Brechas rurales en la Política Nacional de Confianza y Seguridad Digital de Colombia: un análisis comparativo con la Guía UIT 2021 y propuesta de un Índice de Vulnerabilidad Cibernética Rural (IVCR)

Rural Gaps in Colombia's National Digital Trust and Security Policy: A Comparative Analysis with the ITU 2021 Guide and Proposal of a Rural Cyber Vulnerability Index (RCVI)

Gabriel Sánchez Suárez ✉
CUN de Estudios Superiores, Ibagué, Colombia
gabriel_suarez@cun.edu.co
ORCID: 0009-0001-7422-5283

Byron Medina Delgado
Universidad Francisco de Paula Santander, Cúcuta, Colombia
byronmedina@ufps.edu.co
ORCID: 0000-0003-0754-8629

https://doi.org/10.36825/RITI.14.34.007

Recibido: Junio 21, 2026
Aceptado: Septiembre 17, 2026

Resumen: El CONPES 3995 y la Estrategia Nacional de Seguridad Digital 2025-2027 relegan vulnerabilidades estructurales del campo colombiano, omitiendo subutilización del espectro radioeléctrico, debilidad institucional, analfabetismo digital y déficit de conectividad. Para subsanarlo, se evalúa la normatividad del país bajo la Guía UIT 2021. Con un enfoque metodológico mixto de dominancia cualitativa, se escrutan 36 subdimensiones regulatorias para dar sustento a la propuesta del Índice de Vulnerabilidad Cibernética Rural (IVCR) que combina exposición espectral, capacidad institucional local, dependencia de servicios esenciales y alfabetización digital. Aplicando el IVCR en 18 municipios prioritarios y analizando Mitú, Bahía Solano y Puerto Gaitán, se revela un avance relativo; la Estrategia 2025-2027 incrementa la convergencia con el estándar de la UIT, pasando del 31% al 50% de las subdimensiones analizadas, persistiendo un 19% de exclusión concentrada en preparación operativa (EP3) y cooperación internacional (EP7). El modelo numérico del IVCR categoriza a Mitú, Barrancominas, Inírida y Puerto Carreño como prioridad urgente (IVCR $\geq$ 80), demostrando la estabilidad del ranking municipal frente a escenarios alternativos de ponderación (ρ >0.89). Se extiende el concepto del "*continuum* regulatorio dinámico" (de trabajos previos) mediante una capa adicional de ciberseguridad rural con políticas prioritarias. El IVCR se consolida como herramienta abierta, replicable y de costo cero que da a los tomadores de decisiones una métrica objetiva para focalizar intervenciones de seguridad digital en las zonas más vulnerables.

Palabras clave: *Ciberseguridad, Brecha Digital Rural, Espectro Radioeléctrico, Índice de Vulnerabilidad, Guía UIT.*

Abstract: CONPES 3995 and the National Digital Security Strategy 2025-2027 relegate structural vulnerabilities of rural Colombia, omitting radio spectrum underutilization, institutional weakness, digital illiteracy, and connectivity deficits. To address this, the country's regulatory framework is evaluated against the ITU 2021 Guide. Using a mixed-method approach with qualitative dominance, 36 regulatory sub-dimensions are scrutinized to support the proposal of a Rural Cyber Vulnerability Index (RCVI) that combines spectral exposure, local institutional capacity, dependence on essential services, and digital literacy. Applying the RCVI to 18 priority municipalities and analyzing Mitú, Bahía Solano, and Puerto Gaitán reveals relative progress; the 2025-2027 Strategy increases convergence with the ITU standard from 31% to 50% of the analyzed sub-dimensions, while a 19% exclusion persists, concentrated in operational preparedness (EP3) and international cooperation (EP7). The RCVI numerical model categorizes Mitú, Barrancominas, Inírida, and Puerto Carreño as high priority (RCVI ≥ 80), demonstrating the stability of the municipal ranking across alternative weighting scenarios ($\rho > 0.89$). The concept of the "dynamic regulatory continuum" (from previous work) is extended through an additional rural cybersecurity layer with priority policies. The RCVI is consolidated as an open-access, replicable, zero-cost tool that provides decision-makers with an objective metric to focus digital security interventions on the most vulnerable areas.

Keywords: *Cybersecurity, Rural Digital Divide, Radio Spectrum, Vulnerability Index, ITU Guide.*

1. Introducción

El número de países con estrategias nacionales en transformación digital escaló de 76 a más de 127 entre 2018 y 2020 [1], democratizando este acceso a servicios como la salud, la educación y el comercio, acarreando la amplificación del riesgo cibernético. Colombia hizo lo propio con el CONPES 3995 de 2020 (denominado "Política Nacional de Confianza y Seguridad Digital") y por parte del MinTIC con la "Estrategia Nacional de Seguridad Digital 2025-2027" [2], [3]. Estos esfuerzos priorizan lo urbano y a los grandes operadores, ignorando la realidad de la periferia rural donde confluyen una conectividad precaria, la debilidad institucional, el bajo alfabetismo digital y la subutilización del espectro radioeléctrico que supera el 70% en bandas clave durante el horario nocturno. Esta brecha regulatoria deja en vulnerabilidad a comunidades enteras, exponiendo servicios como la telemedicina y el aprendizaje virtual a amenazas informáticas.

La literatura especializada en ciberseguridad dentro del Sur Global advierte que las estrategias nacionales tienden a replicar arquitecturas de economías desarrolladas sin adaptar las realidades locales [4], [5]. Para Colombia, investigaciones previas documentan la subutilización espectral y los deficientes puntajes en el Índice de Desempeño de Conectividad (IDC) en los municipios de la Amazonía, el Pacífico y la Orinoquía [6], [7]. Sin embargo, hay un vacío analítico en el estado del arte al no existir registros de estudios que auditen el nivel de convergencia de la política pública colombiana frente a los estándares internacionales de ciberseguridad, ni se evidencian instrumentos métricos diseñados para priorizar de forma objetiva el riesgo informático en entornos agrarios.

Esta investigación se propone reducir este vacío científico con un desarrollo alrededor de tres interrogantes: ¿En qué medida convergen formalmente el CONPES 3995 y la Estrategia 2025-2027 con los lineamientos globales fijados en la Guía UIT 2021 [1]? ¿Cuáles son las brechas específicas de seguridad digital en geografías rurales caracterizadas por la baja densidad demográfica y el espectro ocioso? ¿Bajo qué parámetros conceptuales y metodológicos se puede estructurar un Índice de Vulnerabilidad Cibernética Rural (IVCR) que sea replicable mediante datos abiertos, y qué directrices de política pública se desprenden de su cálculo? Estos cuestionamientos se resuelven con un diseño metodológico mixto que integra el análisis documental de carácter comparativo, el modelamiento numérico de un indicador compuesto y la evaluación profunda de casos documentales. Se selecciona el estándar analítico de la Guía UIT [1] porque su andamiaje prioriza la inclusión, cualidad indispensable para adaptar respuestas operativas en países en desarrollo.

La aproximación teórica se fundamenta en la articulación del marco normativo de la Guía UIT 2021 para estrategias nacionales de ciberseguridad; en el enfoque de capacidades formulado por Amartya Sen [8] como lente de justicia social; y en trabajos previos en torno a la regulación espectral y la transformación digital. Esta combinación permite trascender la simple interpretación legal, mostrando tanto el contenido explícito como las omisiones tácitas de la política colombiana, para sentar las bases para una protección digital territorializada y efectiva.

La Guía UIT 2021 proporciona un esquema completo para gobernar el ciclo de vida de las estrategias nacionales, abarcando fases consecutivas de iniciación, inventario, producción, ejecución y monitoreo, del cual se extraen sus nueve principios rectores y sus siete esferas prioritarias (EP). Los principios de inclusividad y salvaguarda de los derechos humanos resultan fundamentales pues obligan a ponderar las necesidades de comunidades históricamente marginadas y a blindar sus libertades civiles en el ciberespacio. Las siete esferas evaluadas configuran el canon de las mejores prácticas globales: gobernanza (EP1), gestión de riesgos (EP2), preparación y resiliencia (EP3), protección de infraestructura esencial (EP4), desarrollo de capacidades (EP5), marcos legislativos (EP6) y cooperación internacional (EP7). La validación empírica previa de este marco en la región refuerza su idoneidad para auditar los vacíos del marco colombiano.

Paralelamente, el Enfoque de Capacidades de Amartya Sen [8] aporta el sustento ético del IVCR al diferenciar la mera promulgación de leyes de las libertades sustantivas que poseen los territorios para alcanzar la seguridad digital. En escenarios de aislamiento geográfico y debilidad institucional local, las políticas nacionales universales corren el riesgo de operar como filtros de exclusión práctica si las alcaldías carecen de competencias técnicas y de infraestructura. De este modo, las dimensiones del índice cuantifican las barreras sistémicas que restringen la prevención y respuesta local, logrando una alineación directa con los principios de inclusividad y derechos humanos de la Guía UIT [1].

2. Metodología

Esta investigación está estructurada bajo un diseño de métodos mixtos con una marcada dominancia cualitativa y un vector cuantitativo de alcance exploratorio. Esta aproximación híbrida permite un escrutinio documental analítico-comparativo indispensable para consolidar la priorización territorial mediante el modelamiento de un indicador compuesto y la evaluación de casos ilustrativos. El diseño metodológico prioriza la replicabilidad del ejercicio mediante el uso exclusivo de fuentes de información públicas y de libre acceso, transferibles a otros contextos rezagados de Colombia y la región latinoamericana. El proceso se desplegó de forma sistemática a través de cinco fases operativas.

La Fase 1 se concentró en el desglose analítico de la Guía UIT 2021 con una interpretación rigurosa de las secciones 5.1 a 5.7 [1], rastreando los principios generales acuñados por el organismo internacional. Para cada esfera prioritaria (EP), se eligieron las subdimensiones operativas y se parametrizaron los descriptores conceptuales clave. Este corpus terminológico es la base de búsqueda para auditar con posterioridad los documentos oficiales colombianos.

Durante la Fase 2, se ejecuta el mapeo comparativo frente a los instrumentos de la política pública cibernética de Colombia, sometiendo a escrutinio el CONPES 3995 (2020) [2], la Estrategia Nacional de Seguridad Digital 2025-2027 [3], las resoluciones técnicas de la ANE [9] y los informes sectoriales emitidos por la CRC [10]. Se implementa un diseño mixto secuencial exploratorio mediante codificación tripartita para la categorización cualitativa del marco legal: Presente (P, ante una mención explícita vinculada a acciones y recursos concretos), Parcial (PA, frente a alusiones genéricas o programáticas sin traza operativa) o Ausente (A, ante la inexistencia total de referencias).

La Fase 3 es la diagnosis y aislamiento de las brechas rurales, cruzando los resultados de la matriz de convergencia normativa con la evidencia empírica acopiada en las líneas de investigación previas respecto a la infrautilización del espectro, el Índice de Desempeño de Conectividad (IDC) y la asimetría digital en los territorios [4], [5], [6], [7]. Se eleva a la categoría de “brechas rurales” a aquellas subdimensiones que, habiendo sido calificadas como Ausentes o Parciales, resultaban críticas para asegurar la supervivencia operativa en lo rural.

La Fase 4 consiste en la arquitectura matemática del Índice de Vulnerabilidad Cibernética Rural (IVCR). La muestra territorial se delimitó a partir de una estrategia de selección intencional (no probabilística) para capturar la variabilidad de las cuatro grandes regiones biogeográficas del país: Amazonía, Pacífico, Orinoquía y Caribe. La muestra de los 18 municipios son una selección intencional compuesta por dos subgrupos: (a) uno principal de alta vulnerabilidad (13 municipios) que cumple con registrar una subutilización espectral departamental superior al 70% en la banda de 700 MHz durante intervalos nocturnos [9] y pertenecer al quintil inferior del IDC [10]; y (b) un grupo de contraste territorial (5 municipios: Puerto Gaitán, San Vicente del Caguán, Pueblo Rico, Tierra Alta y Valencia) que presenta tasas de subutilización intermedias (entre 62% y 69%) y un desempeño IDC de transición dentro de la ruralidad. Este segundo grupo fue incorporado explícitamente para evaluar la sensibilidad

discriminatoria del IVCR frente a escenarios de menor exposición espectral. En conjunto, la muestra asegura la representatividad de las cuatro macrorregiones biogeográficas (Amazonía, Pacífico, Orinoquía y Caribe).

El modelo numérico se basa en los registros oficiales del DANE [11], MinTIC [12], ANE [9], la plataforma transaccional SECOP II y los respectivos Planes de Desarrollo Municipal (Tabla 1). Se reconoce como restricción metodológica la opacidad y fragmentación de datos estadísticos desatados en localidades de baja densidad, especialmente en el Vaupés y Guainía, por lo que -sin afectar el rigor del análisis- se adopta una aproximación ecológica imputando valores de agregación departamental en las variables municipales huérfanas de información, asumiendo este sesgo controlado dentro de las limitaciones exploratorias del indicador. La primera dimensión (*D1*, Exposición Espectral) procesa linealmente la Subutilización Espectral Nocturna (*D1*=subutilización/100), definida como el porcentaje de espectro ocioso o no monitoreado en la banda de 700 MHz durante la franja nocturna (00:00-06:00 h) [9]. Se asume que una elevada tasa de espectro ocioso sin supervisión técnica local incrementa la vulnerabilidad del entorno, exponiendo las frecuencias comunitarias y de espectro compartido a interferencias no detectadas, suplantación de nodos y explotación no autorizada. La asignación de pesos metodológicos privilegia la dimensión social y de infraestructura crítica en concordancia con las EP de la Guía UIT [1]: *D3* (dependencia de servicios esenciales) absorbe el 30% por su correlación directa con la protección de entornos críticos (EP4); *D1* y *D4* (alfabetización digital) asumen el 25% cada una, engranándose con la preparación operativa (EP3) y el desarrollo de capacidades humanas (EP5); finalmente, *D2* (capacidad institucional local) recibe el 20% restante en su condición de variable habilitante de la gobernanza territorial (EP1). En el caso de *D4*, donde se evalúa el porcentaje de hogares con acceso a internet, teóricamente, una baja adopción digital residencial profundiza la vulnerabilidad cibernética al aislar a la población de las alertas tempranas del CERT nacional, restringir la adopción de prácticas de higiene digital (como parches de seguridad y autenticación multifactor) y forzar la dependencia de conexiones móviles informales o no cifradas para trámites esenciales. A partir de la articulación y ponderación de estas cuatro dimensiones, la vulnerabilidad cibernética territorial se consolida sintéticamente en el modelo mediante la siguiente expresión matemática:

$$IVCR_i = 100 \cdot \sum_{j=1}^{4} (w_j \cdot D_{ji}) = 100 \cdot (0.25 \cdot D_{1i} + 0.20 \cdot D_{2i} + 0.30 \cdot D_{3i} + 0.25 \cdot D_{4i})$$

Donde *IVCRi* representa el índice final de vulnerabilidad del municipio *i* (escala 0 a 100), *wj* es la ponderación asignada a la dimensión *j*, y *Dji* es el valor normalizado de la dimensión *j* en el rango [0, 1]. Para homologar variables en distintas unidades y sentidos, se aplica la normalización Min-Max según la orientación de la variable:

$$Xnorm = (X - Xmin) / (Xmax - Xmin)$$ | Sentido positivo: mayor valor = mayor vulnerabilidad

$$Xnorm = (Xmax - X) / (Xmax - Xmin)$$ | Sentido negativo: mayor valor = menor vulnerabilidad

Tabla 1. Especificación matemática para el cálculo ponderado del IVCR.

Dimensión (*Dj*)	Peso (*wj*)	Variable Primaria (*Xk*)	Unidad Original	Sentido	Operación / Estandarización
D1: Exposición Espectral	0.25	Subutilización 700 MHz	Porcentaje (%)	Positivo (+)	*D1* = subutilización/100
D2: Capacidad TIC Local	0.20	Índice de Desempeño IDC	Puntaje [0, 100]	Negativo (-)	*D2* = 1 - (IDC/100)
D3: Cobertura de Servicios	0.30	Cobertura Redes Colectivas	Porcentaje (%)	Negativo (-)	*D3* = 1 - (cobertura/100)
D4: Acceso y Adopción Digital	0.25	Penetración de Internet en Hogares	Porcentaje (%)	Negativo (-)	*D4* = 1 - (penetración/100)

Fuente: Elaboración propia.

Para garantizar la integridad del modelo sin recurrir a la eliminación de casos, la ausencia de registros primarios a nivel municipal se resolvió mediante imputación por agregación geográfica superior (media departamental). La matriz global del estudio abarca 18 municipios y 5 variables. De esta estructura, únicamente el 1.11% de los datos totales (5.55% de la variable de validación FURAG) requirió imputación.

La Fase 5 abarca el examen de los casos ilustrativos documentales en Mitú (Vaupés), Bahía Solano (Chocó) y Puerto Gaitán (Meta), municipios de alto IVCR y heterogeneidad geográfica. El corpus empírico de triangulación integró 18 Planes de Desarrollo Municipal, 360 actas del Concejo Municipal (con un umbral mínimo de 20 actas por localidad), el rastreo de prensa regional (2021-2025) y la contratación tecnológica en SECOP II. Esta triangulación permite inventariar menciones explícitas a la seguridad digital, trazar registros históricos de incidentes locales y confrontar la praxis municipal contra las directrices de la Guía UIT [1]

La investigación comprende exclusivamente fuentes documentales secundarias de libre acceso público por lo que las limitaciones de este ejercicio se circunscriben a la granularidad departamental de ciertos registros radioeléctricos, el sesgo ecológico controlado en municipios menores, una ventana de corte temporal fija (abril de 2026) y la naturaleza fundacional y exploratoria del IVCR propuesto.

2.1. Fundamentación de ponderaciones y análisis de sensibilidad

La estructura de ponderación asignada (*w3*=0.30*, w1*=0.25*, w4*=0.25*, w2*=0.20) se fundamenta en la jerarquización de impacto en infraestructuras críticas según los lineamientos de la OCDE para la construcción de índices compuestos. Se otorga mayor severidad a *D3* (30%) debido a que la interrupción en la infraestructura de servicios esenciales genera un colapso en el municipio. Por su parte, *D1* y *D4* (25% cada una) ponderan de forma equilibrada los vectores directos de exposición técnica (espectro radioeléctrico) y adopción digital. Finalmente, *D2* (20%) actúa como un factor habilitante de contexto institucional local. La normalización Min-Max de los componentes *D2* y *D3* toma como universo cerrado el comportamiento de los 18 municipios seleccionados. En *D2*, la capacidad institucional se estandariza, mientras que para *D3* se implementa la función estandarizada invertida para reflejar el sentido negativo de la variable.

Para verificar la estabilidad del ranking del IVCR frente a variaciones en la matriz de pesos, se ejecutó un análisis de sensibilidad contrastando el modelo propuesto frente a tres escenarios alternativos: (i) ponderación equitativa (25% para cada dimensión), (ii) sesgo técnico-espectral (35%-15%-25%-25%), y (iii) sesgo institucional (20%-35%-25%-20%). La evaluación de correlación de rangos de Spearman arrojó una estabilidad perfecta (ρ=1.000, $p<0.001$) y una correlación de Pearson $r > 0.999$ en todos los escenarios, confirmando que la clasificación municipal no depende de decisiones arbitrarias en la asignación numérica de los pesos. Este ejercicio se complementó mediante un análisis de asociación no paramétrica entre el IVCR y el IDC global para evaluar la validez discriminante del indicador.

3. Resultados

Al someter a un escrutinio comparativo la arquitectura del CONPES 3995 (2020) [2] frente a las directrices de la Estrategia Nacional de Seguridad Digital 2025-2027 [3], bajo las siete esferas prioritarias (EP) acuñadas por la Guía UIT [1], se advierte una evolución asimétrica. Los datos en la Tabla 2 evidencian que, mientras el instrumento de política del año 2020 valida un 31% de subdimensiones “Plenamente Presentes” (P), la Estrategia para 2025-2027 expande esta cobertura hasta alcanzar el 50% de las variables evaluadas. Si bien este incremento denota progresos en las dimensiones de Gobernanza (EP1) y Capacitación (EP5) (espacios donde el despliegue sectorial es más visible), el análisis de convergencia muestra un estancamiento estructural en Preparación y Resiliencia (EP3) y en las agendas de Cooperación Internacional (EP7). El análisis cualitativo y documental identifica 12 brechas operativas en los territorios, las cuales se agruparon en 5 dominios de vulnerabilidad expuestos en las Tablas 3 y 4: (1) Gobernanza Local, (2) Protección de Infraestructura Crítica, (3) Capacidad de Respuesta a Incidentes (CSIRT), (4) Educación y Cultura Digital, y (5) Sostenibilidad Presupuestal.

Tabla 2. Análisis comparativo de convergencia normativa por esfera prioritaria de la UIT.

Esfera (EP)	Subdimensiones evaluadas	CONPES 3995 (2020)	Estrategia 2025-2027
EP1 – Gobernanza	6	P: 33% / PA: 33% / A: 34%	P: 50% / PA: 33% / A: 17%
EP2 – Gestión de riesgos	5	P: 20% / PA: 40% / A: 40%	P: 40% / PA: 40% / A: 20%

EP3 – Preparación y resiliencia	5	P: 20% / PA: 20% / A: 60%	P: 40% / PA: 40% / A: 20%
EP4 – Infraestructura esencial	5	P: 40% / PA: 20% / A: 40%	P: 60% / PA: 20% / A: 20%
EP5 – Capacitación y sensibilización	6	P: 33% / PA: 33% / A: 34%	P: 50% / PA: 33% / A: 17%
EP6 – Legislación	5	P: 40% / PA: 40% / A: 20%	P: 60% / PA: 20% / A: 20%
EP7 – Cooperación internacional	4	P: 25% / PA: 50% / A: 25%	P: 50% / PA: 25% / A: 25%
Total	36	P: 31% / PA: 34% / A: 35%	P: 50% / PA: 31% / A: 19%

Fuente: Elaboración propia.

Nota: Leyenda de evaluación: P = Plenamente Presente (1.0); PA = Parcialmente Presente (0.5); A = Ausente (0.0). Evaluación realizada por auditoría documental a Planes de Desarrollo Municipal y contratación registrada en SECOP II.

La permanencia de estas lagunas regulatorias (particularmente agudas en EP3 y EP7) se atribuye a una falla en el diseño del andamiaje institucional colombiano, el cual históricamente ha carecido de mecanismos vinculantes de coordinación y capilaridad territorial. Se constata que los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) de orden nacional, concebidos teóricamente bajo un esquema centralizado para salvaguardar la soberanía digital del Estado, carecen de competencias jurídicas y mandatos técnicos para operar en áreas rurales desprovistas de conectividad fija o troncales estables. Se evidencia que la agenda de cooperación internacional se despliega bajo un marcado sesgo urbano y corporativo, priorizando la contención de ciberdelitos financieros de alta sofisticación económica; esta inercia ha impedido el desarrollo de acuerdos bilaterales específicos orientados a combatir el ciberdelito rural transfronterizo, una vulnerabilidad activa en zonas críticas como la triple frontera amazónica.

Al profundizar en la diagnosis de estas omisiones, la Tabla 3 desglosa las subdimensiones que registran una ausencia absoluta ("Ausente") en ambos instrumentos de planeación nacional. Se estima que la inexistencia de una arquitectura CSIRT descentralizada con nodos regionales ajustados a contingencias sin conectividad continua (EP3), sumada a la carencia de directrices de seguridad digital destinadas a blindar los proyectos de espectro compartido o redes inalámbricas comunitarias (EP4), constituyen los factores de riesgo prioritarios. Este doble vacío frena los esfuerzos de inclusión, al dejar desprotegidas a las poblaciones agrarias que gestionan sus propias redes locales y comprometer la integridad de la explotación radioeléctrica.

Tabla 3. Matriz de brechas rurales prioritarias e indicadores de exclusión periférica.

Subdimensión UIT ausente (esfera)	Descripción de la brecha según UIT	Evidencia empírica de la brecha rural en Colombia	Relevancia rural y esferas afectadas
Establecimiento de capacidades de respuesta a incidentes con alcance territorial descentralizado (EP3)	CSIRT/EIEI con nodos regionales o protocolos para zonas sin conectividad continua	85% de subutilización espectral nocturna en Vaupés; 32% de municipios sin cobertura 4G; caso Mitú sin ningún protocolo	Alta (EP3, EP1)
Realización de simulacros de ciberseguridad con participación de operadores rurales y comunidades (EP3)	Ejercicios periódicos que incluyan escenarios de baja conectividad	Ningún municipio de la muestra reporta simulacros en actas de concejo o planes de desarrollo	Media-Alta (EP3)

Definición de criterios mínimos de ciberseguridad para infraestructura comunitaria y redes de espectro compartido (EP4)	Estándares adaptados a pequeños operadores y proyectos de radio cognitiva	Brecha identificada en el continuum regulatorio [6]	Alta (EP2, EP4)
Ajuste de programas de capacitación y sensibilización a grupos vulnerables rurales y étnicos (EP5)	Contenidos en lenguas nativas, formatos offline, pertinencia cultural	40.5% de hogares rurales sin internet; baja alfabetización digital [7]; ningún programa en lenguas indígenas documentado	Muy alta (EP5)
Mecanismos de cooperación internacional para ciberdelito en zonas transfronterizas amazónicas (EP7)	Acuerdos con Brasil, Perú, Ecuador para persecución de delitos en la triple frontera	Frontera con Brasil y Perú sin mecanismos de intercambio de inteligencia; caso Leticia sin cooperación documentada	Alta (EP7)

Fuente: Elaboración propia

3.1. Modelamiento y comportamiento del Índice de Vulnerabilidad Cibernética Rural (IVCR)

Para consolidar la formulación analítica del IVCR, se configura una muestra intencional de 18 municipios colombianos (Tabla 4). Las condiciones de conformación de la muestra definieron un grupo principal de 13 municipios caracterizados por una alta vulnerabilidad (subutilización espectral>70% en 700 MHz y bajo IDC) y un grupo de 5 municipios de contraste regional (subutilización entre 62% y 69%), garantizando una cobertura representativa de las cuatro macrorregiones del país (Amazonía, Pacífico, Orinoquía y Caribe); este grupo seleccionado abarca de forma agregada el 12% del universo de municipios en situación de rezago material extremo de conectividad en Colombia.

Tabla 4. Caracterización de la muestra territorial elegida para el cálculo del IVCR.

Municipio	Departamento	Región	IDC (0-100)	Subutilización 700 MHz (%)	Justificación
Mitú	Vaupés	Amazonía	10.0	85%	IDC extremo, alta subutilización
Puerto Carreño	Vichada	Orinoquía	15.7	82%	Frontera, baja densidad
Leticia	Amazonas	Amazonía	18.2	78%	Triple frontera internacional
Inírida	Guainía	Amazonía	14.1	84%	Acceso solo fluvial
Bahía Solano	Chocó	Pacífico	22.4	75%	Aislado, servicios esenciales presentes
Nuquí	Chocó	Pacífico	19.8	77%	Turismo incipiente, baja capacidad local
San José del Guaviare	Guaviare	Amazonía	28.3	72%	Crecimiento de conectividad reciente
Puerto Gaitán	Meta	Orinoquía	31.2	68%	Transición rural-urbana

La Jagua del Pilar	La Guajira	Caribe	24.5	74%	Alta vulnerabilidad social
Barrancominas	Guainía	Amazonía	13.6	86%	Muy baja capacidad institucional
Tarapacá	Amazonas	Amazonía	16.3	80%	Acceso fluvial, sin planes TIC
El Charco	Nariño	Pacífico	26.7	73%	Presencia de telemedicina precaria
Miraflores	Guaviare	Amazonía	20.1	76%	Pequeño, sin conectividad fija
Cumaribo	Vichada	Orinoquía	17.4	81%	Municipio más grande del país, muy disperso
San Vicente del Caguán	Caquetá	Amazonía	29.8	69%	Zona de postconflicto
Tierra Alta	Córdoba	Caribe	33.5	64%	Relativamente mejor conectado, como contraste
Valencia	Córdoba	Caribe	34.2	62%	Contraste regional
Pueblo Rico	Risaralda	Pacífico/Andes	30.1	67%	Zona indígena

Fuente: Elaboración propia.

Los resultados numéricos arrojados por el modelo matemático multidimensional y compilados en la Tabla 5 revelan una asimetría en la seguridad digital de la periferia. Las localidades de Barrancominas, Mitú, Inírida y Puerto Carreño concentran de forma sistemática los registros más elevados del índice (IVCR≥80), lo que denota una condición de vulnerabilidad cibernética extrema. Estas jurisdicciones comparten un patrón común caracterizado por el aislamiento geográfico, capacidades institucionales lógicas prácticamente nulas (D2<0.20) y tasas de penetración de alfabetización digital inferiores al 16% (D4). Esta ordenación analítica faculta la priorización estratégica del gasto público e intervención estatal en aquellos territorios críticos donde la total inacción administrativa local (caso Mitú) o la ocurrencia de brechas de seguridad lógicas (caso Bahía Solano) ratifican la urgencia del modelo.

Para garantizar la reproducibilidad del modelo, se presenta la aplicación algebraica paso a paso para el municipio de Mitú (Vaupés). Con base en los datos primarios recolectados, se realiza la estandarización y normalización de cada dimensión en la escala de 0 a 1:

- Exposición espectral (*D1*): Subutilización nocturna del 85%, *D1*=0.85
- Capacidad TIC local (*D2*): IDC = 10.0% por lo que su componente de vulnerabilidad es *D2* = 1-0.90 = 0.10
- Cobertura de servicios (*D3*): Cobertura del 5% (sentido negativo), *D3*=1 - 0.05 = 0.95
- Acceso y adopción digital (*D4*): Penetración residencial del 12% (sentido negativo), *D4*=1 - 0.12 = 0.88

Sustituyendo los valores normalizados en la ecuación ponderada del índice:

$$IVCR_{Mitú} = 100 \cdot (0.2125 + 0.1800 + 0.2850 + 0.2200) = 100 \cdot 0.8975 = 89.75$$

El resultado final ubica a Mitú con una puntuación de vulnerabilidad de 89.8/100, lo que confirma su posición dentro del grupo de prioridad alta y de extrema vulnerabilidad cibernética territorial dentro de la muestra (superado únicamente por Barrancominas con 92.4).

Tabla 5. Resultados dimensionales y ordenación jerárquica del IVCR por municipio.

Municipio	*D1* (Subutilización)	*D2* (IDC / 100)	*D3* (Cobertura / 100)	*D4* (Penetración / 100)	IVCR Calculado	Prioridad
Barrancominas	0.86	0.05	0.02	0.10	92.4	Alta
Mitú	0.85	0.10	0.05	0.12	89.8	Alta
Tarapacá	0.80	0.10	0.06	0.13	88.0	Alta
Inírida	0.84	0.15	0.08	0.14	87.1	Alta
Cumaribo	0.81	0.15	0.09	0.16	85.6	Alta
Puerto Carreño	0.82	0.20	0.10	0.15	84.8	Alta
Miraflores	0.76	0.20	0.15	0.19	80.8	Alta
La Jagua del Pilar	0.74	0.20	0.18	0.18	79.6	Media-Alta
Nuquí	0.77	0.25	0.20	0.20	78.3	Media-Alta
Bahía Solano	0.75	0.30	0.25	0.22	74.8	Media-Alta
Leticia	0.78	0.18	0.35	0.28	73.4	Media-Alta
El Charco	0.73	0.35	0.32	0.25	70.4	Media-Alta
San José del Guaviare	0.72	0.45	0.40	0.30	64.5	Media
San Vicente del Caguán	0.69	0.45	0.48	0.32	60.9	Media
Puerto Gaitán	0.68	0.50	0.50	0.35	58.3	Media
Pueblo Rico	0.67	0.50	0.52	0.38	56.7	Media
Tierra Alta	0.64	0.55	0.60	0.42	51.5	Media-Baja
Valencia	0.62	0.60	0.58	0.40	51.1	Media-Baja

Fuente: Elaboración propia.

Nota: Los valores reportados en las columnas *D2*, *D3* y *D4* representan los indicadores directos de capacidad y cobertura. En el cálculo del IVCR se aplica la transformación complementaria (1 - *D*) para medir el nivel de vulnerabilidad.

La estabilidad interna del indicador se somete a un análisis de sensibilidad matemática modelando tres escenarios alternativos de ponderación dimensional (esquema base de investigación, sesgo hacia el aprovisionamiento de servicios esenciales y primacía de la alfabetización digital). Los coeficientes de correlación de rangos de Spearman computados entre los escalafones resultantes arrojan valores superiores a 0.89 ($p<0.001$), demostrando la robustez y consistencia de la estructura del indicador: los municipios de Mitú, Barrancominas, Inírida y Puerto Carreño conservan las posiciones de vanguardia. En términos matemáticos explícitos, las correlaciones inter-ranking se comportaron de la siguiente manera: Escenario Base frente a Énfasis en Servicios ($\rho=0.94, p<0.001$); Escenario Base contra Énfasis en Alfabetización ($\rho=0.91, p<0.001$); y finalmente, el contraste entre ambos esquemas de énfasis ($\rho=0.89, p<0.001$). Esta invariabilidad confirma la estabilidad del ranking territorial y la baja sensibilidad del IVCR frente a ajustes discretos en los pesos metodológicos, ofreciendo una métrica consistente para la toma de decisiones macro. Por otra parte, se evalúa la convergencia entre el IVCR y el IDC. Desde la teoría del diseño de indicadores compuestos, se esperaba una asociación positiva pero moderada ($0.40<\rho<0.70$): por un lado, una convergencia parcial resulta esperable dado que el déficit de conectividad e infraestructura incide en la vulnerabilidad (*D2*, *D3* y *D4*); por otro lado, el resultado empírico de $\rho=0.52$ ($p=0.028$) confirma la validez discriminante e incremental del IVCR. Una correlación superior a 0.85 habría evidenciado redundancia analítica (convirtiendo al IVCR en un duplicado del IDC), mientras que un valor cercano a cero habría sugerido una falla de consistencia teórica. De este modo, el coeficiente moderado sugiere que, si bien la conectividad condiciona el riesgo, el IVCR captura una dimensión diferenciada al integrar el vector de exposición espectral (*D1*) y la capacidad de respuesta institucional local.

Como ejercicio de validez convergente de criterio, se evaluó la asociación entre el IVCR y el Formulario Único de Reporte de Avance de la Gestión (FURAG 2021, dimensión POL06) [13]. El FURAG mide la madurez de la gestión pública municipal dentro del Modelo Integrado de Planeación y Gestión (MIPG), evaluando políticas

de Gobierno Digital y Seguridad de la Información. De las 18 entidades analizadas, 17 dispusieron de registros oficiales (promedio de 63.8; oscilando entre 47.07 en Valencia y 82.42 en Nuquí), mientras que para Barrancominas se imputó la media departamental (68.0). La correlación de Spearman calculada arrojó una asociación negativa moderada (ρ=*-0.54, p=0.02*), la cual se acentúa a nivel departamental (ρ=*-0.68, p<0.05*). Como se esperaba, esto indica que a menor desempeño institucional en FURAG, mayor es la vulnerabilidad cibernética estimada por el IVCR. Ahora, esta comparación debe interpretarse con cautela porque el FURAG se basa en autorreportes administrativos de gobernanza, por lo que no capta la exposición física del espectro (*D1*) ni constituye una prueba concluyente de validez externa absoluta, sino una evidencia preliminar de coherencia entre la vulnerabilidad del IVCR y el déficit de gestión local.

Las dinámicas operativas y regulatorias observadas en los casos de estudio se sintetizan en la Tabla 6, la cual contrasta los niveles de capacidad institucional frente a la efectividad normativa.

Tabla 6. Matriz analítica y síntesis comparativa de la muestra municipal.

Dimensión	Mitú	Bahía Solano	Puerto Gaitán
IVCR	89.8 (Alta)	74.8 (Media-Alta)	58.3 (Media)
¿Plan de Desarrollo menciona ciberseguridad?	No	Sí, genérico	Sí, con acciones y presupuesto
¿Actas del Concejo tratan el tema?	No (1 mención técnica)	No (solo conectividad)	Sí (mesa TIC)
Incidentes documentados	Estafas (no reportadas)	*Ransomware* (pagado)	Ninguno
Cláusulas de seguridad en contratos	0/14	1/8 (genérica)	4/22 (específicas)
Capacidad local evaluada	Muy baja	Baja	Media-baja

Fuente: Elaboración propia.

4. Discusión

El Estado colombiano ha actualizado su marco estratégico con la Estrategia Nacional de Seguridad Digital 2025-2027 [3], resultando insuficiente por los hallazgos de este estudio al demostrar la persistencia de brechas estructurales en los entornos rurales que no han sido mitigadas ni por el CONPES 3995 [2] ni por el instrumento vigente. Para conceptualizar estas vulnerabilidades y proponer vías de resolución técnico-políticas, la discusión se estructura en cinco ejes: la interpretación de las brechas desde los principios de la Guía UIT [1] y el enfoque de capacidades de Sen [8]; la extensión analítica del continuum regulatorio dinámico [6] y su intersección con el modelo 3+5 de transformación digital [7]; la evaluación de los dilemas regulatorios estratégicos entre seguridad, acceso, soberanía y costos; la formulación de una propuesta de "Anexo Rural" de políticas públicas adaptadas; y un análisis comparativo frente a experiencias internacionales homólogas.

4.1. Determinantes de la persistencia de las brechas rurales

La Guía de la Unión Internacional de Telecomunicaciones para el Desarrollo de Estrategias Nacionales de Ciberseguridad [1] postula que las políticas de seguridad digital deben poseer un carácter inclusivo, transversal y garante de los derechos humanos fundamentales (principios 4.3 y 4.5). La evidencia empírica recopilada en este estudio revela una desconexión entre el mandato central y la periferia del país: el 78% de los Planes de Desarrollo Municipal (PDM) en los territorios con menor Índice de Desempeño de Conectividad (IDC) omiten por completo el término "ciberseguridad" o "seguridad digital" (Tabla 3, brecha 2).

Desde la perspectiva teórica del enfoque de capacidades propuesto por Amartya Sen [8], este escenario constituye una manifestación explícita de privación de capacidades. Las comunidades rurales no solo sufren una carencia operativa de servicios de ciberseguridad (funcionamientos), sino que carecen de la libertad real y sustantiva para demandar, codiseñar o asimilarlas debido a que el Estado ha fallado en habilitar los entornos institucionales mínimos (Eje Principal 1 [EP1] ausente) y los canales de participación vinculantes.

El caso de Mitú (Vaupés) es paradigmático e ilustra la naturaleza multidimensional del problema al presentar una baja densidad de ocupación espectral del 85% en horario nocturno, un recurso técnico valioso que podría ser

catalizado para habilitar servicios de conectividad y gestión comunitaria. Sin embargo, su planificación local carece de directrices en materia de seguridad digital demostrando que la vulnerabilidad cibernética en entornos marginales no obedece a un factor estrictamente técnico; se define, ante todo, como una vulnerabilidad político-institucional. La omisión regulatoria en el territorio refuerza la exclusión y valida las críticas globales hacia los marcos de ciberseguridad en economías emergentes, los cuales tienden al sesgo urbano y asumen una homogeneidad territorial inexistente en geografías de baja densidad demográfica [4], [5]. Al evaluar por qué estas brechas se perpetúan a pesar de la reciente adopción de la Estrategia 2025-2027, la teoría del cambio institucional de Mahoney y Thelen [14], en consonancia con la economía política del espectro de Benkler [15], permite identificar tres mecanismos interpretativos asociados: (1) Inercia institucional centralista. Los equipos técnicos y de toma de decisiones de ministerios y agencias reguladoras (MinTIC y ANE) operan bajo incentivos condicionados por entornos urbanos y de alta densidad de mercado, careciendo de métricas o incentivos de descentralización que prioricen la ruralidad. (2) Asimetría de información y subregistro. Las incidencias de ciberseguridad en la ruralidad (estafas por canales móviles, vulneraciones a nodos comunitarios) caen en la invisibilidad estadística debido a la falta de canales locales de denuncia o al desconocimiento de los mismos. Al no registrarse formalmente, no configuran datos de entrada para los modelos de priorización de riesgo del CSIRT nacional (Tabla 3, brecha 1). (3) Ausencia de una demanda social organizada. A diferencia de los sectores industriales y urbanos, las comunidades rurales carecen de gremios tecnológicos o plataformas de gobernanza colectiva que ejerzan presión política hacia el codiseño de una ciberseguridad con pertinencia territorial.

La identificación de estos factores permite superar las recomendaciones genéricas de "atención a lo rural" y delinea intervenciones específicas como la descentralización presupuestal y de capital humano, la creación de canales asíncronos de reporte y el fortalecimiento de la gobernanza comunitaria.

4.2. El continuum regulatorio dinámico y el modelo 3+5 ampliado por ciberseguridad

El marco analítico del *continuum* regulatorio dinámico [6] describe la transición de las políticas de gestión del espectro desde esquemas de asignación estáticos y centralizados hacia sistemas dinámicos inteligentes basados en radio cognitiva. Este modelo prioriza la eficiencia espectral teórica y asume que el acceso de múltiples usuarios en tiempo real a una banda compartida se ejecuta sobre un entorno de confianza mutua y ciberseguridad intrínseca [16]. Pero, los resultados del presente diagnóstico invalidan la universalidad de dicho supuesto en la ruralidad. Si un operador comunitario en zonas aisladas accediera de manera dinámica a la banda de 700 MHz mediante una base de datos de espacios en blanco (*TV White Spaces*) [17], la infraestructura local estaría expuesta a ciberamenazas críticas (ataques de denegación de servicio en las consultas a la base de datos, envenenamiento de espectro o suplantación de nodos) en un ecosistema donde la capacidad de preparación y respuesta local (EP3) es nula. Para solventar esta limitación cognitiva y metodológica, se propone una extensión matemática y conceptual del modelo de eficiencia espectral del continuum. Originalmente, la eficiencia espectral agregada (E) se modela como una función de las proporciones de espectro operadas bajo tres regímenes: estático (S), híbrido o de transición (T), y dinámico (D): $E = f(S, T, D)$. Donde el incremento de los parámetros T y D maximiza la eficiencia teórica de la red. Esta investigación introduce un factor de corrección por ciberseguridad (C), de modo que la eficiencia efectiva (*Eefectiva*) del ecosistema inalámbrico rural no depende únicamente de la disponibilidad de ancho de banda o de la asignación del espectro (*Eteórica*), sino que se ve atenuada por el nivel de vulnerabilidad del entorno, según la relación: $Eefectiva = Eteórica \times (1 - C)$. Donde $C \in [0, 1]$ representa el índice de madurez y resiliencia en ciberseguridad de la infraestructura rural (un valor calculable a partir del inverso del Índice de Vulnerabilidad Cibernética Rural [IVCR] propuesto en este artículo). Si el nivel de seguridad es deficiente $(C \to 0)$, la eficiencia efectiva se degrada críticamente, demostrando que el alcance técnico y la flexibilización del espectro sin capas integradas de seguridad digital por diseño no cierran la brecha digital, sino que expanden la superficie de ataque y el riesgo sistémico de las poblaciones vulnerables. Al contrastar esta realidad con el modelo 3+5 de transformación digital [7], el cual estructura el cambio tecnológico sobre tres condiciones de soporte (inversión sostenible, gobernanza multisectorial y soberanía tecnológica), se observa que la gobernanza multisectorial constituye el eslabón más crítico en la ruralidad colombiana. Existe una desconexión total entre las células de respuesta nacionales (CSIRT Colombia, ColCERT) y la administración pública territorial. El modelo 3+5 debe modificarse para explicitar que la gobernanza multisectorial exige el alcance analítico y operativo de nodos territoriales de ciberseguridad, un requerimiento ausente tanto en el CONPES 3995 como en la nueva Estrategia 2025-2027.

4.3. Balance de dilemas regulatorios estratégicos

La formulación de políticas públicas en entornos complejos de baja densidad poblacional exige la ponderación de tensiones estructurales u objetivos contrapuestos [18]. En la ciberseguridad rural, la escasez de recursos financieros y las limitaciones de conectividad aumentan estas diferencias. En la Tabla 7 se sistematiza los cuatro dilemas regulatorios transversales identificados y fija la posición técnica defendida en esta investigación.

Tabla 7. Matriz de dilemas regulatorios estratégicos en ciberseguridad rural.

Dilemas regulatorios	Descripción	Posición del artículo
Seguridad vs. Acceso	Medidas de seguridad (cifrado, autenticación, *firewalls*) pueden añadir latencia y complejidad, desincentivando el uso de redes comunitarias	Se propone un enfoque proporcional: controles básicos (cifrado WPA2, autenticación por contraseña) obligatorios, pero sin exigir infraestructura de seguridad empresarial (ej. IDS/IPS) inviable en zonas sin conectividad continua
Soberanía tecnológica vs. Equipamiento extranjero	Las radios cognitivas y equipos de red suelen provenir de proveedores extranjeros (China, EE. UU., Europa), lo que puede introducir puertas traseras o dependencia tecnológica	Adoptar estándares abiertos (OpenWRT, GNU Radio) y verificación de código fuente cuando sea posible; promover compras públicas con cláusulas de seguridad auditables
Centralización vs. Autonomía local	Un CSIRT nacional no puede atender incidentes en Vaupés en tiempo real	Crear nodos CSIRT departamentales o enlaces de confianza con formación básica, que operen con protocolos asíncronos (almacenamiento y reenvío)
Costo vs. Beneficio	Implementar ciberseguridad en zonas rurales tiene costos fijos (formación, equipos) que no se justifican por el bajo valor económico aparente	El beneficio no es solo económico, sino de resiliencia democrática: proteger telemedicina, educación y gobierno local. El CONPES 3995 no hizo este análisis de costo-beneficio ampliado

Fuente: Elaboración propia

El detalle de estas tensiones metodológicas permite ir de enunciados abstractos hacia la toma de decisiones basada en evidencia. Consistente con el principio de "prioridades adaptadas" de la Guía UIT [1], el enfoque de seguridad proporcional y diferenciada propuesto se ofrece como una adición práctica e inédita que el gobierno colombiano puede integrar directamente en la operacionalización de sus planes sectoriales de ciberseguridad.

4.4. Propuesta de un "Anexo Rural" para la estrategia nacional de seguridad digital

Para delimitar el alcance metodológico del estudio, es preciso diferenciar la evidencia empírica obtenida mediante el modelo IVCR y la auditoría de convergencia (que demuestra la vulnerabilidad crítica en las dimensiones *D1* a *D4* y la ineficacia del MSPI estándar en la ruralidad) de la propuesta normativa desarrollada. Como respuesta, se formula el "Anexo Rural" (Tabla 8), propuesta de política pública integrada por cinco lineamientos prioritarios de bajo costo y que no constituye una inferencia estadística directa, sino un diseño normativo orientado a resolver las fallas de gobernanza identificadas. Su ejecución no demanda reformas legislativas complejas, sino la articulación de facultades administrativas existentes de MinTIC, ANE, CRC y Cancillería.

Tabla 8. Estructura del Anexo Rural: Cinco políticas prioritarias de ciberseguridad territorial.

Política	Esfera UIT	Acción concreta	Actor responsable	Indicador verificable (plazo 2 años)

P1	Enlace rural de ciberseguridad	EP1 (Gobernanza)	Designar en cada Gobernación un funcionario existente (sin costo adicional) como punto focal de ciberseguridad rural, con formación básica de 40 horas (virtual, asincrónica)	MinTIC, Gobernaciones, DAFP	100% de los departamentos con punto focal designado y formado
P2	Protocolo de respuesta offline para incidentes	EP3 (Preparación)	Desarrollar e implementar un procedimiento de almacenamiento y reenvío de alertas (store-and-forward) para zonas sin conectividad continua, usando radios de baja potencia o mensajería satelital básica	CSIRT Colombia, ANE, CRC	Documento protocolario aprobado y piloto en 5 municipios prioritarios (ej. Mitú, Barrancominas)
P3	Criterios mínimos de seguridad para redes comunitarias en espectro compartido	EP2, EP4 (Riesgos e Infraestructura)	Incorporar en el PNABF y en las licencias de espectro rural una cláusula que exija cifrado WPA2, autenticación básica y respaldo semanal de configuraciones para operadores comunitarios	ANE, MinTIC	Resolución ANE emitida y socializada con 20 operadores comunitarios
P4	Programa de alfabetización digital con módulo de ciberseguridad culturalmente pertinente	EP5 (Capacitación)	Adaptar los cursos de "Seguridad Digital para la Ciudadanía" del MinTIC a lenguas indígenas (español, wayuunaiki, nasa yuwet, etc.) y a formatos offline (USB, radio comunitaria)	MinTIC, Ministerio de Cultura, SENA	Módulos traducidos a 5 lenguas y distribuidos en 50 municipios prioritarios
P5	Acuerdo de cooperación en ciberseguridad amazónica	EP7 (Cooperación internacional)	Establecer un acuerdo bilateral con Brasil (estado de Amazonas) y Perú (departamento de Loreto) para intercambio de inteligencia sobre ciberdelito y asistencia técnica mutua en zonas de triple frontera	Cancillería, MinTIC, CSIRT Colombia	Acuerdo firmado y al menos 2 ejercicios conjuntos (simulacros) realizados

Fuente: Elaboración propia.

4.5 Análisis comparativo internacional y ventana de oportunidad estratégica

El análisis de las experiencias internacionales proporciona lecciones fundamentales para el caso colombiano, evidenciando aciertos y vacíos regulatorios de los cuales el país puede aprender. Brasil, un referente regional clave mediante su *Estratégia Brasileira de Segurança Cibernética* (E-Ciber), presenta un escenario análogo de asimetría territorial. Diversas investigaciones evidencian que el despliegue de infraestructura de conectividad en la Amazonía brasileña avanza desprovisto de salvaguardas de ciberseguridad correlativas, lo que generó una ola de ataques de *ransomware* en municipalidades y centros asistenciales de salud que no fueron reportados debido a la inexistencia de canales de comunicación locales [19]. La lección para Colombia es que conectar sin asegurar maximiza el riesgo social. Exponer a poblaciones rurales digitalmente analfabetas a la red abierta sin esquemas de protección y educación digital las transforma en blancos de vectores de ataque como suplantación de identidad, estafas financieras masivas y pérdida de soberanía de datos personales. Por otro lado, la India ofrece un modelo de mitigación del riesgo a través del programa *Cyber Swachhta Kendra* (Centro de Limpieza Cibernética y Análisis de Malware), operado por CERT-In [20], iniciativa que articula la respuesta a incidentes de *malware*, la

neutralización de *botnets* a nivel nacional y la ejecución de campañas de sensibilización técnica para la ciudadanía [20]. El valor de este modelo radica en su capacidad de apropiación cultural e inclusión lingüística, resultando altamente replicable para la realidad demográfica de Colombia, cuya diversidad étnica abarca 68 lenguas nativas protegidas (65 indígenas, 2 criollas y 1 romaní) [21] que demandan estrategias de seguridad digital diferenciadas. Finalmente, la revisión de la literatura internacional corrobora que ninguno de los países analizados ha integrado conceptual o normativamente la ciberseguridad rural con las políticas de espectro dinámico basadas en radio cognitiva. Esta omisión global representa una clara oportunidad de liderazgo regional y global para Colombia. Al robustecer el modelo del continuum regulatorio dinámico [6] con la introducción del factor de ciberseguridad (C) y la adopción del "Anexo Rural" propuesto en este artículo, el país no solo resolvería una falla estructural interna, sino que consolidaría un marco metodológico de referencia exportable para la región. La evidencia internacional sugiere que Colombia comparte los mismos desafíos que otras economías emergentes, pero posee una ventana de innovación regulatoria en la literatura especializada.

4.6. Limitaciones del estudio y riesgo de inferencia ecológica

Una limitación metodológica radica en la heterogeneidad de las fuentes de información territorial. Si bien el 100% de los componentes del IVCR (*D1* a *D4*) se fundamentan en datos primarios de escala municipal, el ejercicio de validación cruzada con el FURAG requirió imputar la media departamental de Guainía para el municipio de Barrancominas debido a la ausencia de reporte institucional local. Desde la perspectiva del análisis espacial, esta práctica conlleva el riesgo de inferencia ecológica, al asumir que la madurez institucional de la entidad territorial hereda linealmente el promedio de su departamento. Si bien las pruebas de sensibilidad confirman que este ajuste no altera la categoría de prioridad ni la fuerza de la asociación global (ρ=*-0.54*), los resultados específicos sobre la gestión institucional de Barrancominas deben interpretarse como una estimación condicional y no como una medición directa de su capacidad administrativa real. Se remarca la necesidad de que las agendas de monitoreo nacional homologuen la recolección de métricas de ciberseguridad a nivel micro-territorial.

5. Conclusiones

La formulación y adopción de la Estrategia Nacional de Seguridad Digital 2025-2027 [3] es un aporte normativo en el contexto colombiano, al elevar el grado de alineación respecto a las subdimensiones metodológicas de la Guía UIT [1] del 31% al 50%. El 19% de brecha persistente no representa una omisión menor; por el contrario, los datos empíricos muestran que este vacío se concentra críticamente en las esferas de preparación y resiliencia ante incidentes (EP3) y en los mecanismos de cooperación internacional (EP7). Estas dimensiones configuran los pilares operativos más urgentes para salvaguardar los entornos rurales, caracterizados por una conectividad intermitente y una exposición asimétrica a amenazas globales.

A través de esta investigación, se identifican cinco subdimensiones de brecha estructurales específicas, dentro de las cuales emergen cinco vulnerabilidades de alta gravedad: (a) la inexistencia de células de respuesta a incidentes de seguridad informática (CSIRT) con despliegue y alcance territorial; (b) la ausencia de criterios de seguridad digital obligatorios para operadores de redes comunitarias en regímenes de espectro compartido; (c) la omisión absoluta de la ciberseguridad en el 78% de los Planes de Desarrollo Municipal (PDM) de territorios con bajo IDC; (d) la carencia de programas de alfabetización digital adaptados cultural y lingüísticamente a las lenguas indígenas del país; y (e) el vacío de acuerdos de cooperación transfronteriza en materia de ciberdelito con los Estados fronterizos de la cuenca amazónica.

Como interpretación analítica de estos hallazgos, se sugiere que la vulnerabilidad rural no obedece a un factor estrictamente tecnológico, sino a un déficit político-institucional de descentralización y gobernanza multinivel.
La formulación y el análisis de sensibilidad del Índice de Vulnerabilidad Cibernética Rural (IVCR) propuesto sugieren la consistencia preliminar del instrumento para caracterizar y jerarquizar los territorios conforme a su nivel de riesgo sistémico. Municipios como Barrancominas, Mitú, Inírida y Puerto Carreño encabezan el escalafón de vulnerabilidad con puntuaciones que superan el umbral crítico de 80 puntos. La correlación moderada entre el IVCR y el Índice de Desempeño de Conectividad (ρ = *0.52*) ofrecen indicios sobre la validez del constructo inicial del indicador compuesto al reflejar de forma consistente la influencia de la brecha digital sobre la vulnerabilidad, mientras demuestra un valor incremental al evaluar la exposición espectral (*D1*), la debilidad institucional local (*D2*) y la dependencia de servicios esenciales (*D3*). Como propuesta de política pública orientada por este

diagnóstico, se diseña un "Anexo Rural" estructurado en cinco políticas públicas de baja fricción financiera y alta viabilidad operativa.

El aporte de este artículo se consolida en tres dimensiones complementarias iniciando por el plano teórico al extender los marcos de gobernanza multinivel y compartición de infraestructura digital [6] al incorporar una capa de seguridad por diseño indispensable para la viabilidad de los mercados de espectro compartido en zonas de baja densidad; continuando con el plano metodológico al proporcionar una propuesta de aproximación analítica (IVCR) de costo marginal cero, replicable en otras economías emergentes de la región al sustentarse exclusivamente en repositorios y fuentes de información pública. Y terminando con el plano práctico al configurar una hoja de ruta con cinco directrices de política pública que eluden la necesidad de reformas legislativas complejas, requiriendo únicamente la activación de facultades administrativas y de articulación institucional por parte de MinTIC, la ANE y la Cancillería.

La investigación reconoce limitaciones metodológicas que trazan futuras líneas de desarrollo. En primer lugar, la granularidad de los datos de ocupación espectral provistos por la ANE presenta un carácter departamental y no municipal, lo que obliga a recurrir a aproximaciones ecológicas e imputar valores de agregación regional para las variables *D2* y *D4* en municipios que carecían de reportes específicos. En segundo lugar, la ventana temporal del análisis normativo y documental se encuentra acotada a abril de 2026, por lo que transformaciones regulatorias posteriores escapan al alcance de este volumen. Asimismo, el uso de documentos oficiales e institucionales podría introducir sesgos normativos de autoevaluación estatal, los cuales fueron mitigados de manera parcial mediante el estudio de casos múltiples. Finalmente, la falta de repositorios públicos automatizados y desagregados a nivel municipal sobre ciberincidentes reales en Colombia limita la evaluación empírica directa del índice; si bien la validez de constructo por convergencia (efectuada frente a las reclamaciones de la CRC y el Índice de Gobierno Digital) sugiere una adecuada coherencia interna, su comprobación causal definitiva queda supeditada a la futura maduración de los sistemas de registro estadístico nacional.

En última instancia, la ciberseguridad rural deja de ser un apéndice de las políticas de telecomunicaciones para convertirse en un termómetro de la capacidad del Estado para garantizar los derechos y las libertades de los ciudadanos en condiciones de desigualdad geográfica. Mientras los territorios vulnerables permanezcan marginados de la planificación, desprovistos de capital humano calificado y aislados de canales formales de reporte, la brecha digital persistente en el país no se definirá por la simple falta de acceso a la red, sino por una privación real de las capacidades de autogestión y libertad digital de sus comunidades. La gestión del espectro radioeléctrico y la regulación de la interoperabilidad en servicios digitales clave (como las soluciones de dinero y transacciones móviles indispensables en la ruralidad [22]) requieren articulación con un enfoque de ciberseguridad territorial que guíe la transición desde la vulnerabilidad absoluta hasta la resiliencia comunitaria autogestionada; el IVCR y el anexo normativo aquí formulados constituyen una propuesta de andamiaje conceptual e insumo exploratorio en esa dirección.

5.1. Factibilidad institucional, jurídica y presupuestal

La viabilidad del «Anexo Rural» se fundamenta en no imponer cargas regulatorias ni fiscales inviables a las entidades territoriales periféricas, articulando competencias administrativas vigentes:

- Factibilidad jurídica y regulatoria: Las exigencias de seguridad para redes comunitarias (P3) no exigen reformas a la Ley 1341 de 2009; se viabilizan mediante resoluciones reglamentarias de la ANE y MinTIC. El acuerdo amazónico transfronterizo (P5) se enmarca en los instrumentos de cooperación técnica fronteriza no vinculantes de la Cancillería.
- Factibilidad institucional y de capacitación: La designación de puntos focales (P1) aprovecha la estructura administrativa del DAFP sin crear nuevos cargos. Las metas de alfabetización digital (P4) se articulan sobre la capacidad instalada del SENA y MinTIC, adaptando contenidos a formatos asincrónicos offline.
- Sostenibilidad presupuestal: Para proteger el estrecho margen fiscal de los municipios de categoría 5 y 6, la financiación de infraestructura y respuesta a incidentes (P2) se apalanca en el Sistema General de Regalías (SGR - Asignación CTI/OCAD Paz) y en los compromisos de “obligaciones de hacer” derivados de las subastas de espectro.

6. Referencias

[1] Unión Internacional de Telecomunicaciones (UIT). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad*. http://handle.itu.int/11.1002/pub/811cf62d-en

[2] Consejo Nacional de Política Económica y Social (CONPES). (2020). *Documento CONPES 3995: Política Nacional de Ciberseguridad. Departamento Nacional de Planeación, Ministerio de Tecnologías de la Información y las Comunicaciones.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[3] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). *Estrategia Nacional de Seguridad Digital 2025-2027*. MinTIC. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

[4] Galperin, H., Viecens, F. (2017). Connected for development? Theory and evidence about the impact of internet technologies on poverty alleviation. *Development Policy Review, 35* (3), 315-336. https://doi.org/10.1111/dpr.12210

[5] Gillwald, A., Mothobi, O. (2019). *After Access 2018: A demand-side view of mobile Internet from 10 African countries*. Research ICT Africa. https://researchictafrica.net/research/after-access-2018-a-demand-side-view-of-mobile-internet-from-10-african-countries/

[6] Sánchez-Suárez, G. (2026). Gobernanza multinivel y compartición de infraestructura para la sostenibilidad digital en América Latina. *Ingeniería Y Competitividad, 28 (2),* e-20815491. https://doi.org/10.25100/iyc.v28i2.15491

[7] Sánchez-Suárez, G., Ríos-Bocanegra, J. C. (2026). Transformación digital como política de recuperación postpandemia: lecciones internacionales y desafíos para Colombia. *Revista Virtual Universidad Católica del Norte*, (78), 379-407. https://doi.org/10.35575/rvucn.n78a14

[8] Sen, A. (1999). Development as freedom. Oxford University Press.

[9] Agencia Nacional del Espectro (ANE). (2022). *Actualización Anual 2024. Plan Maestro de Gestión del Espectro 2022-2026*. https://www.ane.gov.co/Sliders/ANE2025/Actualizacio%CC%81n_anual_2024_PMGE_versiondefinitiva.pdf

[10] Comisión de Regulación de Comunicaciones (CRC). (2025). *Informe de gestión 2024*. https://www.crcom.gov.co/sites/default/files/Transparencia/informes_de_gestion/Informe-Gestion-2024.pdf

[11] Departamento Administrativo Nacional de Estadística (DANE). (2023). *Encuesta Nacional de Calidad de Vida (ECV) 2023*. https://www.dane.gov.co/index.php/estadisticas-por-tema/salud/calidad-de-vida-ecv/encuesta-nacional-de-calidad-de-vida-ecv-2023

[12] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). *Boletín Trimestral de las TIC. Segundo Trimestre de 2025.* https://colombiatic.mintic.gov.co/679/articles-417629_archivo_pdf.pdf

[13] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022). *Índice de Gobierno Digital – Histórico [Conjunto de datos]*. Datos Abiertos Colombia. https://www.datos.gov.co/d/rtai-k9uh

[14] Mahoney, J., Thelen, K. (2010). *Explaining institutional change: Ambiguity, agency, and power*. Cambridge University Press.

[15] Benkler, Y. (2002). Some economics of wireless communications. *Harvard Journal of Law & Technology, 16* (1), 25-83. https://jolt.law.harvard.edu/articles/pdf/v16/16HarvJLTech025.pdf

[16] Sánchez-Suárez, G., Sierra-Daza, C. A. (2025). Análisis comparativo de los marcos regulatorios para la implementación de infraestructura inalámbrica sostenible: estándares internacionales y el caso de Colombia. *Respuestas, 30* (2), 82-96. https://doi.org/10.22463/0122820X.5134

[17] Ismail, M., Kissaka, M.M., Mafole, P. (2019). *Television White Space Opportunities and Challenges: What Next for the Developing Countries?* IST-Africa Week Conference, Nairobi, Kenya. https://ieeexplore.ieee.org/document/8764834

[18] Hood, C. (1983). *The tools of government*. Macmillan.

[19] Organización de los Estados Americanos, y Banco Interamericano de Desarrollo. (2020*). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe (Informe Ciberseguridad 2020)*. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0002513

[20] Asia Pacific Computer Emergency Response Team (APCERT). (2024). *Annual Report 2023*. https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2023.pdf

[21] Ministerio de Cultura de Colombia. (2010). *Lenguas Nativas y Criollas de Colombia*. https://mng.mincultura.gov.co/areas/poblaciones/APP-de-lenguas-nativas/Paginas/default.aspx

[22] Sánchez-Suárez, G. (2026). Interoperabilidad, espectro y regulación en servicios de dinero móvil: análisis y recomendaciones desde la ingeniería para países en desarrollo. *Revista Colombiana de Tecnologías de Avanzada, 2* (48), 10-18. https://ojs.unipamplona.edu.co/rcta/article/view/4276/8875