adelat

www.adelat.com

RESUMEN EJECUTIVO DSO REVIEW

REDES BAJO ATAQUE

CIBERSEGURIDAD ELÉCTRICA EN LA ERA DE LA TRANSICIÓN ENERGÉTICA



Resumen Ejecutivo · DSO Review N.º 11 - Serie: Tecnología

AUTORES

Alessandra Amaral, Roberto Cajamarca Gómez, Nívia Celestino, Joaquín Lazo Sánchez.

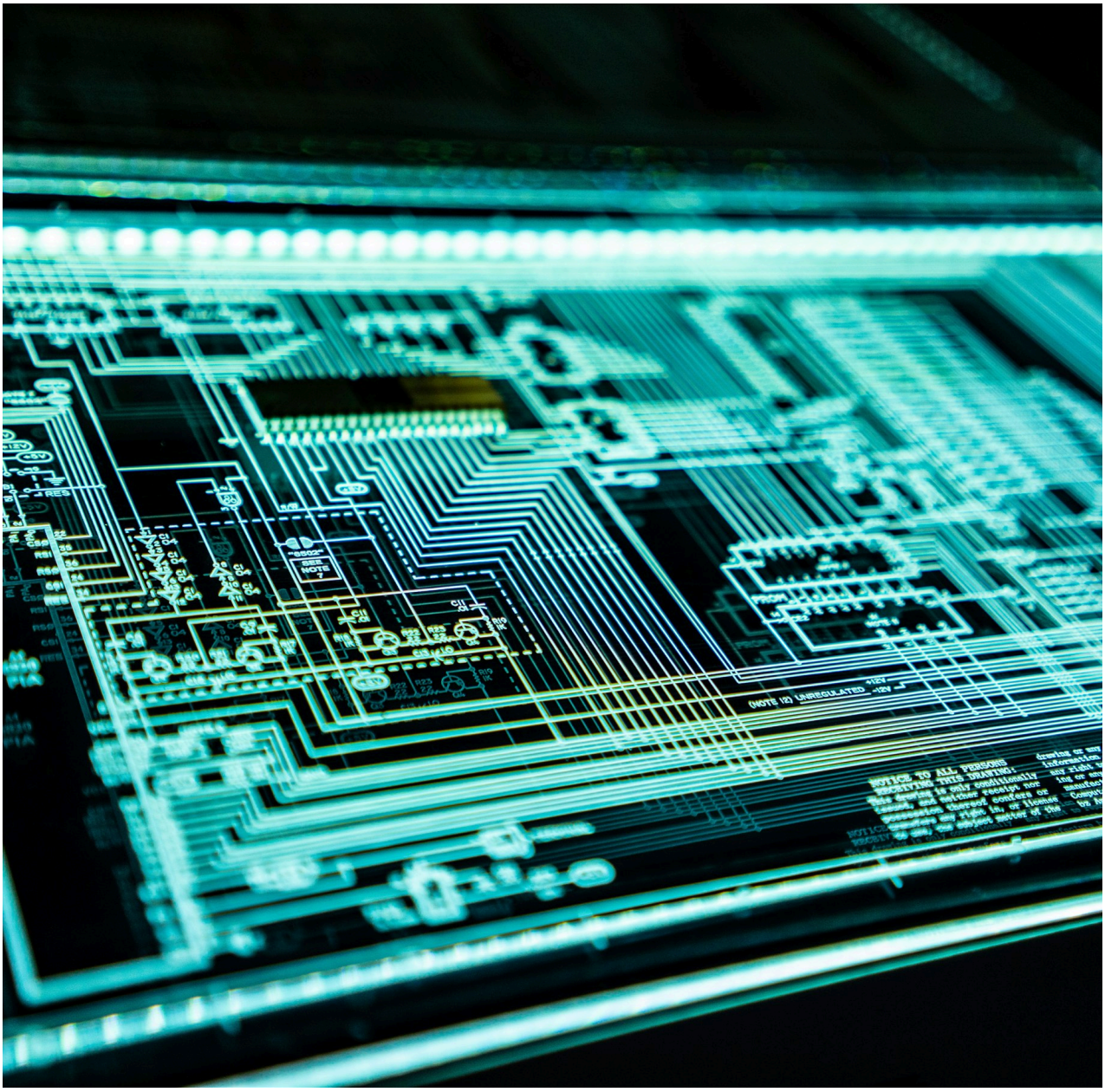
COLABORADORES

Daniel Aranibar, Edward Kenneth Arias Palacio, Rafael Bacis, Guillermo Andrés Cepeda Rodríguez, Nicolás Elgueta C., Alfredo Gallegos González, Jorge Gelmetti, Cristóbal Jaramillo, Luis Jorge Llapiz, Mario Alberto Martínez Martínez, Rubens Mazzon Jr., Gerald Moran, Rodrigo Oliva, Luis Quispe, Emanuel Rodríguez, Rosimiro Santos Ferreira, Juanjo Servetti, Franchesco Somontes Marín, Mariela Uribe Olivas, Fernando Varela, Julián David Velasco Jaramillo, Iván Zamudio.

Septiembre de 2026

PRESENTACIÓN

La transición energética que la regulación impulsa es, en la práctica, una transición digital. Cada avance de la modernización, la medición inteligente, el telecontrol, los recursos distribuidos y la automatización, amplía la superficie de ataque de la red, y proteger ese nuevo frente tiene costos permanentes que hoy ni la tarifa ni la norma reconocen. Este DSO Review examina ese desajuste con evidencia propia: un benchmarking de madurez en ciberseguridad respondido por veinticinco distribuidoras de diez países de América Latina, una revisión de once marcos regulatorios de la región y el análisis de seis jurisdicciones internacionales de referencia. De ese recorrido se desprende la conclusión del documento: mientras el costo de proteger la red no exista para la tarifa, la seguridad seguirá dependiendo de la convicción y de la holgura financiera de cada empresa, un resultado que el propio marco regulatorio produjo y que solo él puede revertir.



01

UNA RED DIGITAL ES UNA RED EXPUESTA

La ciberseguridad de una red de distribución no equivale a la de una oficina. En toda distribuidora conviven dos mundos digitales: los sistemas corporativos, que administran la facturación y la información comercial, y los sistemas de operación, que supervisan y comandan la red física. Proteger el segundo es un problema de naturaleza distinta, porque sus activos están dispersos en miles de kilómetros, buena parte de los equipos fue diseñada antes de la conectividad y opera con vidas útiles de veinte años o más, y todo ocurre en tiempo real, de modo que detener un sistema para revisarlo ya es el daño que se busca evitar.

Los ataques documentados contra empresas eléctricas se ordenan según hasta dónde consiguen llegar. En el primer nivel, el ataque no alcanza la red: el ransomware detiene la facturación y la atención al cliente durante días mientras el suministro continúa, y las filtraciones exponen los datos de millones de clientes. Pero ese nivel no siempre se queda ahí. Cuando la empresa no logra determinar hasta dónde llegó el intruso, recurre al apagado preventivo de su operación, como ocurrió en 2023 en Dinamarca, donde veintidós empresas energéticas fueron comprometidas a través de una vulnerabilidad en el equipo de un mismo proveedor. En el segundo nivel, el ataque alcanza los sistemas de control y el incidente se convierte en un corte de suministro: en 2015, en Ucrania, los atacantes abrieron los interruptores de tres distribuidoras a distancia y dejaron sin electricidad a doscientos veinticinco mil clientes, y un año después el malware Industroyer repitió el efecto sin operador humano, dialogando por sí solo con los protocolos de las subestaciones. La capacidad existe, está probada en terreno y sigue perfeccionándose.



Fig. 1. Los dos niveles de un ciberataque contra una distribuidora

Que el registro regional de incidentes se concentre en el primer nivel no autoriza a concluir que el segundo esté fuera de alcance. Hasta hace poco América Latina no tuvo obligación de reportar incidentes, de modo que el mapa disponible describe mejor el estado

de la norma que el de la amenaza. En la región ya circularon los datos de millones de clientes de una distribuidora, y en 2022 una versión actualizada de Industroyer fue detectada y neutralizada horas antes de ejecutarse contra la red ucraniana. Lo que sí admite medición es la capacidad de cada empresa para contener un ataque antes de que alcance su operación, y a eso se dedicó el benchmarking.

Para quien se queda sin electricidad da lo mismo si el corte se originó en un temporal o en una intrusión informática, y la regulación tampoco distingue: ese corte queda registrado en los mismos indicadores de continuidad que se exigen y se sancionan. Lo que cambia es la causa y lo que hace falta para evitarla, porque un ataque no depende del clima, puede repetirse y puede escoger el momento en que más daño causa, y ninguna de las medidas que la regulación reconoce y remunera hoy sirve para prevenirlo.



02

EL DIAGNÓSTICO REGIONAL

El benchmarking de ADELAT examinó la madurez del sector en cinco dimensiones, desde la protección de la infraestructura que opera la red hasta la gobernanza que decide y financia esa protección. Los resultados, presentados de forma anónima y agregada, describen un sector en movimiento, con un patrón que se repite en las cinco dimensiones: se avanza donde la protección se comporta como una inversión y se rezaga donde exige gasto permanente.

Infraestructura de operación. La protección se organizó durante décadas alrededor de un anillo, la separación entre la red corporativa y la red de operación, y ahí está el mayor avance: un 74% de las empresas ya cuenta con segregación avanzada, con cortafuegos industriales capaces de leer los protocolos eléctricos o aislamiento estricto. Los canales de acceso remoto que atraviesan ese anillo retroceden al 65% con verificación robusta de identidad, y los dispositivos de campo, los medidores y reconectadores instalados en postes y cajas de calle, caen al 21% de protección activa, con cinco empresas que aún mantienen las credenciales de fábrica. La exposición crece así con mayor velocidad exactamente donde la capacidad de contenerla es más débil, porque cada programa de medición inteligente multiplica los dispositivos.

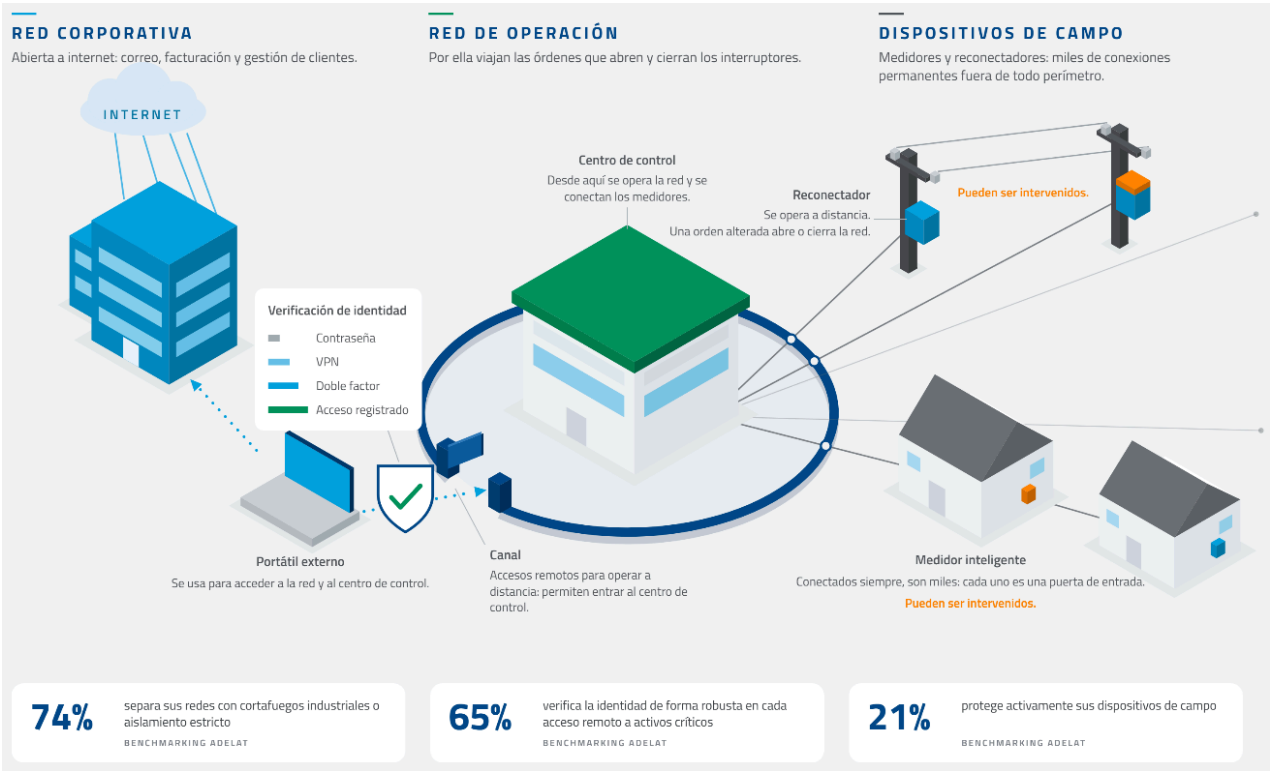


Fig. 2. Los tres frentes de la infraestructura de operación

El detalle de los canales ilustra el tipo de brecha que el diagnóstico revela. El acceso remoto existe por diseño y no por descuido, porque una subestación sin personal permanente necesita atenderse desde otro lugar; el error más frecuente es tratar la VPN como solución completa, porque cifra lo que viaja pero no verifica quién está del otro lado, y

una credencial robada entra por ese mismo túnel sin levantar sospechas. Doce empresas ya exigen un segundo factor de autenticación, pero solo una de las veinte que respondieron alcanza el estándar de accesos creados por tarea, con expiración y registro, de manera que entre un trabajo y el siguiente no exista ningún permiso permanente que robar.

Detección y respuesta. Ninguna barrera es perfecta, y lo que se mide entonces es cuánto se tarda en advertir una intrusión y cuánto en recuperar la operación. Un 46% del sector no observa su red de operación, de modo que una intrusión en esa red solo se advierte cuando ya afecta al servicio. En la recuperación está el dato más alentador del diagnóstico: un 43% de las empresas valida su plan de respuesta con simulacros técnicos anuales, la prueba de que una parte del sector ya entiende que la respuesta se entrena. El mercado ya resolvió cómo proveer esta capacidad, porque de las 13 empresas con monitoreo permanente de ambas redes, 9 lo contratan como servicio tercerizado, una factura mensual y no un activo; lo que sigue sin resolverse es cómo pagarla, porque una suscripción de vigilancia es exactamente el tipo de gasto recurrente que los marcos tarifarios comprimen. Y en la frontera de la anticipación, 13 de las 22 empresas que respondieron ya operan o evalúan la detección de anomalías con analítica avanzada, la contramedida contra los ataques que no usan código extraño sino órdenes legítimas emitidas por quien no debía.



Fig. 3. Las capacidades que administran el tiempo del incidente

Terceros y datos. La exposición de una distribuidora ya no termina en su propia infraestructura: el monitoreo se contrata como servicio, los sistemas se alojan en nubes de terceros y los equipos llegan con el software de su fabricante. El sector gestiona ese frente con instrumentos que se ejercen una vez, la cláusula se firma, la ley se cumple, y se detiene donde comienza la verificación permanente: 12 de 24 empresas exigen cláusulas de ciberseguridad y derecho a auditoría en sus contratos, pero solo una somete cada compra a pruebas técnicas de vulnerabilidad, y un 57% protege los datos de sus clientes hasta donde la ley obliga, con el cifrado todavía como excepción. La protección de datos personales deja además una lección regulatoria: es el frente donde la obligación legal

llegó primero y a más países, y es también el único donde la mayoría de las empresas converge a un estándar común. Donde hubo norma hubo piso.

Las personas. Cualquier trabajador con un correo es una puerta de entrada, y los especialistas que dominan a la vez la red eléctrica y la seguridad informática escasean en todo el mercado. Un 44% de las empresas ya entrena a su personal con simulaciones de phishing y un 12% adicional declara una cultura de seguridad medida con indicadores. En talento, el diagnóstico entrega su resultado más uniforme: 17 de las 25 empresas, un 68%, declaran brechas de conocimiento en áreas específicas, la tecnología de operación entre las primeras, y ninguna declara tener el perfil que necesita completamente cubierto. Es la única brecha que no distingue a las empresas sino que las iguala, porque la escasez es del mercado laboral y no de cada compañía.

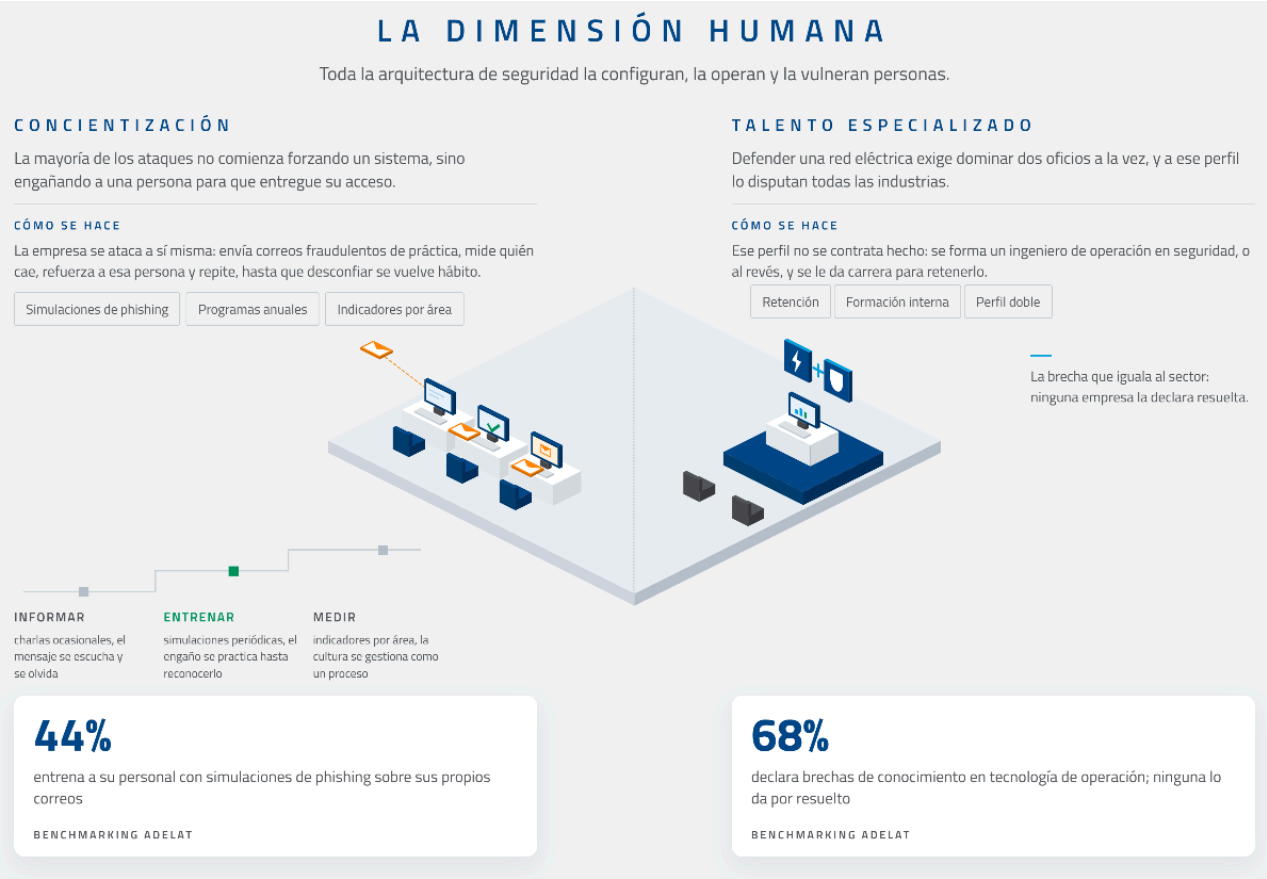


Fig. 4. La dimensión humana, concientización y talento

Gobernanza y presupuesto. La seguridad ya tiene cargo pero rara vez rango: 12 de las 25 empresas aún delegan la responsabilidad en la jefatura de tecnologías de la información, y 8 de las 22 que respondieron solo presentan informes al directorio tras un incidente grave. Ya tiene gasto pero muchas veces sin partida: en 6 de las 20 empresas que respondieron, el gasto en ciberseguridad no existe como línea propia, aunque la evidencia muestra que cuando la partida existe el financiamiento la sigue, porque 12 de las 14 que individualizaron el gasto ya le destinan al menos el 3% de su presupuesto de tecnología. Y ya tiene método pero no habla todavía el idioma en que se deciden las inversiones: solo una de las 23 empresas traduce su riesgo cibernético a términos económicos. La conclusión de la dimensión resume el capítulo completo: la madurez técnica de una distribuidora nunca supera por mucho tiempo a la gobernanza que la financia, y la gober-

nanza interna puede decidir gastar, pero no puede decidir que ese gasto se reconozca en la tarifa.

Leídas en conjunto, las cinco dimensiones confirman el mismo patrón. Los frentes que se resuelven con una obra que puede darse por terminada muestran los mejores resultados; los que exigen turnos que no terminan, ensayos que se repiten, auditorías que deben ejercerse y salarios que se pagan todos los meses muestran los peores. El desempeño del sector disminuye a medida que el costo deja de parecerse a una inversión y empieza a parecerse a un gasto operativo permanente, y esa correlación apunta directamente a los esquemas de remuneración: la parte de la ciberseguridad que más falta hace es también la que el modelo regulatorio menos sabe pagar.



03

LA RESPUESTA REGULATORIA EN AMÉRICA LATINA

La regulación de la región se está moviendo, y en varios casos de forma casi simultánea: entre fines de 2025 y comienzos de 2026, Colombia, Perú, Argentina y Bolivia reformaron su institucionalidad de ciberseguridad en una ventana de apenas tres meses, la señal más clara de que el tema ganó prioridad de agenda. El análisis de once marcos regulatorios, los diez países donde operan las empresas participantes del diagnóstico más Paraguay, muestra sin embargo un avance desigual.

Tres países conforman el núcleo maduro. Brasil, Chile y Colombia ya cuentan con obligaciones sectoriales eléctricas vinculantes que alcanzan expresamente a las distribuidoras, por caminos distintos: la resolución del regulador eléctrico en Brasil (REN ANEEL 964/2021, fiscalizada activamente desde 2025), la ley marco con estándar sectorial en Chile (Ley 21.663 de 2024, con sanciones vigentes desde 2025), y los acuerdos del operador del sistema en Colombia. Un grupo intermedio, Perú, Argentina y Ecuador, construyó institucionalidad nacional que todavía no baja al sector eléctrico, aunque Ecuador dio en 2026 un paso mayor al declarar por ley a la energía eléctrica como infraestructura crítica, con notificación de incidentes en 72 horas y un principio valioso, la notificación de buena fe no constituye por sí sola prueba de negligencia. Y un grupo inicial, Costa Rica, El Salvador, Guatemala, Bolivia y Paraguay, aún no cuenta con norma sectorial eléctrica dedicada.

País	Norma sectorial eléctrica	Alcanza a la distribución	Reporte de incidentes	CSIRT	Reconocimiento tarifario
Brasil	Sí (REN ANEEL 964/2021)	Sí	Sí	Nacional	No
Chile	Sí (Ley 21.663 y estándar del CEN)	Sí	Sí, con sanciones	Nacional; CEN de facto sectorial	No
Colombia	Sí (Acuerdos CNO 1960 y 2088)	Sí	Sí	Nacional y sectorial eléctrico	No
Argentina	No	No aplica	No	Nacional	No
Perú	Parcial (normas técnicas conexas)	Parcial	Sí	Nacional	No
Ecuador	Sí, desde 2026 (Ley Orgánica de Ciberseguridad)	Parcial	Sí (72 horas)	Nacional	No
Costa Rica	No	No aplica	No	Nacional	No
El Salvador	Parcial (Decreto 143/2024)	En principio	Pendiente de reglamento	Nacional	No
Guatemala	No (proyecto en trámite)	No aplica	No	No	No
Bolivia	No	No aplica	No	Nacional	No

Tabla 1. Marco regulatorio de ciberseguridad eléctrica por país
Elaboración propia a partir de la normativa vigente a agosto de 2026. Paraguay, sin regulador eléctrico independiente ni proceso de revisión tarifaria regulada, se analiza en el documento principal.

Bajo esos grupos corren patrones comunes. El estándar norteamericano NERC CIP aparece como referencia técnica tanto en Chile como en Perú, una vía de convergencia de facto incluso donde no hay norma propia. Chile, El Salvador y Ecuador aprobaron su ley de ciberseguridad casi en simultáneo con una ley de protección de datos personales, duplicando las obligaciones de notificación para un mismo incidente sin resolver todavía la coordinación institucional. Y aunque diez de los once países cuentan con un CSIRT nacional operativo, un equipo de respuesta dedicado al sector eléctrico solo existe formalmente en Colombia.

Lo más revelador no es la distancia entre los grupos sino lo que todos comparten. En ninguno de los once países la ciberseguridad existe como rúbrica tarifaria explícita y autónoma: donde la obligación existe, los costos se diluyen en partidas genéricas de operación, mantenimiento o planes de inversión. Es el único punto en el que los once marcos coinciden sin matices, y convierte el problema del financiamiento en el hallazgo regulatorio central de este documento: la exigencia avanza más rápido que los mecanismos para costearla.



04

LA EXPERIENCIA INTERNACIONAL

Seis jurisdicciones llevan entre seis y dieciocho años regulando la ciberseguridad de sus sistemas eléctricos: Estados Unidos, la Unión Europea, el Reino Unido, Australia, la provincia canadiense de Ontario e India. Su experiencia admite una lectura transversal por los problemas de diseño que cada instrumento resuelve.

Cada caso resolvió el problema con un diseño distinto. Estados Unidos construyó el régimen más antiguo y sancionatorio, pero concentrado en el sistema mayorista, con la distribución en manos de cada estado; su instrumento de financiamiento, un incentivo tarifario creado por mandato legislativo en 2021, no ha recibido solicitudes, una lección sobre calibración. La Unión Europea superpuso una directiva general (NIS2) y el primer código de red dedicado a la ciberseguridad eléctrica, con alcance definido por criticidad y no por tamaño. El Reino Unido reunió en el mismo organismo la autoridad de ciberseguridad y la regulación económica, y su control tarifario vigente separa la ciberseguridad del plan de negocio ordinario y le asigna una partida propia condicionada a planes verificables. Australia construyó un marco de madurez sectorial junto con su industria y lo volvió obligatorio por ley solo después de años de medición voluntaria. Ontario reguló a sesenta distribuidoras heterogéneas con autocertificación anual firmada por el máximo ejecutivo antes de pasar a un estándar exigible. E India, el sistema más grande y desigual, optó por regular sin esperar madurez, apostando a que la obligación genere la capacidad.

En la exigencia, los tres modelos coexisten: el control prescriptivo estadounidense (NERC CIP), que se audita mejor que ningún otro pero envejece rápido y castiga a las empresas pequeñas; el sistema de gestión europeo del primer código de red dedicado a ciberseguridad (Reglamento 2024/1366); y los marcos de madurez británico, australiano y canadiense, que definen niveles verificables y gradúan la exigencia según la criticidad de cada operación y no según el tamaño de cada empresa. Ninguna jurisdicción resolvió la heterogeneidad de su sector eximiendo a las pequeñas: todas usan instrumentos de graduación, desde perfiles acumulativos hasta plazos diferenciados.

En el financiamiento, el punto donde la experiencia internacional es más escasa, se identifican cuatro instrumentos, de menor a mayor complejidad institucional: medir el costo de la ciberseguridad como categoría separada y comparable (Unión Europea), el único que no exige modificar el marco tarifario; admitir casos de negocio ante el regulador económico para alcanzar niveles definidos de madurez (Australia); un activo regulatorio con diferimiento y retorno (Estados Unidos), cuya falta de uso es una advertencia sobre la calibración; y una partida tarifaria específica condicionada a un plan verificable, con revisión periódica y devolución de lo no ejecutado (Reino Unido), el diseño más completo. La observación central es que ninguno de estos instrumentos forma parte de la norma de seguridad: todos viven en la regulación económica. La norma define qué hay que hacer; el marco de remuneración define si es posible hacerlo.

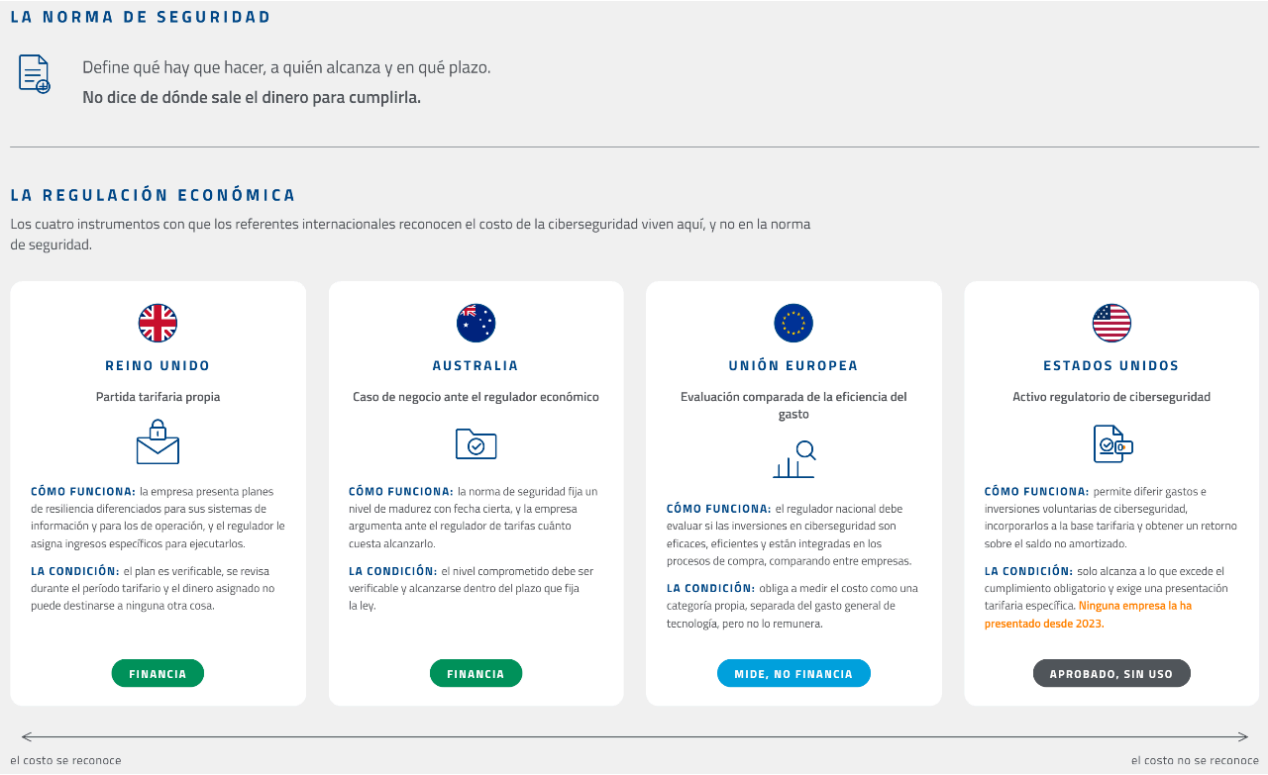


Fig. 5. Cómo se financia la ciberseguridad: cuatro instrumentos internacionales

De ese repertorio, seis elementos resultan aplicables en la región en el corto plazo y con costo regulatorio bajo: medir antes de exigir, como hicieron Australia y Ontario durante años, un camino que el benchmarking de este documento ya inició; adoptar un marco de madurez público como lenguaje sectorial común; la autocertificación anual del nivel de madurez firmada por el máximo ejecutivo, el mecanismo con mejor relación entre costo regulatorio y efecto de gobernanza; separar la norma habilitante del estándar técnico, para que el detalle se actualice con la industria sin reformar la ley; trasladar la ciberseguridad a las condiciones de compra de las adquisiciones nuevas; y medir el costo como categoría separada, el paso previo a cualquier discusión tarifaria.

Técnica	Jurisdicción	Qué se le exige a la empresa más pequeña
Umbrales de impacto sobre el sistema	Unión Europea	Nada si está bajo el umbral; controles mínimos si lo supera
Niveles de impacto del activo	Estados Unidos	Requisitos reducidos, proporcionales al activo
Perfiles de seguridad acumulativos	Australia	Alcanzar el primer perfil, con fecha cierta
Evaluación por resultados	Reino Unido	Demostrar resultados de seguridad, no implementar una lista
Madurez autocertificada	Ontario	Declarar su nivel real y su plan de mejora, con firma del máximo ejecutivo
Plazos diferenciados	Todas	Más tiempo para alcanzar el mismo objetivo

Tabla 2. Técnicas de proporcionalidad en la experiencia internacional

05

CONCLUSIONES Y RECOMENDACIONES

El problema de fondo que este documento describe no es técnico sino de diseño regulatorio. El diagnóstico mostró que el sector avanza donde la protección toma la forma de inversión en activos, el gasto de capital que los marcos tarifarios saben incorporar a la base de remuneración, y se rezaga donde exige gasto operativo permanente, la categoría que esos mismos marcos tienden a comprimir en nombre de la eficiencia. La revisión regional confirmó que en once de once marcos ese gasto no existe como categoría reconocida en la tarifa, y la experiencia internacional enseña que la exigencia y su financiamiento constituyen un solo problema de diseño: donde la obligación llegó sin vía de costeo el cumplimiento se estancó, y donde ambos se diseñaron juntos la protección dejó de competir por recursos contra el resto del presupuesto. Revertir ese resultado no consiste en elegir entre exigir y financiar, sino en hacer ambas cosas en un mismo diseño.

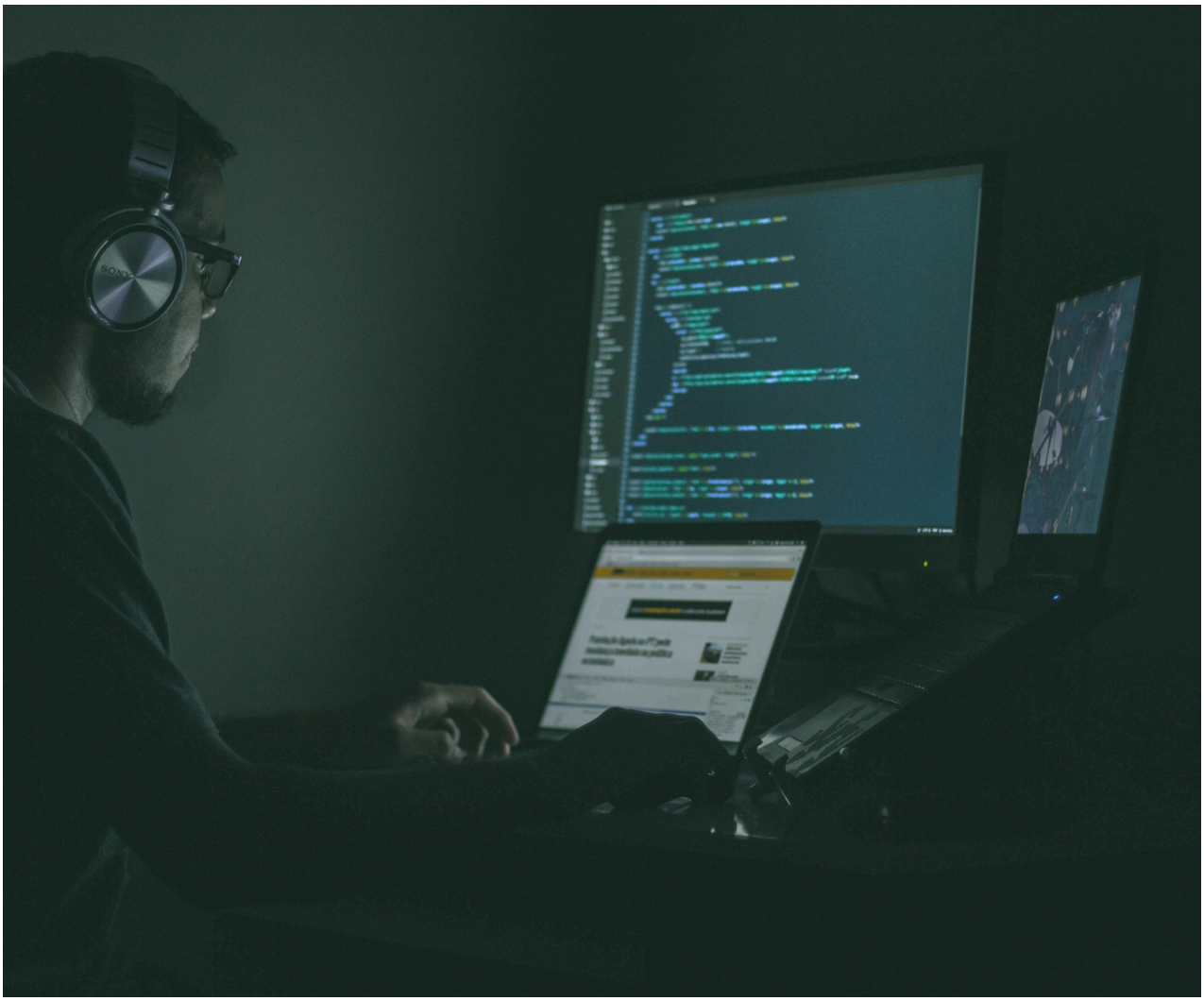
Al regulador, la evidencia le sugiere comenzar por la exigencia: una norma sectorial con enfoque de madurez, graduada por la criticidad de cada operación y no por el tamaño de cada empresa, que separe la norma habilitante, la que fija el nivel a alcanzar y su plazo, del estándar técnico que define cómo medirlo, de modo que la empresa pequeña y la grande recorran la misma escala a ritmos distintos pero verificables. El financiamiento, por su parte, debe definirse como el conjunto de mecanismos para justificar, supervisar y verificar las inversiones que efectivamente reducen el riesgo operativo, siguiendo el repertorio probado: medir el costo como categoría separada, admitir casos de negocio, y establecer una partida tarifaria condicionada a un plan verificable.

Hay un tercer frente que no exige reformas tarifarias, porque depende de decisiones que el regulador puede tomar directamente: el reporte obligatorio de incidentes con confidencialidad y principio de buena fe, que la legislación ecuatoriana de 2026 ya incorporó; la respuesta coordinada, porque la interdependencia del ecosistema eléctrico permite que el compromiso de un eslabón se propague por la cadena y ese espacio está hoy casi vacío en la región, con un solo CSIRT eléctrico formalizado; y la ciberseguridad como requisito de diseño en los mismos planes de medición inteligente y telecontrol que los reguladores impulsan y aprueban, de manera que la modernización no siga ampliando la superficie expuesta más rápido de lo que se protege.

Las empresas, por su parte, no necesitan esperar a la regulación, y el propio diagnóstico muestra que ya comenzaron: seguir midiéndose periódicamente, adoptar un marco de madurez público como lenguaje común, llevar la ciberseguridad al gobierno corporativo con una partida propia y el riesgo expresado en términos económicos, asegurar contractualmente cada compra nueva, y enfrentar en conjunto la escasez de talento especializado, que es del mercado y no de cada empresa. Nada de esto sustituye la tarea del regulador, pero la facilita, porque un sector que se mide, se gobierna y demuestra sus avances vuelve verificable el gasto que pide reconocer. En última instancia, la decisión pendiente es un cálculo simple: regular y financiar la protección de las redes cuesta menos hoy que el incidente que esa protección evita, y el costo de postergarla no desaparece, se acumula en silencio y lo termina pagando el usuario, como interrupción del servicio, como fuga de sus datos o como gasto de emergencia.



Fig. 6. Recomendaciones según complejidad de implementación




adelat