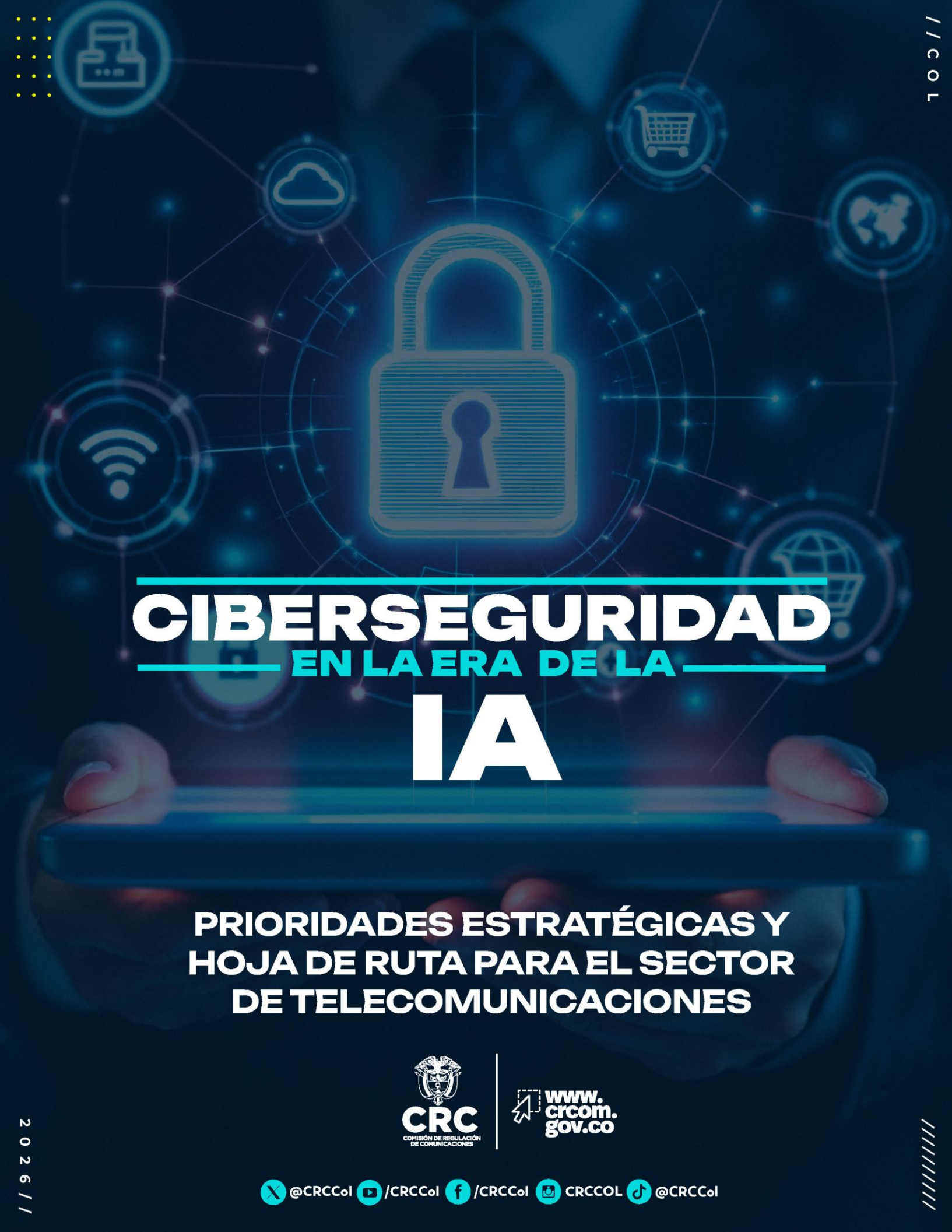

CIBERSEGURIDAD
EN LA ERA DE LA
IA

PRIORIDADES ESTRATÉGICAS Y HOJA DE RUTA PARA EL SECTOR DE TELECOMUNICACIONES

CRC
COMISIÓN DE REGULACIÓN DE COMUNICACIONES

www.crcom.gov.co

@CRCCol /CRCCol /CRCCol CRCCOL @CRCCol

//COL

2026//

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CIBERSEGURIDAD EN LA ERA DE LA IA: PRIORIDADES ESTRATÉGICAS Y HOJA DE RUTA PARA EL SECTOR DE TELECOMUNICACIONES

El panorama digital atraviesa una transformación acelerada, impulsada por la adopción masiva de inteligencia artificial, la creciente interdependencia de las infraestructuras críticas y la sofisticación cada vez mayor de las amenazas cibernéticas y digitales. Frente a este escenario, la Comisión de Regulación de Comunicaciones (CRC) presenta este documento como una hoja de ruta para comprender los riesgos emergentes de mayor urgencia y las capacidades estructurales necesarias para fortalecer la resiliencia digital del sector.

El análisis se organiza en cinco ejes temáticos, ordenados según su nivel de urgencia e impacto sistémico: desde los riesgos que exigen atención inmediata —como la presión energética derivada de la IA y la protección de infraestructuras críticas— hasta las capacidades estructurales de mediano y largo plazo, como la preparación frente a la era post-cuántica y el fortalecimiento de la cibercultura organizacional. Sin perder de vista esta progresión, cada eje combina componentes tecnológicos, organizacionales y humanos necesarios para sostener la resiliencia digital:

- **Crisis dual de la IA:** presión energética y ciberseguridad de la infraestructura eléctrica. Es la prioridad más urgente porque la expansión acelerada de la IA está aumentando la demanda eléctrica y, al mismo tiempo, ampliando la superficie de ataque sobre redes energéticas, centros de datos e infraestructuras críticas. Combina dos riesgos estratégicos: sostenibilidad energética y ciberseguridad.

- **Infraestructuras críticas:** gobernanza, resiliencia y gestión del riesgo sistémico. Es prioritaria porque los servicios esenciales energía, telecomunicaciones, salud, transporte, finanzas y gobierno dependen cada vez más de sistemas digitales interconectados. Una falla o ciberataque puede generar efectos en cascada, por lo que se requiere gobernanza, coordinación y capacidad de recuperación.

- **Seguridad cuántica:** preparación del ecosistema digital frente a la era post-cuántica. Tiene una prioridad estratégica de mediano plazo, ya que la computación cuántica podría comprometer los esquemas actuales de cifrado por lo que representa un riesgo emergente que requiere preparación anticipada. Prepararse desde ahora permite proteger información sensible, redes de telecomunicaciones, certificados digitales, identidades digitales y servicios críticos frente a riesgos futuros.

- **Cibercultura:** el factor humano como eje de la resiliencia digital y la cibercultura como una capacidad que atraviesa todas las prioridades anteriores. Es una prioridad transversal por que el componente humano es el que permite que las estrategias técnicas, regulatorias y

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

organizacionales funcionen en la práctica. Las personas siguen siendo determinantes en la prevención, detección y respuesta ante incidentes. Fortalecer hábitos, formación, liderazgo y reporte oportuno reduce errores humanos, phishing, ingeniería social y fallas de cumplimiento.

- **Entrenamiento y pedagogía:** constituye un eje para fortalecer la protección de las personas, las organizaciones y las instituciones del Estado frente a los riesgos del entorno digital. Su implementación debe trascender la difusión de información técnica y orientarse a la consolidación de capacidades, la adopción de comportamientos seguros y la construcción de una cultura digital basada en la prevención, la corresponsabilidad y la resiliencia.

En adición a estos temas se presenta un mapa de navegación en recomendaciones de ciberseguridad para los PRST sin importar su tamaño ni nivel de adaptación a la ciberseguridad y que busca brindar herramientas para todos los agentes del sector de como avanzar y adaptar las recomendaciones internacionales atendiendo las temáticas ya descritas.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Crisis dual de la IA: presión energética y ciberseguridad de la infraestructura eléctrica

La ciberseguridad energética debe entenderse como una condición habilitante de la economía digital: sin energía segura, resiliente y ciberprotegida, no hay inteligencia artificial sostenible ni soberanía digital efectiva.

La expansión acelerada de la inteligencia artificial y de los centros de datos está redefiniendo la relación entre energía, soberanía digital y ciberseguridad. La creciente demanda eléctrica necesaria para entrenar y operar modelos avanzados de IA convierte a la infraestructura energética en un activo estratégico, pero también en un objetivo crítico para ciberataques dirigidos a redes eléctricas, sistemas de tecnología de la información (IT) y tecnología operativa (OT), centros de datos, plataformas de enfriamiento, proveedores y cadenas de suministro energético-digitales. En este contexto, la ciberseguridad energética debe abordarse como una disciplina interconectada que combine planificación eléctrica, protección de infraestructuras críticas, continuidad operativa, integración segura de IA en entornos OT, gestión de proveedores y coordinación regulatoria. La resiliencia energética ya no depende únicamente de contar con capacidad de generación suficiente, sino de garantizar que la infraestructura que sostiene la economía digital sea segura, sostenible, interoperable y ciberprotegida frente a amenazas cada vez más automatizadas y sofisticadas.

La energía se está consolidando como un habilitador estratégico de la soberanía digital: la capacidad de entrenar y operar modelos avanzados de IA depende cada vez más de contar con infraestructura energética propia, confiable y segura. En consecuencia, la capacidad computacional, los centros de datos y los servicios basados en IA solo podrán considerarse verdaderamente estratégicos si cuentan con un suministro eléctrico confiable, resiliente y protegido frente a amenazas cibernéticas.

El crecimiento de los centros de datos de IA está presionando la planeación eléctrica, incrementando las exigencias de generación, transmisión, distribución, calidad de potencia, refrigeración y continuidad operativa. Esta concentración de grandes cargas digitales puede generar cuellos de botella, congestión y nuevas interdependencias entre la infraestructura eléctrica y los servicios digitales críticos, lo que convierte a la propia estabilidad de la red en un asunto de ciberseguridad.

La digitalización del sector energético está rompiendo el aislamiento tradicional de los entornos OT, exponiendo sistemas industriales, redes eléctricas y procesos físicos a amenazas propias del mundo IT. A esto se suma que muchas infraestructuras energéticas todavía operan con tecnologías heredadas, difíciles de actualizar y con limitaciones para incorporar controles modernos de ciberseguridad, lo que constituye una vulnerabilidad estructural persistente. Como resultado, incidentes que originalmente afectan entornos IT —como ransomware, accesos remotos comprometidos o fallas en proveedores— pueden terminar obligando a desconectar sistemas operativos críticos, afectando directamente la continuidad del suministro.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

La inteligencia artificial no solo representa un desafío defensivo, sino que también potencia las capacidades ofensivas de los atacantes: actores maliciosos pueden usarla para automatizar reconocimiento, ingeniería social, explotación de vulnerabilidades, adaptación de malware y ataques dirigidos contra sistemas o plataformas de monitoreo. Por eso, la integración de IA dentro de los propios entornos OT debe ser controlada y supervisada; si bien puede mejorar el mantenimiento predictivo, la gestión de carga y la respuesta ante incidentes, requiere límites claros, validación de datos, supervisión humana y controles que eviten manipulaciones o decisiones inseguras.

Las organizaciones deben prepararse para escenarios de crisis combinadas, en los que fallas energéticas, eventos climáticos, congestión de red y ciberataques ocurran de manera simultánea. Este riesgo se ve agravado por la naturaleza sistémica de la cadena de suministro energético-digital: la operación de la IA depende de energía, semiconductores, nube, conectividad, enfriamiento, software industrial y mantenimiento especializado, de modo que una falla en cualquiera de estos eslabones puede afectar a todo el ecosistema.

Frente a estos riesgos, que ya no pertenecen a un solo sector, la ciberseguridad energética exige una coordinación regulatoria intersectorial que articule energía, telecomunicaciones, protección de datos, defensa, seguridad digital y regulación ambiental. En definitiva, la resiliencia energética ya no depende únicamente de contar con capacidad de generación suficiente: se requiere una infraestructura ciberprotegida, sostenible, eficiente e interoperable, capaz de sostener los servicios digitales esenciales frente a amenazas cada vez más automatizadas y sofisticadas.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Infraestructuras críticas: gobernanza, resiliencia y gestión del riesgo sistémico

La protección de infraestructuras críticas cibernéticas debe pasar de una visión técnica y sectorial a una estrategia nacional de resiliencia sistémica, basada en riesgo, coordinación interinstitucional y capacidades verificables.

La ciberseguridad de las infraestructuras críticas es una prioridad estratégica para garantizar la continuidad de los servicios esenciales, la seguridad nacional, la estabilidad económica y el bienestar de la población. Su interrupción puede afectar directamente la seguridad nacional, la economía, la salud pública y la calidad de vida de las personas. En un entorno cada vez más digitalizado, sectores como energía, telecomunicaciones, salud, transporte, finanzas, agua y gobierno dependen de plataformas tecnológicas, proveedores, servicios en la nube, sistemas de identidad y redes interconectadas cuya interrupción puede generar efectos sistémicos; de hecho, la propia digitalización está convirtiendo la infraestructura crítica tradicional en infraestructura crítica cibernética. Por ello, su protección exige identificar y priorizar activos esenciales, establecer una gobernanza clara, fortalecer la coordinación interinstitucional, gestionar las interdependencias digitales, asegurar la cadena de suministro, definir capacidades mínimas de ciberseguridad y preparar mecanismos efectivos de reporte, respuesta y recuperación ante incidentes.

No todo activo digital tiene el mismo nivel de criticidad, por lo que la identificación y priorización de activos esenciales es el punto de partida de cualquier estrategia de protección. Esto implica clasificar las infraestructuras según su impacto, su dependencia digital, la población afectada, el tiempo máximo tolerable de interrupción y su exposición cibernética.

La gobernanza es tan importante como los controles técnicos: la protección de infraestructuras críticas requiere autoridades claras, operadores responsables, canales de reporte, esquemas de supervisión, coordinación interinstitucional y capacidades operativas como CSIRT o CERT nacionales.

Las interdependencias digitales aumentan el riesgo sistémico: un incidente en un territorio de la región puede propagarse a otros por dependencias con proveedores cloud, conectividad, servicios de identidad, software industrial, telecomunicaciones o cadenas de suministro globales. En esta misma línea, la cadena de suministro forma parte del propio perímetro de seguridad, ya que proveedores de software, hardware, nube, conectividad, mantenimiento y servicios gestionados pueden convertirse en puntos de entrada o propagación de ataques de alto impacto.

La seguridad física y la ciberseguridad deben gestionarse de forma integrada, dado que los incidentes digitales pueden generar efectos físicos y los eventos físicos pueden, a su vez, comprometer sistemas digitales esenciales. Por ello, la resiliencia de las infraestructuras críticas no puede limitarse a controles técnicos aislados: debe contemplar escenarios híbridos e integrar seguridad física, ciberseguridad, continuidad operativa, inteligencia de amenazas, ejercicios periódicos y comunicación de crisis.

Las capacidades mínimas de ciberseguridad deben ser verificables y proporcionales al riesgo: las organizaciones críticas deben contar con inventario de activos, control de accesos, autenticación multifactor, segmentación IT/OT, gestión de vulnerabilidades, monitoreo, respaldo, recuperación y respuesta a incidentes. Sin embargo, esta resiliencia debe ser demostrable y no meramente declarativa; no basta con tener políticas o planes, sino que es necesario realizar ejercicios, pruebas de recuperación, simulacros de crisis, medición de capacidades y aprendizaje posterior a los incidentes.

La gestión de incidentes requiere reporte oportuno y comunicación coordinada: la respuesta a incidentes críticos debe incluir protocolos de escalamiento, clasificación de severidad, coordinación con autoridades y comunicación transparente con usuarios y ciudadanía. A esto se suma el papel de la inteligencia de amenazas como fortalecedora de la defensa colectiva, ya que el intercambio de indicadores, tácticas y alertas entre sectores permite anticipar ataques, mejorar la detección y reducir la propagación de amenazas.

Los marcos internacionales ofrecen referentes útiles para orientar estos esfuerzos: modelos como NIS2, CER, NIST CSF, CISA y ENISA muestran la importancia de combinar regulación, supervisión, capacidades mínimas, notificación de incidentes y ejercicios de resiliencia.

Para los miembros del Foro Latinoamericano de Entes Reguladores de Telecomunicaciones, el avance en lineamientos, capacidades institucionales y política de seguridad digital representa una base relevante; sin embargo, persisten desafíos en la implementación homogénea, la madurez sectorial, la actualización de inventarios críticos, la participación de operadores privados y la medición objetiva de avances. En este sentido, la protección de infraestructuras críticas cibernéticas debe consolidarse como una política pública intersectorial, basada en riesgo, coordinación y resiliencia demostrable, ya que la ciberseguridad de los servicios esenciales no puede depender de esfuerzos aislados: requiere la articulación conjunta de gobierno, reguladores, operadores, proveedores, academia y sector privado.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Seguridad cuántica: Preparación del ecosistema digital frente a la era post-cuántica

La seguridad cuántica no debe abordarse como un riesgo futuro, sino como una transición estratégica que debe comenzar hoy para proteger datos, redes e infraestructuras críticas frente a la era post-cuántica.

La seguridad cuántica debe entenderse como una transición estratégica que las organizaciones deben iniciar desde ahora, aun cuando la madurez plena de los computadores cuánticos todavía sea incierta. La computación cuántica representa simultáneamente una oportunidad tecnológica y un riesgo estratégico para la ciberseguridad del ecosistema digital: aunque persiste incertidumbre sobre el momento en que los computadores cuánticos alcancen plena capacidad criptográficamente relevante, sus riesgos ya son actuales. Por ello, la preparación cuántica no debe abordarse como un riesgo futuro, sino como una condición necesaria para preservar la confidencialidad, continuidad y resiliencia del ecosistema digital en la era post-cuántica.

Los principales riesgos de esta transición se relacionan con la posible vulneración de esquemas criptográficos tradicionales, la amenaza de "cosechar ahora, descifrar después" y la exposición de datos de larga vida útil, redes 5G, IoT e infraestructuras críticas. Algoritmos como RSA y ECC, ampliamente utilizados para proteger comunicaciones, certificados, identidades digitales y redes 5G, podrían ser comprometidos por computadores cuánticos criptográficamente relevantes. A esto se suma un riesgo ya inmediato: actores maliciosos pueden interceptar y almacenar información cifrada hoy para descifrarla en el futuro, cuando existan capacidades cuánticas suficientes, lo que afecta especialmente a los datos que requieren confidencialidad por años o décadas.

Antes de reemplazar algoritmos, las organizaciones deben identificar dónde se usa criptografía, qué activos protege, qué dependencias existen y cuáles sistemas son críticos para la continuidad operativa. Esta priorización debe basarse en la sensibilidad y la vida útil de los datos, ya que no todos los activos requieren la misma urgencia: deben priorizarse aquellos que necesitan confidencialidad prolongada, como información gubernamental, financiera, de salud, de usuarios, propiedad intelectual e infraestructura crítica.

La cripto-agilidad será una capacidad estratégica: las organizaciones deben diseñar sistemas, contratos y procesos que permitan cambiar algoritmos, certificados y protocolos de forma ordenada, interoperable y sin afectar la prestación de servicios. En paralelo, los enfoques híbridos facilitarán una transición gradual, ya que durante varios años coexistirán mecanismos criptográficos clásicos y post-cuánticos; estos esquemas permitirán probar rendimiento, interoperabilidad, latencia y compatibilidad antes de despliegues masivos.

La cadena de suministro será determinante en la seguridad cuántica, dado que muchos componentes criptográficos están integrados en software, firmware, equipos de red, servicios en la nube, dispositivos

IoT y soluciones de terceros; por ello, los proveedores deberán demostrar capacidad de actualización y soporte post-cuántico. El sector de telecomunicaciones será particularmente sensible a esta transición, debido a su dependencia del cifrado para proteger redes móviles, infraestructura heredada, dispositivos IoT, servicios críticos y datos de larga vida útil, lo que exige una preparación gradual basada en inventarios criptográficos, clasificación de activos, priorización de información sensible, cripto-agilidad, enfoques híbridos, gestión de proveedores y pruebas de interoperabilidad.

La internet cuántica y la distribución cuántica de claves abren nuevas posibilidades: tecnologías como QKD y las redes cuánticas podrían habilitar modelos de comunicación más seguros, aunque todavía enfrentan retos de madurez, escalabilidad, interoperabilidad y adopción sectorial.

La migración post-cuántica exige gobernanza y coordinación sectorial, ya que la transición no es solo técnica: involucra presupuesto, regulación, contratos, estándares, pruebas piloto, responsabilidades institucionales y coordinación entre operadores, proveedores, autoridades y sectores críticos. Los estándares internacionales serán la base de esta transición; iniciativas como las de NIST, CISA, GSMA y la Post-Quantum Cryptography Coalition orientan la identificación de riesgos, la gestión de inventarios, la adopción de PQC y la definición de hojas de ruta. Se resalta, además, la importancia de la cooperación entre los miembros del sector, los estándares internacionales, la gobernanza regulatoria y una hoja de ruta coordinada que permita avanzar hacia infraestructuras digitales más resilientes frente a la era post-cuántica.

La preparación cuántica debe incorporarse a la resiliencia digital: las organizaciones deben integrar el riesgo cuántico en sus estrategias de ciberseguridad, continuidad operativa, gestión de proveedores, protección de datos, seguridad de redes y modernización tecnológica. Para lograrlo, la transición debe ser gradual, medible y adaptable; una hoja de ruta efectiva debe incluir sensibilización, inventario, clasificación de activos, evaluación de exposición, pruebas, actualización contractual, implementación progresiva, monitoreo del riesgo residual y revisión periódica.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Cibercultura: el factor humano como eje de la resiliencia digital

La ciberseguridad sostenible no depende únicamente de mejores tecnologías, sino de organizaciones capaces de convertir a las personas en agentes activos de prevención, detección, respuesta y resiliencia digital.

En un entorno digital marcado por la aceleración tecnológica, la expansión de la inteligencia artificial y la sofisticación creciente del ciberdelito, la ciberseguridad ya no puede entenderse únicamente como un asunto técnico. Si bien las herramientas de detección, automatización y protección son indispensables, la evidencia muestra que el factor humano continúa siendo uno de los principales puntos de exposición, pero también una de las capacidades más relevantes para fortalecer la defensa y la resiliencia organizacional. Las personas siguen siendo uno de los principales vectores de riesgo, pero también pueden convertirse en la primera línea de defensa cuando cuentan con formación, conciencia y canales adecuados de reporte.

La cibercultura, entendida como componente estratégico de la seguridad digital, parte de reconocer que los atacantes suelen aprovechar errores, fatiga, desconocimiento, credenciales comprometidas o técnicas de ingeniería social para acceder a sistemas protegidos. En un entorno donde los ataques explotan precisamente esos comportamientos, la cultura se consolida como un perímetro de defensa que permite transformar hábitos cotidianos en capacidades preventivas y de respuesta. Frente a ello, las organizaciones deben avanzar hacia una cultura de ciberseguridad sostenible, en la que las personas no sean vistas únicamente como vulnerabilidades, sino como actores activos en la prevención, detección, reporte y respuesta frente a incidentes.

La tecnología por sí sola no garantiza resiliencia: aunque la automatización, la inteligencia artificial y las herramientas de detección son indispensables, su efectividad depende del juicio humano, la capacidad de contextualizar riesgos y la toma de decisiones bajo presión.

La formación debe ir más allá del cumplimiento formal: las capacitaciones anuales o los cursos genéricos no son suficientes. Se requieren simulaciones de phishing, ejercicios de crisis, casos prácticos, campañas continuas y entrenamiento adaptado a los riesgos reales de cada organización. Junto con ello, el reporte temprano es tan importante como evitar el error: no es realista esperar que todos los usuarios eviten siempre hacer clic en enlaces sospechosos, por lo que lo esencial es que sepan reportar rápidamente cualquier actividad anómala, permitiendo una respuesta oportuna que limite el impacto.

El liderazgo define el tono de la cultura de ciberseguridad: la alta dirección y los líderes de cada área deben modelar comportamientos seguros, asignar recursos, comunicar la importancia estratégica de la ciberseguridad y convertirla en una responsabilidad organizacional compartida. En esa línea, la seguridad debe ser una responsabilidad transversal que no corresponde únicamente a los equipos técnicos o de TI, sino que debe involucrar a las áreas jurídicas, financieras, operativas, comerciales, de talento humano y a todos los niveles de la organización.

Una cultura resiliente requiere confianza y empoderamiento: los errores deben tratarse como oportunidades de aprendizaje y no como motivos de sanción automática, lo que fomenta la comunicación abierta, el reporte oportuno y la mejora continua. Para saber si esta cultura efectivamente avanza, medir comportamientos es clave: no basta con medir la asistencia a capacitaciones, sino que deben evaluarse indicadores como las tasas de reporte de phishing, el uso de autenticación multifactor, la rapidez en la aplicación de parches, la calidad de los reportes y la higiene de credenciales.

La escasez de competencias sigue siendo una barrera crítica: la falta de talento especializado y de habilidades internas limita la capacidad de las organizaciones para anticipar, detectar y responder a amenazas sofisticadas. A esto se suma que la inteligencia artificial aumenta tanto los riesgos como las capacidades defensivas: los atacantes la emplean para automatizar campañas, crear contenidos maliciosos más persuasivos y coordinar operaciones, mientras que las organizaciones pueden usarla para identificar tendencias de riesgo humano y focalizar sus intervenciones.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

El entrenamiento y pedagogía en ciberseguridad debe extenderse a toda la sociedad

En el entorno digital contemporáneo, una sociedad informada, formada y consciente es un pilar estratégico para construir un ciberespacio más seguro.

La ciberseguridad es una condición esencial para proteger a las personas, las organizaciones y los Estados frente a los riesgos del entorno digital. Sin medidas adecuadas de prevención, formación y respuesta, la ciudadanía, las empresas y las instituciones quedarían expuestas a amenazas que pueden afectar la privacidad, la continuidad de los servicios, la confianza pública y la seguridad de la información.

El entrenamiento y la pedagogía en ciberseguridad son iniciativas que reflejan un esfuerzo global por sensibilizar y empoderar a las personas en esta materia. Su propósito no se limita a divulgar información, sino que apunta a transformar hábitos, fortalecer capacidades y consolidar una cultura digital. En este sentido, una sociedad informada y consciente constituye un pilar fundamental para la construcción de un ciberespacio más seguro.

En general, las campañas de promoción de la cibercultura persiguen tres objetivos principales:

- **Visibilizar amenazas digitales:** alertar sobre tácticas de ciberdelincuentes, riesgos emergentes, vulnerabilidades en entornos IT/OT y prácticas inseguras que pueden comprometer la información.
- **Impulsar acciones concretas:** motivar a empresas, entidades públicas y personas a revisar sus controles de seguridad, actualizar políticas, fortalecer capacidades y adoptar buenas prácticas.
- **Empoderar a la sociedad:** ofrecer recursos comprensibles y accesibles para que no solo los expertos, sino también ciudadanos, pequeñas empresas y organizaciones, puedan desenvolverse de forma más segura en línea.

Distintos gobiernos y entidades han impulsado campañas de sensibilización orientadas a promover la ciberseguridad. Estas iniciativas buscan fortalecer acciones en entrenamiento, prevención y colaboración.

Uno de los antecedentes más relevantes es el *National Cyber Security Awareness Month*, declarado oficialmente en Estados Unidos en 2004 para promover la ciberseguridad entre ciudadanos y organizaciones. Esta conmemoración, celebrada durante el mes de octubre, busca difundir información actualizada, fortalecer la sensibilización pública e incentivar el intercambio de buenas prácticas.

Europa adoptó esta práctica en 2012 mediante el *Mes Europeo de la Ciberseguridad*, iniciativa organizada por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Posteriormente, en 2018, Chile se convirtió en el primer país latinoamericano en celebrar este mes, como parte de un esfuerzo por promover la ciberseguridad y desarrollar ejercicios nacionales en la materia.

Además de estas campañas, existen fechas simbólicas orientadas a sensibilizar a la sociedad sobre la protección de la información. Entre ellas se encuentra el Día Internacional de la Seguridad de la Información, conmemorado el 30 de noviembre, establecido después del gusano Morris de 1988 —uno de los primeros programas maliciosos de propagación masiva en internet— como recordatorio de la necesidad de proteger los datos digitales.

Construir una pedagogía y entrenamiento en seguridad digital requiere continuidad, recursos y compromiso institucional. Los cambios de comportamiento sostenibles no se logran de manera inmediata; por ello, las siguientes prácticas ayudan a fortalecer un comportamiento sólido y sostenible:

- **Simulacros para medir la capacidad de los protocolos.** Los simulacros de ciberseguridad son una herramienta esencial para convertir los planes en capacidades reales de respuesta. Estos ejercicios permiten recrear, en un entorno controlado, escenarios como ataques, filtraciones de datos, interrupciones de servicios críticos o compromisos de proveedores, con el fin de evaluar cómo actúan los equipos bajo presión, qué tan claros son los roles y responsabilidades, si los canales de comunicación funcionan adecuadamente y cuánto tiempo toma escalar, contener y recuperar un incidente.

  Su valor no reside únicamente en probar tecnología, sino en identificar brechas de coordinación, vacíos procedimentales y decisiones críticas que no deberían tomarse por primera vez durante una crisis real. Por ello, los simulacros deben realizarse de manera periódica, involucrar tanto a las áreas técnicas como a la alta dirección y a las unidades jurídicas, operativas, financieras y de comunicaciones, y concluir con lecciones aprendidas, métricas de desempeño y ajustes concretos a los planes de respuesta, continuidad y recuperación.

- **Desarrollo de competencias y cierre de brechas laborales.** Las organizaciones deben invertir tiempo y recursos en el desarrollo del talento humano necesario para enfrentar la ciberdelincuencia. La escasez de especialistas y de competencias en ciberseguridad sigue siendo uno de los principales desafíos para consolidar capacidades internas.

  Para responder a esta necesidad, muchas empresas destinan presupuestos a contratación, formación y actualización profesional. Asimismo, evalúan tecnologías como la inteligencia artificial generativa para apoyar tareas especializadas, optimizar procesos y reducir parcialmente las brechas de talento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **Liderazgo y gestión.** Cuando los líderes adoptan comportamientos ejemplares como el uso de contraseñas robustas, la notificación de eventos e incidentes y el cumplimiento de los protocolos de protección de datos, transmiten que la ciberseguridad es una responsabilidad compartida y un riesgo estratégico del negocio, no solo un asunto técnico.

- **Comunicación y preparación.** Los líderes de todas las áreas deben conocer con claridad sus funciones y responsabilidades frente a un incidente de ciberseguridad. También deben saber cómo comunicarse entre sí y con los equipos técnicos para coordinar decisiones oportunas. Cuanto más se practiquen y evalúen las respuestas ante distintos escenarios, mayor será la preparación y confianza institucional para enfrentar una crisis.

- **Comunicación abierta.** Las organizaciones deben promover entornos en los que los empleados puedan informar riesgos, errores o actividades sospechosas de manera temprana y sin temor a represalias. Esta apertura permite detectar amenazas potenciales con mayor rapidez y responder antes de que escalen. Además, los nuevos empleados deben conocer desde el primer día las políticas, directrices y comportamientos esperados en materia de ciberseguridad.

- **Seguridad psicológica y empoderamiento.** Los errores deben abordarse como oportunidades de aprendizaje, no como motivos de sanción automática. Para ello, las personas necesitan sentirse seguras y motivadas para reportar situaciones inusuales o comportamientos que parezcan incorrectos. Una cultura orientada al aprendizaje empodera a los empleados para expresarse, compartir ideas, mejorar de forma continua y tomar decisiones seguras en su trabajo diario.

- **Responsabilidad compartida.** La ciberseguridad debe asumirse como una responsabilidad de toda la organización, no únicamente del área de tecnología. Áreas como legal, operaciones, finanzas y talento humano también inciden en la protección de la información y deben incorporar prácticas seguras en sus procesos. Cuando las personas comprenden cómo sus acciones afectan la seguridad institucional, es más probable que adopten comportamientos responsables y colaboren con otros equipos para reducir riesgos.

- **Gestión de operaciones complejas.** La complejidad operativa es una de las principales cargas para los equipos de seguridad. A medida que los sistemas se vuelven más complejos, aumenta la probabilidad de errores, configuraciones incorrectas y brechas aprovechables por los atacantes. Por ello, es indispensable validar periódicamente la eficacia de las configuraciones, revisar la implementación de controles y reducir la posibilidad de que el error humano se convierta en una vulnerabilidad.

- **Políticas de ciberseguridad claras y comprensibles.** Las políticas deben ser prácticas, accesibles y fáciles de aplicar. No basta con definir reglas generales; también es necesario explicar el "cómo" y el "por qué" de cada directriz, de manera que las personas comprendan su utilidad y puedan incorporarlas a sus actividades cotidianas. Además, estas políticas deben

revisarse periódicamente para reflejar nuevas amenazas, cambios tecnológicos y necesidades organizacionales.

- **Demostrar el retorno de la inversión.** Para la dirección financiera, el gasto en ciberseguridad puede percibirse como difícil de medir, especialmente cuando sus beneficios se expresan en riesgos evitados. Por esta razón, los centros de operaciones de seguridad deben justificar sus inversiones con indicadores claros que muestren su aporte a la continuidad del negocio, la reducción de incidentes y la protección de activos críticos.

  La ciberseguridad también debe evidenciar su impacto en el desempeño financiero mediante la prevención de brechas, la reducción de falsos positivos, la automatización de tareas, la respuesta rápida ante incidentes y la actualización constante de controles. Estos elementos permiten reducir riesgos, optimizar recursos y demostrar valor ante la alta dirección.

- **Medición del desarrollo y cambio de comportamiento.** No se puede mejorar aquello que no se mide. Sin embargo, limitar la evaluación a los índices de finalización de cursos no permite identificar cambios reales en los comportamientos. Por ello, es necesario utilizar indicadores que muestren si las personas están incorporando prácticas seguras en su actividad cotidiana, tales como:

  - ✓ Medir no solo quién hace clic en enlaces sospechosos, sino también quién los reporta oportunamente.
  - ✓ Medir qué tan pronto se instalan las actualizaciones críticas.
  - ✓ Medir la fortaleza de las contraseñas y los patrones de reutilización.
  - ✓ Medir la frecuencia, oportunidad y calidad de los reportes realizados por los empleados.

  Con esta información, los líderes pueden tomar decisiones basadas en evidencia y demostrar avances ante directivos, auditores y reguladores.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Mapa de navegación en recomendaciones de seguridad digital para PRST

Una guía de referencia para los proveedores de redes y servicios de telecomunicaciones (PRST), de redes fijas y móviles.

1. Presentación y alcance

Las redes de telecomunicaciones son la infraestructura sobre la que descansan la economía digital, los servicios esenciales y la vida cotidiana de las personas. Proteger su seguridad y resiliencia es un interés compartido por todo el sector. Este mapa ofrece a los proveedores de redes y servicios de telecomunicaciones (PRST) una guía de navegación hacia los marcos, esquemas y buenas prácticas de seguridad digital que la industria y los organismos internacionales han desarrollado a lo largo de los años.

Su propósito es funcionar como una puerta de entrada ordenada: en lugar de prescribir controles, señala dónde encontrarlos, qué problema resuelve cada recurso y en qué orden conviene aproximarse a ellos según el tamaño y la madurez de cada operador. La Comisión de Regulación de Comunicaciones (CRC) actúa aquí en su papel de articulador, facilitando el acceso del sector a un cuerpo de conocimiento que ya existe y que se encuentra disperso entre múltiples fuentes.

Esta guía está dirigida a todos los PRST, con independencia de la tecnología de acceso que operen. La mayoría de los recursos que se reseñan son transversales: los marcos de gestión de riesgo, los sistemas de gestión de la seguridad de la información, la respuesta a incidentes o los principios de confianza cero aplican por igual a una red fija, a una red móvil o a una red convergente. Un subconjunto menor es específico de redes móviles (por ejemplo, el aseguramiento del equipo de red móvil o la protección de la señalización entre operadores móviles). Cada recurso del mapa indica su alcance.

El mapa presentado es una guía de referencia de carácter orientativo. No constituye una norma de obligatorio cumplimiento, no establece política pública, y no es un instrumento de inspección, vigilancia y control. La adopción de los recursos que aquí se reseñan es enteramente voluntaria y queda a criterio de cada operador, en la medida en que su contexto y sus capacidades lo permitan.

Coherente con uno de los principios rectores de la regulación en Colombia, esta guía se elabora con estricta neutralidad tecnológica: describe los recursos por las funciones de seguridad que abordan y no favorece a ningún fabricante, proveedor, solución comercial ni arquitectura de red en particular. Las referencias a tecnologías concretas se hacen únicamente cuando son necesarias para ubicar el recurso, y siempre en términos genéricos.

La guía incorpora además una neutralidad de escala: reconoce que el universo de PRST es heterogéneo, desde grandes operadores de cobertura nacional hasta proveedores pequeños y regionales, y que un

recurso útil para uno puede resultar desproporcionado para otro. Por ello cada recurso se acompaña de una indicación de madurez sugerida.

2. Por qué importa la seguridad digital en las redes

Los operadores de telecomunicaciones enfrentan un panorama de amenazas mixto que combina los riesgos tradicionales de las tecnologías de la información con los propios de las redes de comunicaciones. A medida que las redes evolucionan, ese panorama se amplía por tres vías principales:

- Una superficie de ataque creciente, derivada de la mayor cantidad de dispositivos conectados, servicios y puntos de interconexión entre redes.
- La adopción de arquitecturas abiertas y virtualizadas, que sustituyen elementos de red basados en hardware dedicado por entornos de software flexibles. Esta transición aporta agilidad y diversidad de proveedores, pero introduce nuevas consideraciones de seguridad asociadas a la virtualización, la segmentación de red y la computación en el borde.
- La dependencia de cadenas de suministro complejas y globales, donde la seguridad de un operador depende también de las prácticas de sus proveedores de equipo y servicios.

Existe un cuerpo maduro de marcos internacionales que abordan estos riesgos. El reto para muchos operadores no es la ausencia de orientación, sino su dispersión y, en ocasiones, su fragmentación. Cuando cada jurisdicción traduce los mismos marcos en requisitos locales divergentes, el costo de cumplimiento aumenta y la diversidad de proveedores disponibles puede reducirse, en perjuicio de la competencia y del usuario.[1]

Frente a ello, ofrecer un mapa de navegación hacia marcos comunes y ampliamente reconocidos aporta un valor concreto: evita reinventar soluciones, facilita que operadores de distinta escala encuentren un punto de partida apropiado, y contribuye a una aproximación coherente a la seguridad digital del sector.

3. Cómo usar esta guía

El corazón de esta guía es el mapa de recursos de la Sección 5, organizado por fuente de referencia (GSMA, NIST, CISA, ENISA, 3GPP, UIT y OEA). Cada fuente se presenta como una «estantería» con sus documentos concretos. Para cada documento se indica: qué problema resuelve, su tipo de acceso y su enlace oficial.

[1] OCDE (2026), Towards international coherence of cybersecurity regulations, OECD Digital Economy Papers. El estudio identifica que la fragmentación regulatoria en ciberseguridad incrementa los costos de cumplimiento y desvía recursos de las funciones esenciales de seguridad, y observa que muchos gobiernos prefieren desarrollar marcos propios en lugar de incorporar estándares internacionales, lo que conduce a normas nacionales divergentes. Disponible en https://www.oecd.org/en/publications/towards-international-coherence-of-cybersecurity-regulations_bd1f199a-en.html

La Sección 4 ofrece la capa de gestión que da sentido al mapa: cómo entrar (gestión de riesgo y Sistema de Gestión de Seguridad de la Información - SGSI), cómo operar la seguridad en el día a día, y cómo avanzar por niveles de madurez.

3.1. Leyenda de acceso y alcance

- Público: disponible de forma gratuita y abierta en el sitio oficial del publicador.
- Miembros: requiere membresía, registro o compra en la entidad correspondiente.
- Transversal: aplicable a operadores fijos, móviles y convergentes por igual.
- Móvil: específico de redes móviles o de la interconexión entre ellas.

3.2. Niveles de madurez del lector

- Inicial: operadores pequeños o regionales que están estableciendo sus primeras prácticas estructuradas de seguridad.
- Intermedio: operadores con prácticas establecidas que buscan robustecer su gestión operativa de la seguridad.
- Avanzado: operadores de mayor escala o que despliegan tecnologías de nueva generación, con necesidades de aseguramiento más exigentes.

4. La capa de gestión: cómo entrar, operar y avanzar

Antes del catálogo de recursos conviene situar las tres decisiones de gestión que estructuran cualquier programa de seguridad. Esta sección es la columna vertebral; el mapa de la Sección 5 es la caja de herramientas que la alimenta.

4.1. Cómo entrar: gestión de riesgo y sistema de gestión de la seguridad

Todo operador necesita un punto de partida que le permita entender su riesgo y estructurar su programa. Existen dos puertas de entrada complementarias, y conviene distinguirlas porque cumplen funciones distintas.

La primera es un marco de gestión de riesgo. El *NIST Cybersecurity Framework (CSF) 2.0* organiza la seguridad en seis funciones: gobernar, identificar, proteger, detectar, responder y recuperar. Sirve para diagnosticar la postura de seguridad y priorizar mejoras con un lenguaje común entre la dirección y los equipos técnicos[2]. Es una entrada ligera, de acceso público y con versión en español, idónea para operadores que inician.

[2] NIST, *Cybersecurity Framework 2.0*. Versión oficial en español disponible. https://www.nist.gov/cyberframework

La segunda es un sistema de gestión de la seguridad de la información (SGSI). La norma *ISO/IEC 27001* define un sistema de gestión certificable, con políticas, roles y controles sometidos a mejora continua. A diferencia del CSF, que ayuda a *diagnosticar y priorizar*, el SGSI proporciona la *estructura de gestión formal* que sostiene el programa en el tiempo. Para el sector, la *Recomendación UIT-T X.1051* traduce los controles de ISO/IEC 27002 al contexto específico de las organizaciones de telecomunicaciones[3]. Ambos enfoques son complementarios: es habitual usar el CSF para orientar y un SGSI para gobernar.

4.2. Cómo operar: gestión operativa de la seguridad

Una vez establecido el punto de partida, el reto de la mayoría de los operadores, especialmente los de nivel intermedio, es operar la seguridad en el día a día. Cinco frentes convierten un marco en una práctica viva:

- **Gobernanza:** responsables, políticas esenciales y comités de decisión.
- **Gestión de vulnerabilidades:** inventario de activos, identificación, priorización y remediación recurrentes, apoyándose en marcos transversales estandarizados como los CISA CPG, NIST SP 800-53 y las prácticas internas de gestión de riesgo del operador.
- **Monitoreo y detección:** registro centralizado de eventos, alertas y, en organizaciones más maduras, un centro de operaciones de seguridad (SOC).
- **Respuesta a incidentes:** la guía *NIST SP 800-61 Rev. 3* (2025) se alinea con el CSF 2.0 y presenta la respuesta a incidentes como parte de la gestión de riesgo de ciberseguridad[4], de modo que el operador que adoptó el CSF como entrada encuentra continuidad de lenguaje. La *Guía Práctica para CSIRTs* de la OEA es un excelente apoyo regional para constituir un equipo de respuesta[5].
- **Gestión del riesgo de la cadena de suministro:** criterios de seguridad para proveedores, apoyados en *NIST SP 800-161 Rev. 1* y, en redes móviles, en esquemas de aseguramiento de equipo como NESAS.

4.3. Cómo avanzar: arquitecturas abiertas, virtualización y confianza cero

A medida que las redes incorporan virtualización, segmentación y computación en el borde, el perímetro tradicional pierde eficacia como única línea de defensa. El paradigma de confianza cero responde a ese cambio: parte de no conceder confianza implícita por la mera ubicación en la red y exige verificar cada acceso de forma continua.

---

[3] Recomendación UIT-T X.1051 (06/2023), *Information security controls based on ISO/IEC 27002 for telecommunications organizations*. https://www.itu.int/rec/T-REC-X.1051-202306-I/en

[4] NIST SP 800-61 Rev. 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (abril de 2025). https://csrc.nist.gov/pubs/sp/800/61/r3/final

[5] OEA, Guía Práctica para CSIRTs (Vol. 2, 2023). https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Hay dos referencias oficiales y de acceso público especialmente útiles. La primera define la arquitectura de confianza cero y sus componentes lógicos[6]. La segunda ofrece un modelo de madurez por etapas, de lo tradicional a lo óptimo, a través de cinco pilares (identidad, dispositivos, redes, aplicaciones y datos), pensado para adoptarse de forma flexible según el tamaño y el punto de partida de cada organización[7]. Para redes móviles, la microsegmentación del núcleo y el análisis de amenazas de virtualización (recursos GSMA y ENISA del mapa) complementan este enfoque.

5. El mapa de recursos por fuente

Esta sección es el catálogo navegable. Cada fuente se presenta como una estantería de documentos concretos. Los recursos marcados como «Miembros» requieren membresía en la entidad correspondiente.

5.1. GSMA: Asociación global de operadores móviles

La base de conocimiento de ciberseguridad de la GSMA es uno de los repositorios sectoriales más relevantes de buenas prácticas específicas del sector móvil[8]. Se organiza en dominios; a continuación, los documentos públicos más relevantes y una selección de los reservados a miembros.

Gestión de riesgo

Documento	Qué resuelve	Acceso
Baseline Security Controls (FS.31)	Conjunto de controles de seguridad de base para establecer una postura sólida; con autoevaluación.	Público
MoTIF Framework (FS.57)	Marco de inteligencia de amenazas: tácticas, técnicas y procedimientos con que los adversarios atacan redes móviles.	Público
Coordinated Vulnerability Disclosure (FS.23)	Programa para que investigadores reporten vulnerabilidades y se gestione su corrección.	Público
Post-Quantum Telco Impact Assessment (PQ.01)	Dependencias y plazos para la transición del sector a tecnología cuántico-segura.	Público
Guidelines for Quantum Risk Management for Telco (PQ.02)	Adapta la evaluación de riesgo tradicional a los riesgos criptoanalíticos.	Público
T-ISAC Service Offering (FS.32)	Centro de intercambio y análisis de información de amenazas del sector.	Público
Security Manual (FS.30)	Manual de amenazas clave a las redes móviles.	Miembros
AI Security Guidelines (FS.49)	Guías de seguridad para riesgos asociados a tecnología de IA.	Miembros

[6] NIST SP 800-207, *Zero Trust Architecture* (agosto de 2020); de acceso gratuito. Existe traducción no oficial al español. https://csrc.nist.gov/pubs/sp/800/207/final
[7] CISA, *Zero Trust Maturity Model v2.0* (abril de 2023). https://www.cisa.gov/zero-trust-maturity-model
[8] GSMA, *Cybersecurity Knowledge Base*. https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Seguridad de la red del operador

Documento	Qué resuelve	Acceso
5G Security Guide (FS.40)	Visión integral de la seguridad 5G: referencias y controles para la evolución de la red.	Público
Network Function Virtualisation (FS.33)	Análisis de amenazas de la virtualización de funciones de red y su infraestructura.	Público
Micro-Segmentation in 5G Core (FS.61)	Guía para proteger el tráfico este-oeste del núcleo 5G mediante microsegmentación.	Público
Voicemail Security (SG.20)	Gestión de PIN y contraseñas para el acceso seguro al correo de voz.	Público
Exchange of Subscriber Credentials (FS.28)	Protección de credenciales UICC intercambiadas entre operadores y proveedores.	Público
VoLTE Security (FS.22)	Amenazas conocidas de voz sobre LTE y contramedidas.	Miembros
SMS Blasters Briefing (FS.67)	Amenaza de falsas estaciones base usadas para phishing por SMS.	Miembros

Seguridad de dispositivos

Documento	Qué resuelve	Acceso
IoT Security Guidelines (FS.60)	Metodología para desarrollar servicios IoT seguros y mitigar amenazas comunes.	Público
Device Anti-Theft (SG.24)	Requisitos para localizar dispositivos perdidos/robados y proteger sus datos.	Público
Cryptographic Algorithms (FS.35)	Algoritmos de autenticación, privacidad e integridad en GSM, UMTS, LTE y 5G.	Público
Device Software Updates (FS.25)	Requisitos para actualizaciones de software críticas durante incidentes.	Público
(e)UICC Profiles (FS.27)	Configuración segura de perfiles UICC.	Público
Operator Guide to Mobile Malware (SG.19)	Métodos de ataque, tipos de malware móvil y estrategias de defensa.	Miembros

5.2. NIST: Instituto Nacional de Estándares y Tecnología (EE. UU.)

Los marcos del NIST son transversales (sirven a redes fijas y móviles), de acceso público y, varios de ellos, disponibles en español. Constituyen la espina dorsal de la capa de gestión.

Documento	Qué resuelve	Acceso
Cybersecurity Framework (CSF) 2.0	Marco de gestión de riesgo en seis funciones; diagnóstico y priorización. Versión en español.	Público · Transversal
SP 800-53 Rev. 5	Catálogo exhaustivo de controles de seguridad y privacidad para sistemas de información.	Público · Transversal

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Documento	Qué resuelve	Acceso
SP 800-61 Rev. 3	Recomendaciones de respuesta a incidentes, alineadas con las funciones del CSF 2.0.	Público · Transversal
SP 800-207 (Zero Trust)	Define la arquitectura de confianza cero y sus componentes lógicos.	Público · Transversal
SP 800-161 Rev. 1	Gestión del riesgo de ciberseguridad en la cadena de suministro (C-SCRM).	Público · Transversal

5.3. CISA: Agencia de Ciberseguridad e Infraestructura (EE. UU.)

CISA traduce marcos y buenas prácticas en herramientas accionables y modelos de madurez. Aunque su origen es federal, varios de sus recursos son de acceso público y pueden servir como referencia para organizaciones de distintos sectores.

Documento	Qué resuelve	Acceso
Zero Trust Maturity Model v2.0	Modelo de madurez por etapas y cinco pilares; adopción flexible según escala.	Público · Transversal
Secure by Design	Principios para que los productos se diseñen seguros desde el origen (coautoría internacional, con la OEA).	Público · Transversal
Cross-Sector Cybersecurity Performance Goals (CPG)	Conjunto priorizado de prácticas base de alto impacto, útil para operadores que inician.	Público · Transversal

5.4. ENISA: Agencia de la Unión Europea para la Ciberseguridad

ENISA aporta orientación de detalle para entornos 5G, virtualización y medidas de seguridad sectoriales. Sus recursos son públicos y mapean a las especificaciones técnicas subyacentes.

Documento	Qué resuelve	Acceso
5G Security Controls Matrix	Catálogo consolidado de objetivos y controles técnicos y no técnicos para 5G.	Público · Móvil
NFV Security in 5G – Challenges and Best Practices	60 retos de seguridad y 55 buenas prácticas para la virtualización de funciones de red.	Público · Móvil
Security in 5G Specifications	Análisis de los controles de seguridad presentes en las especificaciones del estándar.	Público · Móvil
Threat Landscape for 5G Networks	Panorama de amenazas, activos y vulnerabilidades del entorno 5G.	Público · Móvil
Guideline on Security Measures under the EECC	Medidas de seguridad para proveedores de redes y servicios de comunicaciones electrónicas.	Público · Transversal

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5.5. 3GPP: Proyecto de especificaciones de redes móviles

El 3GPP define la base técnica de la seguridad de las redes móviles. Sus especificaciones son públicas y constituyen el fundamento sobre el que operan esquemas como NESAS.

Documento	Qué resuelve	Acceso
TS 33.501 — Security architecture for 5G	Arquitectura y procedimientos de seguridad del sistema 5G.	Público · Móvil
SCAS — Security Assurance Specifications	Casos de prueba de seguridad para el equipo de red; base técnica de NESAS.	Público · Móvil

Nota sobre aseguramiento de equipo (GSMA + 3GPP): el esquema NESAS combina la auditoría de los procesos del fabricante (GSMA) con los casos de prueba SCAS (3GPP). Es voluntario y funciona como una línea de base sobre la cual cada operador o autoridad puede añadir requisitos. Véase el Apéndice B.

5.6. UIT: Unión Internacional de Telecomunicaciones

La UIT aporta recomendaciones de seguridad específicas del sector de telecomunicaciones y programas de fortalecimiento de capacidades, con fuerte presencia en español y pertinencia regional.

Documento	Qué resuelve	Acceso
Rec. UIT-T X.1051	Controles de seguridad de la información para organizaciones de telecom, basados en ISO/IEC 27002.	Público · Transversal
Rec. UIT-T X.1055	Guía de gestión de riesgo y perfil de riesgo para organizaciones de telecomunicaciones.	Público · Transversal
Rec. UIT-T X.1056	Guía de gestión de incidentes de seguridad para organizaciones de telecomunicaciones.	Público · Transversal
Global Cybersecurity Index (GCI)	Referencia comparativa del estado de la ciberseguridad por país.	Público · Transversal
Guía de Estrategia Nacional de Ciberseguridad (NCS Guide)	Marco para el desarrollo de capacidades y estrategias nacionales.	Público · Transversal

5.7. OEA: Organización de los Estados Americanos (CICTE)

La OEA es el referente regional más cercano: coordina la red hemisférica de respuesta a incidentes y publica guías en español, varias pensadas para el contexto latinoamericano.

Documento	Qué resuelve	Acceso
Guía Práctica para CSIRTs (Vol. 2, 2023)	Modelo para constituir y operar un equipo de respuesta a incidentes de forma sostenible.	Público · Transversal
Buenas Prácticas para establecer un CSIRT nacional (2016)	Proceso para crear y desplegar un CSIRT: misión, alcance, servicios y recursos.	Público · Transversal

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Documento	Qué resuelve	Acceso
Red CSIRTAméricas	Plataforma hemisférica de intercambio de información entre CSIRTs gubernamentales.	Público · Transversal
Portal de publicaciones del Programa de Ciberseguridad	Reportes de madurez regional, infraestructura crítica y white papers (incl. marco NIST).	Público · Transversal

6. Ruta sugerida de adopción por madurez

La siguiente ruta reordena los recursos del mapa en una secuencia práctica, según el nivel de madurez del operador. No es una prescripción, sino una sugerencia de por dónde empezar y cómo avanzar. Es válida para operadores fijos y móviles; los pasos específicos de redes móviles se señalan como tales.

6.1. Nivel inicial, establecer la base

Caso típico de operadores pequeños o regionales. La prioridad es construir una visión estructurada del riesgo con recursos de acceso público.

1. Comience por el NIST CSF 2.0 (versión en español) para adoptar un lenguaje común de gestión de riesgo y diagnosticar su postura actual.
2. Use los CISA CPG o los GSMA FS.31 para identificar y priorizar mejoras de base de forma proporcionada.
3. Defina un mínimo de gobernanza: responsables, políticas esenciales y un procedimiento básico de respuesta a incidentes (apóyese en la *Guía Práctica para CSIRTs* de la OEA).

6.2. Nivel intermedio, operar la seguridad

Nivel donde se ubica la mayoría de los operadores y donde el salto de capacidades es más exigente. El foco se desplaza de «tener un marco» a «operar la seguridad de forma sostenida».

1. Formalice un SGSI tomando *ISO/IEC 27001* y la *Rec. UIT-T X.1051* como referencias sectoriales.
2. Implemente una gestión de vulnerabilidades recurrente (apóyese en la orientación sectorial de la UIT y en los CISA CPG).
3. Establezca monitoreo y detección con registro centralizado de eventos.
4. Robustezca la respuesta a incidentes con *NIST SP 800-61 Rev. 3*, definiendo manuales por tipo de incidente.
5. Incorpore seguridad en la cadena de suministro con *NIST SP 800-161*; en redes móviles, solicite a proveedores evidencia de participación en NESAS.

6.3. Nivel avanzado, asegurar y modernizar

Para operadores de mayor escala o que despliegan tecnologías de nueva generación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. Adopte progresivamente principios de confianza cero, usando el modelo de madurez de CISA para planear la transición de forma escalonada.
2. En redes móviles, considere NESAS / SCAS para el aseguramiento del equipo de red y los recursos GSMA/ENISA de virtualización y microsegmentación.
3. Apóyese en la 5G Security Controls Matrix de ENISA y la Guía de seguridad 5G (FS.40) para los entornos de arquitecturas abiertas y virtualizadas.

La progresión no es lineal ni obligatoria: cada operador adopta lo que resulte apropiado y proporcionado a su realidad, en la medida en que su entorno lo permita.

7. Glosario

Término	Definición
CSF	*Cybersecurity Framework*. Marco de gestión de riesgo de ciberseguridad del NIST.
C-SCRM	Gestión del riesgo de ciberseguridad en la cadena de suministro.
CSIRT	Equipo de respuesta a incidentes de seguridad informática.
ENISA	Agencia de la Unión Europea para la Ciberseguridad.
GSMA	Asociación global que representa a los operadores de telefonía móvil.
NESAS	Esquema de aseguramiento de la seguridad del equipo de red (GSMA + 3GPP).
NFV	Virtualización de funciones de red.
SCAS	Especificaciones de aseguramiento de seguridad definidas por el 3GPP.
SGSI	Sistema de gestión de la seguridad de la información (p. ej., ISO/IEC 27001).
SOC	Centro de operaciones de seguridad.
Confianza cero	Paradigma que no concede confianza implícita por la ubicación en la red y verifica cada acceso de forma continua.
3GPP	Proyecto que desarrolla las especificaciones técnicas de las redes móviles.

8. Apéndice A — Tabla maestra de recursos

Fuente	Documento	Acceso	Alcance	Madurez
NIST	CSF 2.0	Público	Transversal	Inicial
ISO/UIT	ISO 27001 / X.1051	Miembros /Público	Transversal	Intermedio
CISA	CPG	Público	Transversal	Inicial
GSMA	FS.31 Baseline Controls	Público	Móvil	Inicial/Interm.
OEA	Guía Práctica CSIRTs	Público	Transversal	Inicial/Interm.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Fuente	Documento	Acceso	Alcance	Madurez
UIT	UIT-T X.1051, X.1055, X.1056	Público	Transversal	Intermedio
NIST	SP 800-61 Rev. 3 (incidentes)	Público	Transversal	Intermedio
NIST	SP 800-161 (cadena de suministro)	Público	Transversal	Intermedio
NIST	SP 800-53 Rev. 5 (controles)	Público	Transversal	Intermedio/Avanzado
NIST	SP 800-207 (Zero Trust)	Público	Transversal	Intermedio/Avanzado
CISA	Zero Trust Maturity Model	Público	Transversal	Intermedio
GSMA	FS.40 Guía de seguridad 5G	Público	Móvil	Avanzado
GSMA	FS.33 NFV / FS.61 Microseg.	Público	Móvil	Avanzado
ENISA	5G Security Controls Matrix	Público	Móvil	Avanzado
ENISA	NFV Security in 5G	Público	Móvil	Avanzado
3GPP	TS 33.501 / SCAS	Público	Móvil	Avanzado
GSMA+3GPP	NESAS	Público	Móvil	Intermedio/Avanzado

9. Apéndice B — Detalle de NESAS y SCAS

Naturaleza del esquema. NESAS es un esquema voluntario definido conjuntamente por la GSMA y el 3GPP. Se compone de dos partes: una auditoría de los procesos de desarrollo y de gestión del ciclo de vida del producto por parte del fabricante, y una evaluación de productos por laboratorios acreditados, con base en los casos de prueba SCAS.

Relación NESAS / SCAS. Las especificaciones SCAS, del grupo de seguridad del 3GPP, son los casos de prueba técnicos: especifican *qué* se evalúa y *cómo*. NESAS es el esquema que gobierna el proceso: define las reglas de auditoría, acredita los laboratorios y publica los resultados. En el contexto de NESAS, ambos componentes son complementarios: SCAS aporta la base técnica de prueba y NESAS estructura el esquema de auditoría/evaluación.

Uso por parte del operador. NESAS proporciona evidencia independiente de que el equipo de un proveedor fue evaluado frente a un estándar reconocido. Es recomendable solicitar a los proveedores participar en el esquema y aportar la evidencia durante las adquisiciones. SCAS es una línea de base común, sobre la cual cada operador o autoridad conserva la libertad de exigir requisitos adicionales según su contexto.

Distinción de alcance. NESAS y SCAS son específicos del equipo de redes móviles. Un operador exclusivamente fijo encontrará más pertinentes los marcos transversales (NIST, UIT, CISA, ISO 27001) y centrará el aseguramiento de proveedores en criterios contractuales y de gestión.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Todos los enlaces de este documento fueron incluidos con base en la información disponible al momento de elaboración del mismo. Este es un documento de referencia orientativo de la CRC y no constituye norma, política pública ni instrumento de inspección, vigilancia y control.