y clandestino. En esa línea, se proponen modificaciones en el Código Tributario para aquellas personas o empresas que busquen insertar material robado al mercado formal a través de declaraciones fiscales. De igual manera, se menciona la necesidad de profundizar en sistemas obligatorios de trazabilidad de la información en sectores de difícil fiscalización vinculados al crimen organizado, donde se menciona con especial atención el cobre.

> **Registro público de comercio de cobre.** Ante estos antecedentes, una propuesta pertinente para las instituciones de seguridad, operadores y sociedad en general sería la creación un registro público de vendedores de cobre con carácter de obligatoriedad para el comercio de este material. Este registro debe ser accesible a la ciudadanía y en formato de datos abiertos para permitir un cruce de datos y la identificación de correlaciones en caso de detectar irregularidades.

> **Incentivos tributarios a la denuncia de cobre robado.** Las chatarrerías, centro de reciclaje y fundidoras se deben plantear un espacio que puedan servir como aliados en el combate contra el vandalismo de las telecomunicaciones. Para ello, una alternativa puede ser ofrecer incentivos de rebajas tributarias para aquellos negocios que colaboren denunciando la recepción de cobre robado en sus instalaciones.

### Fiscalización en los puertos y aduanas

Los puertos marítimos son otra área que merece atención. En 2023, el Sindicato de Telefonistas de México afirmó que la mayoría del cobre robado termina en la red de mercado de negro de las fundidoras para luego ser transportado al puerto de Lázaro Cárdenas, en Michoacán, para luego ser exportado a países como China. De igual manera, en Uruguay durante el 2020, se notificó la exportación de 2.860 toneladas, una cifra llamativa considerando que en ese país no se explota dicho mineral.

> **Control de aduanas.** Bajo esta línea, se puede proponer un control aleatorio de los principales puertos marítimos de América Latina con foco en embarcaciones de exportación hacia países procesadores de cobre. Esto se podría complementar con un análisis predictivo, a través de los datos proporcionados por las instituciones públicas sobre el tráfico de este material.

**83.** Cámara de Diputados de Chile. (2024, 15 de septiembre). Informe de la Comisión de Transporte y Telecomunicaciones.

### Coordinación internacional con países receptores de cobre robado e intersectorial de industrias de telecomunicaciones, minería, aduanas y exportación

Resulta importante generar un marco de gobernanza y colaboración a nivel multiactor con aquellas autoridades y empresas de diversos sectores y países que juegan un rol dentro de las redes de tráfico legal e ilegal de cobre. Para materializar una propuesta de esta naturaleza es necesario actualizar mecanismos multilaterales de coordinación que pueden incluir el tráfico de cobre robado y otros componentes. Por ejemplo, a través de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional se podría proponer la creación de un protocolo para prevenir y combatir el robo y tráfico ilícito de metales e infraestructura de telecomunicaciones.

Bajo un esquema como este, se puede comprometer países, autoridades y empresas de los ecosistemas de telecomunicaciones, minería, aduanas y exportación para que exista una mayor colaboración en el combate a este fenómeno. En forma concreta, esto permitiría elementos clave como la asistencia judicial mutua (cooperación legal entre países), extradición de delincuentes identificados, así como monitoreo y decomiso de materiales. Finalmente, se sugiere que en vista de poder generar incentivo por parte de los países involucrados, estas colaboraciones puedan formar parte de las conversaciones y acuerdos comerciales entre los países interesados.

> **Coordinación internacional en el comercio del cobre.** A nivel de las relaciones internacionales entre los países, se debería promover coordinaciones basadas en cláusulas comerciales para castigar el tráfico y compra de cobre robado. Esto sería especialmente útil entre los países de América Latina y países con amplias relaciones comerciales en cobre y otros metales.

# 7. Conclusiones

**La infraestructura de las telecomunicaciones es víctima de redes del crimen organizado con implicaciones puede ir desde la reventa localizada hasta el tráfico transcontinental**

En este estudio se puede observar cómo el fenómeno del robo de cables y el vandalismo de las telecomunicaciones, no se trata de un hecho aislado sino de un fenómeno regional con múltiples elementos. Pero, sin lugar a duda, se puede notar que se trata de una situación que requiere de la coordinación de todo el ecosistema de las telecomunicaciones, pero especialmente de las instituciones de seguridad pública de los Estados.

Si se recapitula en los hallazgos de esta investigación, se puede afirmar que la infraestructura de las telecomunicaciones es víctima de redes del crimen organizado con implicaciones puede ir desde la reventa localizada hasta el tráfico transcontinental con un especial foco en Asia.

Sin embargo, dimensionar el impacto no es una tarea sencilla. En primer lugar, existe una carencia de datos agregados sobre el robo de cables y el vandalismo de las telecomunicaciones. Este análisis es un primer esfuerzo regional registrado por consolidar la información desagregada por países sobre este fenómeno. A través de las notas de prensa y las denuncias puntuales de ciertas operadoras, se ha podido construir este primer panorama general. Pero, sin duda, existe una oportunidad de mejora para registrar mejor los casos de robos de cables, baterías y otras afectaciones. Esta tarea es un trabajo colectivo, donde operadores, reguladores, agencias de seguridad y organismos internacionales pueden sumar esfuerzos para construir una base de datos que permita hacerle un seguimiento más cercano a este fenómeno.

Otro punto para dimensionar mejor el impacto del vandalismo de las telecomunicaciones se trata de los efectos directos e indirectos que esto implica. Por esa razón, se abordó como el robo de cables puede tener efectos en la calidad de servicio, el cierre de brechas y la inversión en conectividad de la región.

Finalmente, este análisis lejos de quedarse en un diagnóstico pasivo también contiene un llamado a la acción claro, a través de propuestas legales y políticas públicas para combatir el robo de cables y el vandalismo de las telecomunicaciones. De igual manera, se proponen una serie políticas de prevención y mitigación que puedan tomar las instituciones de los Estados de América Latina; así como los reguladores, los operadores e inclusive la ciudadanía, todos juntos y bajo una colaboración que permita enfrentar este problema del robo de cables y el vandalismo de las telecomunicaciones.

# Referencias

**Estas URL hacen referencias a las notas al pie de todo el documento.**

**2.** https://www.fiscalia.gob.ec/formulario-en-linea-para-el-registro-de-presuntos-delitos-de-robo-y-hurto/

**3.** https://insightcrime.org/wp-content/uploads/2024/12/Informe-Fiscalia-de-Chile-Crimen-Organizado-En-Chile-Noviembre-2024.pdf

**4.** https://www.eaco.int/admin/docs/publications/CURBING%20THE%20COMMUNICATION%20INFRASTRUCTURE%20VANDALISM%20VICE%20IN%20EAST%20AFRICA.pdf

**5.** https://www12.senado.leg.br/radio/1/noticia/2025/04/09/plenario-aprova-aumento-de-penas-para-furto-de-fios-de-energia-e-telecomunicacoes

**6.** https://openknowledge.worldbank.org/server/api/core/bitstreams/875eff6e-5a5d-48e9-8af8-9546917647ca/content

**8.** https://tucumandespierta.com/roban-baterias-de-las-antenas-de-personal-y-claro/

**9.** https://eju.tv/2021/08/capturan-a-cinco-persona-vinculadas-al-robo-de-baterias-de-una-antena-de-entel/

**10.** https://bogota.gov.co/mi-ciudad/seguridad/por-hurto-de-baterias-de-antenas-telefonicas-cayeron-los-bodegueros

**11.** https://www.policia.gov.co/noticia/en-una-rapida-accion-policial-se-logro-frustrar-hurto-29-baterias-para-antenas

**12.** https://www.montevideo.com.uy/Noticias/Los-cables-de-cobre-en-Uruguay-un-robo-que-deja-vidas-en-el-camino-y-ataca-a-la-sociedad-uc814650

**13.** https://www.ecuavisa.com/noticias/quito/habitantes-de-calle-robado-cables-telefonia-fija-primer-mes-2025-EA8763420

**14.** https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

**15.** https://www.bandab.com.br/seguranca/trio-preso-furtar-triturar-cabos-telefonicos-campina-grande-sul/

**16.** https://teletime.com.br/12/01/2024/roubo-de-equipamentos-de-telecom-se-multiplica-para-alem-dos-cabos/

**17.** https://www.infobae.com/sociedad/policiales/2025/05/05/simulaban-ser-tecnicos-de-una-empresa-para-robar-cables-en-la-plata-hay-9-detenidos/

**18.** https://elmuro.pe/policial/los-telematicos-caen-robando-cables-de-telefonia-en-el-cerro-san-cristobal/

**19.** https://www.ultimahora.com/detienen-a-miembro-de-una-banda-dedicada-al-robo-de-baterias-de-alto-valor-para-empresas-telefonicas

**20.** https://www.lanacion.com.py/pais/2024/11/15/copaco-investiga-a-tecnicos-por-robo-de-1800-metros-de-cables-en-san-vicente/

**21.** https://columbia.co.cr/cifras-de-robo-de-cable-bajan-pero-perjuicio-economico-sigue-siendo-alto/

**22.** https://unitel.bo/noticias/seguridad/la-venta-de-cobre-en-el-mercado-negro-una-de-las-razones-que-vecinos-apuntan-como-causa-para-el-robo-de-cables-GB13746101

**23.** https://teletime.com.br/12/01/2024/roubo-de-equipamentos-de-telecom-se-multiplica-para-alem-dos-cabos/

**24.** https://interlira-reports.com/es/news/copper-cable-theft-gangs-connected-to-organized-crime/29/04/2025/

**25.** https://www.sinembargo.mx/4321884/el-robo-de-cables-del-metro-cfe-telmex-y-mas-servicios-se-dispara-306-en-5-anos/

**26.** https://doi.org/10.1080/0376835X.2024.2352057

# Referencias

**Estas URL hacen referencias a las notas al pie de todo el documento.**

**27.** https://www.proceso.com.mx/opinion/2023/8/25/crimen-organizado-ataca-infraestructura-de-telecom-313508.html

**28.** https://diariolalibertad.com/sitio/2020/02/16/con-explosivos-guerrilla-intento-derribar-torre-de-antenas-en-rio-de-oro-ocana-norte-de-santander/

**30.** https://conexis.org.br/mais-de-54-milhoes-de-metros-de-cabos-de-telecom-foram-roubados-em-2023/

**31.** https://www.telefonica.co/movistar-presenta-campana-la-ruta-del-cable-perdido/

**32.** https://www.telefonica.co/270-mil-clientes-de-movistar-se-vieron-afectados-por-el-hurto-de-infraestructura-en-el-2023/

**33.** https://mioriente.com/mi-oriente/robo-cable-afecto-293000-hogares.html

**34.** https://concejodebogota.gov.co/en-el-2023-en-bogota-se-hurtaron-en-cobre-el-total-de-kilometros/cbogota/2024-09-16/154307.php

**35.** https://www.lanacion.com.ar/seguridad/robo-cables-un-delito-miles-damnificados-perjuicios-nid2442555/

**36.** https://peru21.pe/lima/callao-5-anos-de-prision-efectiva-a-delincuente-por-robo-de-cables-telecomunicaciones-movistar-cables-poblacion-telefonia-noticia/

**37.** https://plataforma.ipnoticias.com/

**38.** https://chiletelcos.cl/noticia/comision-investigadora-de-la-camara-analiza-redes-delictuales-y-consecuencias-del-robo-de-cables/

**39.** https://www.telesemana.com/blog/2022/08/29/en-chile-se-robaron-mas-de-725-000-kilos-de-cables-de-telecomunicaciones-en-lo-que-va-del-ano/

**40.** https://www.ecuavisa.com/noticias/quito/habitantes-de-calle-robado-cables-telefonia-fija-primer-mes-2025-EA8763420

**41.** https://columbia.co.cr/cifras-de-robo-de-cable-bajan-pero-perjuicio-economico-sigue-siendo-alto/

**42.** https://elmorichal.com/la-policia-recupero-baterias-hurtadas-a-antenas-de-telefonia-celular-en-puerto-carreno/

**43.** https://dplnews.com/republica-dominicana-proteccion-cables-submarinos/

**44.** https://www.unidiversidad.com.ar/argentina-se-puso-a-prueba-ante-un-escenario-de-guerra-electronica

**45.** https://www.infobae.com/america/mundo/2025/07/20/cables-submarinos-la-infraestructura-critica-que-sostiene-al-mundo-en-medio-de-constantes-amenazas-de-sabotaje/

**46.** https://www.noroeste.com.mx/nacional/sera-delito-grave-robo-de-cable-de-cobre-LMNO859882

**47.** https://www.camara.cl/verDoc.aspx?prmID=310726&prmTipo=DOCUMENTO_COMISIÓN

**48.** https://www.diarioestrategia.cl/texto-diario/mostrar/5389539/idicam-valora-aprobacion-ley-endurece-sanciones-robo-cables-telecomunicaciones

**49.** https://www.in.gov.br/en/web/dou/-/lei-n-15.181-de-28-de-julho-de-2025-644943933

**50.** https://www.oas.org/dil/esp/codigo_penal_colombia.pdf

**51.** https://redfibra.mx/telecomunicaciones-en-ee-uu-asociaciones-exigen-medidas-federales-contra-ataques-a-la-infraestructura

**52.** https://www.researchgate.net/publication/377850159_Policy_Mechanism_for_Security_of_National_Vital_Objects_in_the_Telecommunications_Sector_in_Indonesia

**53.** https://doi.org/10.37811/cl_rcm.v7i1.5038

# Referencias

**Estas URL hacen referencias a las notas al pie de todo el documento.**

**54.** https://www.crhoy.com/ampliacion-de-red-de-fibra-optica-solucionaria-problema-del-robo-de-cable/

**56.** https://amarok.com/blog/9-security-threats-facing-power-plants/

**57.** https://www.integracionsocial.gov.co/index.php/noticias/116-otras-noticias/6377-quenorobentuconexion-etb-e-integracion-social-se-unen-para-promover-la-denuncia-de-vandalismo-contra-redes-de-internet

**58.** https://www.intelligencefusion.co.uk/insights/resources/article/top-physical-security-threats-to-the-telecom-industry/

**59.** https://doi.org/10.20533/JITST.2046.3723.2022.0093

**60.** https://doi.org/10.3390/safety10030080

**61.** https://doi.org/10.1063/1.5002481

**62.** http://repository.wyb.ac.lk/bitstream/handle/1/1562/ASRITE-2014-175.pdf?sequence=2

**63.** https://www.computerweekly.com/news/366582538/Openreach-reaps-benefit-of-invisible-DNA-marking-with-cable-thefts-down-30-per-cent

**64.** https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

**65.** https://primicia.com.ve/nacion/cicpc-y-cantv-definen-estrategias-para-evitar-robo-de-cables/

**66.** https://dplnews.com/panama-reforzaran-acciones-contra-vandalismo-de-cables/

**67.** https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector

**68.** https://www.ncta.com/news/protecting-networks-battling-the-rise-in-copper-theft-and-vandalism/

**69.** https://www.azevedosette.com.br/news/en/telecommunications-cybersecurity-recent-developments/6099

**70.** https://www.loc.gov/item/global-legal-monitor/2025-01-30/chile-framework-law-on-cybersecurity-comes-into-force/

**71.** https://repository.umng.edu.co/server/api/core/bitstreams/edfd39a5-cbb5-439a-9ac8-fe8ba2f172bf/content

**72.** https://ayuda.movistar.com.ar/pregunta/como-denuncio-el-robo-de-cables-en-mi-zona-desde-la-app.html

**73.** https://atencionalcliente.movistar.cl/internet-fijo/como-denunciar-el-robo-de-cables-del-servicio-de-movistar/

**74.** https://www.telesemana.com/blog/2016/02/01/honduras-claro-hondutel-y-tigo-acuerdan-acciones-contra-el-robo-de-celulares/

**75.** https://www.infobae.com/colombia/2024/10/23/desmantelada-banda-que-robaba-equipos-a-empresa-claro-colombia-en-santander/

**76.** https://dplnews.com/mexico-el-negocio-del-cobre-robado-que-termina-en-el-mercado-negro/

**77.** https://ellibero.cl/columnas-de-opinion/la-ruta-del-cobre-y-de-la-droga/

**78.** https://www.ex-ante.cl/far-west-en-el-norte-grande-2-peru-y-paises-asiaticos-son-el-destino-del-cobre-robado-por-mafias-similares-a-los-narcos/

**79.** https://www.computerweekly.com/news/366582538/Openreach-reaps-benefit-of-invisible-DNA-marking-with-cable-thefts-down-30-per-cent

**80**. https://chiletelcos.cl/noticia/impacto-del-robo-de-cables-en-chile/

**81.** https://coppermark.org/about/governance/

**82.** https://coppermark.org/wp-content/uploads/2023/10/RRA-Criteria-Guide_2023_

**83.** https://www.camara.cl/verDoc.aspx?prmID=313489&prmTipo=DOCUMENTO_COMISION

www.cet.la

cet.la
Centro de Estudios de Telecomunicaciones de América Latina