GSMA

El impacto de la regulación de ciberseguridad en los operadores móviles

November 2025

GSMA

La GSMA es una organización global que une al ecosistema móvil para descubrir, desarrollar y ofrecer innovación esencial para entornos comerciales positivos y cambios sociales. Nuestra visión consiste en liberar todo el poder de la conectividad para que las personas, la industria y la sociedad prosperen. Como representante de los operadores móviles y organizaciones de todo el ecosistema móvil e industrias adyacentes, la GSMA realiza su contribución a sus miembros bajo tres grandes pilares: Conectividad para el Bien, Servicios & Soluciones de Industria, y Alcance & Difusión. Esta actividad incluye promover políticas públicas, abordar los mayores desafíos sociales de la actualidad, apuntalar la tecnología y la interoperabilidad que hacen funcionar a la conectividad móvil, y proporcionar la plataforma más grande del mundo que reúne al ecosistema móvil en las series de eventos MWC y M360.

Te invitamos a conocer más en **gsma.com**

frontier economics

Frontier Economics es una empresa líder de consultoría económica. Frontier utiliza principios económicos para ofrecer asesoramiento y análisis claros sobre asuntos complejos a muchas de las empresas más importantes del mundo, reguladores sectoriales líderes, departamentos gubernamentales y organizaciones internacionales. Con más de 350 empleados en Dublín, Ámsterdam, Berlín, Bruselas, Colonia, Londres, Madrid, París y Praga, Frontier Economics Limited (www.frontier-economics.com) es una de las consultoras económicas más importantes e influyentes de Europa. La empresa cuenta con profesionales expertos de renombre en una amplia gama de sectores, como los mercados digitales, las telecomunicaciones, la energía, el transporte, el servicio postal, el agua y la salud, habiendo asesorado a partes interesadas tanto del sector público como del privado en el diseño y la adopción de mejores prácticas en políticas regulatorias, teniendo en cuenta el posible impacto de estas políticas en el comportamiento de las partes interesadas y, por ende, en los mercados en general. Frontier trabaja en estrecha colaboración con su empresa filial y legalmente independiente: Frontier Economics Australia.

01.
Resumen ejecutivo

La conectividad móvil y la ciberseguridad en un mundvo digital

La conectividad móvil es fundamental en las economías y sociedades modernas. Permite la comunicación, el acceso a la información y a los servicios públicos y la participación económica. A medida que la dependencia en lo digital aumenta, también lo hace la exposición a amenazas cibernéticas, lo que supone riesgos graves no solo para las personas, los negocios y los Gobiernos, sino también para toda la sociedad en su conjunto. Garantizar la seguridad y la protección de las redes móviles no es, por lo tanto, una preocupación meramente técnica, sino un requisito para establecer confianza y seguridad en un mundo conectado digitalmente.

La naturaleza cambiante de las ciberamenazas genera aumentos en los costos y complejidad que deben enfrentar los operadores móviles para implementar un monitoreo y protección eficaz de la ciberseguridad , lo cual hace cada vez más importante el papel de una regulación balanceada. Las regulaciones bien diseñadas brindan apoyo a los operadores móviles a la hora de gestionar los riesgos de manera proporcionada y eficaz, fortaleciendo así la seguridad y la resiliencia de la red.

En cambio, los marcos normativos mal diseñados y desalineados pueden imponer costos desproporcionados, complicar las operaciones e, incluso, empeorar las vulnerabilidades.

Los marcos regulatorios fragmentados o mal diseñados pueden desviar los recursos de las verdaderas mejoras de seguridad, retrasar la respuesta ante incidentes y frenar la innovación en materia de tecnologías de protección. A fin de cuentas, esta situación no solo pone en peligro las redes móviles, sino también la seguridad y la confiabilidad de los servicios digitales esenciales.

En este informe, encargado por la GSMA, se explora la manera en que la regulación de ciberseguridad afecta la capacidad de los operadores móviles de defenderse contra amenazas cambiantes. Además, se centra en los costos, las dificultades y las oportunidades que plantea la regulación y analiza cómo las políticas bien diseñadas pueden mejorar la resiliencia, mientras que los marcos desalineados aumentan los riesgos

El alto costo de la ciberseguridad para los operadores móviles

Actualmente, la ciberseguridad es un pilar fundamental para las operaciones de las redes móviles y requiere, cada vez más, de recursos importantes. En este informe, se estima que los operadores móviles, a nivel mundial, destinan entre USD 15.000 millones y USD 19.000 millones al año en actividades de ciberseguridad “centrales”, incluidas las funciones de seguridad técnica y los equipos de monitoreo de amenazas.[1] Es probable que esta cifra sea un cálculo menor al gasto total real en ciberseguridad, ya que no incluye actividades más amplias, como la gobernanza, la capacitación y la garantización de la resiliencia de las redes. A medida que las amenazas evolucionen, se prevé que los costos aumentarán a cifras entre los USD 40.000 millones y los USD 42.000 millones para 2030. La carga de estas inversiones es muy pesada, especialmente para los operadores móviles de los países de bajos y medios ingresos (LMIC), donde los elevados costos fijos en ciberseguridad deben recuperarse de una base de clientes con un promedio de ingresos por usuario (ARPU) bajo.

Buenas prácticas en la regulación de ciberseguridad

Los operadores móviles de todo el mundo se enfrentan a dificultades comunes en el cumplimiento de la regulación de ciberseguridad, que incluyen políticas y marcos regulatorios fragmentados, capacidad institucional limitada para apoyar a los operadores móviles, normas rígidas o prescriptivas, y una carencia de plataformas eficaces para intercambiar inteligencia sobre amenazas. Como consecuencia, los operadores a menudo incurren en costos desproporcionados o innecesarios al abordar las preocupaciones de ciberseguridad y, en algunos casos, las políticas mal diseñadas pueden incluso aumentar los riesgos cibernéticos. Muchas de estas dificultades se pueden mitigar a través de mejores prácticas regulatorias, como enfoques de regulación de ciberseguridad más coordinados, basados en riesgos y centrados en resultados.

En muchos países, los operadores se ven regidos por un mosaico de leyes que se superponen, políticas específicas para el sector y obligaciones impuestas por múltiples reguladores. Frecuentemente, esta falta de coherencia provoca costos de cumplimiento más elevados, requerimientos de presentación de informes duplicados y una falta de armonización en las definiciones o en los procesos, sin que nada de esto aporte en reducir las ciberamenazas. En algunos casos, los operadores están sujetos a obligaciones contradictorias o deben presentar informes sobre el mismo incidente a través de varios canales.

La regulación mal diseñada crea ineficiencias operativas y desvía los recursos hacia el cumplimiento en lugar de destinarlos a la verdadera mitigación de riesgos. Además, puede reducir la inversiones en innovación, tanto en servicios avanzados como en nuevas soluciones de seguridad.

Los formuladores de políticas públicas deberían garantizar que los marcos de cumplimiento y presentación de informes de incidentes estén alineados en todos los sectores y ámbitos normativos. Con marcos horizontales bien diseñados, se puede preservar la flexibilidad específica para el sector y, a la vez, impulsar estrategias coherentes de ciberseguridad nacional.

1 Análisis de Frontier Economics.

Los estándares internacionales pueden utilizarse para lograr una coherencia transfronteriza

Las ciberamenazas son un riesgo internacional, pero las políticas de ciberseguridad se implementan a nivel nacional, lo que provoca discrepancias entre los distintos países. Esta desalineación entre marcos nacionales complica a los operadores que trabajan en distintas jurisdicciones. Incluso dentro de la Unión Europea (UE), donde las políticas están diseñadas para ser coherentes entre los Estados miembros, los operadores siguen enfrentándose a inconsistencias en la implementación a nivel nacional. Los estándares incongruentes resultan en ineficiencias y obstaculizan las respuestas eficaces a las amenazas que surgen.

Las políticas incoherentes en materia de ciberseguridad nacional encarecen los costos de los operadores que brindan servicios en distintos mercados. Las políticas nacionales de ciberseguridad pueden alinearse a los estándares internacionales y de la industria reconocidos mundialmente (p. ej., la ISO[2], el NIST[3] y la GSMA[4]) para fomentar la coherencia transfronteriza y así permitir que los operadores implementen protecciones eficientes en costos en todas sus operaciones internacionales. El uso de estándares mundiales como base permite que las políticas se adapten a los contextos nacionales y, a su vez, mantengan una alineación con los principios reconocidos internacionalmente: las divergencias deberían ser una excepción y tener una justificación clara.

La regulación basada en riesgos y centrada en resultados es más efectiva que las normas formalistas

Las medidas efectivas de ciberseguridad deberían abordar riesgos reales en lugar de imponer obligaciones generales para todos, ya que, de no hacerlo, podrían ser desproporcionadas en relación con el nivel de amenaza o el contexto operativo. Los enfoques formalistas, creados en base a listas de verificación de cumplimiento o instrumentos obligatorios, por lo general, producen ineficiencias, promueven una cultura burocrática y desvían recursos, alejándolos de la mitigación de riesgos reales. Incluso, para los usuarios finales, las normas formalistas pueden disminuir la resiliencia de las redes frente a nuevas amenazas al ralentizar la incorporación de nuevas soluciones de seguridad, lo cual socava tanto la confiabilidad como la variedad de opciones de servicios digitales.

Por el contrario, la regulación basada en riesgos y centrada en resultados garantiza la imposición de obligaciones proporcionadas, destina los recursos adonde más se necesitan y les da a los operadores la flexibilidad para innovar y desplegar las tecnologías y prácticas más eficaces para fortalecer la resiliencia.

La cultura regulatoria debería fomentar la confianza, la colaboración y el intercambio de inteligencia sobre amenazas

La manera en que los reguladores hacen cumplir las normas de ciberseguridad afecta enormemente su efectividad. Una cultura punitiva o centrada en la asignación de culpas erosiona la confianza, desincentiva el intercambio de información y hace que el cumplimiento sea un proceso burocrático enfocado en evitar responsabilidades legales en lugar de reducir riesgos. Los lineamientos poco claros y las sanciones desproporcionadas no hacen más que limitar aún más la colaboración.

Por el contrario, un buen intercambio de inteligencia sobre amenazas sigue siendo clave para prevenir ataques y coordinar respuestas. Las plataformas de inteligencia sobre amenazas a menudo se construyen sobre el principio de reciprocidad: los operadores son más propensos a participar de manera activa y ofrecer información en lugares donde obtienen valor. Sin embargo, en muchas jurisdicciones, las plataformas de inteligencia sobre amenazas no existen o brindan un valor limitado a los operadores móviles, lo cual atenta contra su utilidad.

Un enfoque productivo puede promover la colaboración, la participación y la confianza mutua. Al acudir a operadores mediante grupos de trabajo o consultas públicas, los reguladores crean condiciones para lograr una responsabilidad compartida y una mejora continua. Así, una cultura de aplicación que favorece el aprendizaje y el desarrollo de capacidades en lugar de las sanciones puede mejorar la transparencia, reducir la resistencia y apoyar una implementación más eficaz. Las plataformas seguras y de confianza para intercambiar inteligencia sobre amenazas pueden ampliar estos beneficios permitiendo identificar y divulgar las amenazas con mayor rapidez, lo cual mejoraría la respuesta ante incidentes y crearía condiciones para innovar en soluciones de seguridad que fortalezcan la resiliencia del ecosistema digital en su conjunto.

2 La ISO es la Organización Internacional de Normalización.
3 El NIST es el Instituto Nacional de Estándares y Tecnología de EE. UU.
4 GSMA Cybersecurity Knowledge Base

Las políticas de ciberseguridad deberían promover un enfoque proactivo y de seguridad por diseño a fin de mitigar riesgos

Resulta costoso cumplir con regulaciones de ciberseguridad que son reactivas e impulsadas por incidentes o atención mediática en lugar de una planificación a largo plazo. Un enfoque proactivo para mitigar riesgos, que ponga énfasis en la prevención, la resiliencia y permita la planificación a largo plazo, resulta más efectivo y rentable. Si bien una respuesta reactiva es esencial cuando ocurre un incidente, las mejores prácticas añaden a eso un enfoque proactivo y de seguridad por diseño, basado en normas claras centradas en resultados, que permiten cierto grado de flexibilidad en la implementación. Entonces, se requiere una mitigación de riesgos temprana, para además acompañar una inversión sistémica en mejoras de resiliencia.

Una capacidad institucional sólida es importante para lograr una seguridad eficaz

Ni siquiera los marcos de ciberseguridad mejor diseñados pueden tener éxito sin instituciones fuertes que los implementen y supervisen. Una capacidad regulatoria y gubernamental débil —ya sea por falta de presupuesto, de conocimiento técnico o de mandatos claros— socava la aplicación de las normas, reduce la credibilidad y debilita la disuasión de la ciberdelincuencia, generando incertidumbre.

Los operadores necesitan obligaciones claras y agencias con suficientes recursos, personal experto y herramientas modernas que tengan la capacidad de interactuar exitosamente con las partes interesadas. La presencia de instituciones fuertes e independientes asegura una aplicación más coherente de las políticas, aumenta la confianza con los operadores y crea un entorno estable que ofrece una protección más confiable para los usuarios finales.

Seis principios de mejores prácticas para las políticas de ciberseguridad

En este informe, se exponen seis principios centrales que legisladores y reguladores deberían tener en cuenta a la hora de diseñar políticas de ciberseguridad. Si se aplican con coherencia, estos minimizan los costos innecesarios para los operadores, y les dan la posibilidad de encauzar sus esfuerzos y atención en los verdaderos riesgos y en cómo mitigarlos. Estos principios aplican a todos los países. Aquellos que tengan marcos digitales más nuevos pueden beneficiarse aplicandolos como guía en el desarrollo de las políticas digitales, garantizando así que a medida que las politicas evolucionen, estas den soporte a los operadores móviles.

En los países con marcos digitales más avanzados, los principios ayudarán a los formuladores de políticas públicas a consolidar y perfeccionar las normas existentes, para que la labor de los operadores se centre en hacer frente a las amenazas y proteger a los usuarios finales.

Los seis principios de mejores prácticas en políticas de ciberseguridad son los siguientes:

- **Armonización:** alinear las políticas de ciberseguridad con los estándares internacionales siempre que sea posible para reducir la fragmentación y la incoherencia regulatoria.
- **Coherencia**: garantizar que las nuevas políticas y marcos sean coherentes con las políticas existentes para evitar duplicaciones o conflictos.
- **Con base en riesgos y resultados:** adoptar enfoques basados en riesgos y resultados en el diseño y la implementación de la regulación de ciberseguridad, dándoles a los operadores la flexibilidad para innovar y desplegar soluciones eficaces.
- **Colaboración:** promover una cultura regulatoria colaborativa con la industria, respaldada por el intercambio seguro de inteligencia sobre amenazas para fortalecer la resiliencia, aumentar la conciencia sobre las mismas, fomentar un entorno constructivo y promover un enfoque conjunto para luchar contra la ciberdelincuencia.
- **Seguridad por diseño:** fomentar un enfoque proactivo y de seguridad por diseño para la mitigación de riesgos cibernéticos.
- **Desarrollo de capacidades:** fortalecer la capacidad institucional de las autoridades de ciberseguridad para garantizar un enfoque integral desde el Gobierno y una aplicación efectiva de las políticas y las regulaciones.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
gsma.com