tigo MILLICOM
THE DIGITAL LIFESTYLE

2020

Informe del Grupo Millicom sobre divulgación a las autoridades judiciales (LED)

Creemos en lo mejor.
Creemos en tigo

Lo que contiene este informe

Contenido

1. Introducción

El informe sobre divulgación a las autoridades judiciales (Law Enforcement Disclosure, LED) de Millicom de 2020 resume el alcance y el contexto de nuestras interacciones con las agencias y gobiernos a cargo del cumplimiento de la ley en relación con cuestiones que afectan la privacidad o la libertad de expresión de nuestros clientes.

En un año de desafíos y oportunidades sin precedentes, la privacidad y la libertad de expresión siguen siendo los temas más importantes y relevantes para las empresas que brindan servicios de comunicación. La pandemia de la COVID-19 causó una gran alteración en el contexto de un entorno tecnológico que ya cambiaba rápidamente. Mientras los gobiernos luchaban por contener el brote del virus en sus países, muchos buscaron en la tecnología un medio para controlar y mitigar sus efectos. En todo el mundo ha surgido una proliferación de aplicaciones de rastreo de contactos y soluciones de salud digital, algunas de las cuales han suscitado inquietudes sobre la privacidad y la vigilancia. Millicom se ha mantenido firme en nuestro enfoque con los gobiernos y siempre está dispuesto a brindar apoyo crucial donde sea necesario, sin nunca comprometer nuestros principios y valores en lo que respecta a la privacidad y los derechos de libertad de expresión.

Desde el 2015, Millicom ha producido el informe LED anual que va de la mano con nuestro deseo de ser lo más transparentes posible con nuestros clientes sobre cómo manejamos solicitudes gubernamentales sobre sus datos, los desafíos que enfrentamos cada cierto tiempo al hacer acuerdos ante una solicitud gubernamental y la manera en que manejamos esos desafíos. En este informe también establecemos nuestro compromiso y progreso continuos en las áreas de privacidad y libertad de expresión, cómo nuestras operaciones pueden afectar los derechos humanos en general y cómo trabajamos de forma independiente y con los demás para minimizar posibles impactos negativos. Emitimos este informe en inglés y español, en vista de que nuestro negocio se enfoca principalmente en América Latina.

Nuestro éxito empresarial se basa en la confianza de los clientes en cuanto al respeto a su privacidad y libertad de expresión, lo que también va de la mano con nuestro deber de respetar las normas internacionales, así como las leyes locales en los países donde operamos. Es por ello que, en 2013, Millicom se convirtió en miembro fundador del Diálogo de la Industria de las Telecomunicaciones (Telecommunications Industry Dialogue, TID), un grupo de operadores de telecomunicaciones centrado en asuntos relacionados con la privacidad y la libertad de expresión. Desde entonces, el TID se ha fusionado con la Iniciativa de Red Global (Global Network Initiative, GNI), que comprende más de 60 organizaciones miembros, incluidas empresas de tecnología, inversores éticos, académicos y organizaciones de derechos humanos. Millicom busca continuamente aprovechar su participación en la GNI para apoyar la libertad de expresión y los derechos de privacidad en nuestros países de operación. La GNI evaluó positivamente el desarrollo de Millicom en esta área en 2019, lo que marcó la primera vez que se evaluó a una empresa de telecomunicaciones como parte de la GNI. Los detalles sobre nuestra experiencia de evaluación se incluyen en nuestro informe de LED de 2019.

Un panorama tecnológico en constante evolución crea mayores desafíos para nuestro sector, los gobiernos y las autoridades judiciales de todo el mundo. Cada vez más, los legisladores y reguladores

están lidiando con hallar la mejor manera de regular el discurso de odio, eliminar el contenido extremista y evitar las campañas de desinformación, al tiempo que preservan la libertad de expresión. El fenómeno de las "noticias falsas" o las campañas de desinformación a través de las redes sociales, que crean impactos tangibles en los eventos electorales, es solo un ejemplo de los desafíos que emanan de una sociedad centrada en los datos. Las agencias de seguridad presionan de manera continua a los gobiernos para que impongan mayores obligaciones de seguridad pública a las empresas de tecnología. Los métodos y procedimientos convencionales establecidos para solicitar información relacionada con investigaciones penales se están quedando en el pasado.

Además, a medida que avanzamos hacia un futuro aún más conectado, nuestros valores en lo que respecta a la gobernanza de Internet seguirán siendo cruciales para nuestras sociedades y vidas. Las nuevas tecnologías, como la red 5G, continuarán llevándonos a una sociedad más conectada y permitirán el desarrollo masivo de aplicaciones de próxima generación, como la realidad aumentada (augmented reality, AR), la robótica y ciudades inteligentes. A medida que nuestras vidas se digitalizan cada vez más y la mejora de la conectividad impulsa una mayor convergencia de sectores y tecnologías, debemos trabajar a la par con los legisladores, los reguladores, la industria y la sociedad civil, para asegurarnos de encontrar el equilibrio adecuado en las respuestas a las grandes preguntas que nos esperan.

Debemos equilibrar nuestro respeto por los derechos de los clientes con nuestro deber de cumplir con las leyes locales en los países donde operamos. Estas leyes nos obligan a divulgar información sobre nuestros clientes a agencias a cargo del cumplimiento de la ley y a otras autoridades gubernamentales en relación con su deber legítimo de proteger la seguridad nacional y la seguridad pública, o para prevenir o investigar delitos como los actos de terrorismo. Cuando nos enfrentamos a una solicitud de un gobierno para obtener información del cliente, buscamos minimizar el impacto de esa solicitud en el derecho a la privacidad y a la libertad de expresión de nuestros clientes. Antes de responder a cualquier solicitud legal, determinamos que hemos recibido el tipo correcto de solicitud según la ley aplicable para el tipo de información solicitada. Además, cuando surge un conflicto entre la ley local y la Declaración Universal de los Derechos Humanos u otras normas internacionales de derechos humanos, nos esforzamos por resolver ese conflicto de manera que respete el derecho a la privacidad y a la libertad de expresión de las personas, así como su derecho fundamental del acceso a Internet y a servicios de comunicaciones.

Estudiamos e implementamos continuamente las lecciones aprendidas a través de nuestros colegas en la industria y la participación de las partes interesadas. Esperamos que esta edición de nuestro informe LED contribuya al trabajo constructivo entre los diferentes grupos de partes interesadas para proteger mejor la libertad de expresión y la privacidad de nuestros usuarios.

Luxemburgo, febrero de 2021

Karim Lesina
Vicepresidente Ejecutivo y Director de Asuntos Externos

Salvador Escalón
Vicepresidente Ejecutivo y Director de Asuntos Jurídicos y de Cumplimiento.

2. Informes de Millicom

Millicom es un proveedor líder de servicios de cable y móviles dedicado a mercados emergentes. Operamos con la marca Tigo en nueve países de América Latina y en Tanzania. También mantenemos presencia en Ghana, tras haber decidido en 2017 fusionar las operaciones de Tigo en el país con las de Bharti Airtel. Nuestra compañía marca la pauta al ofrecer The Digital Lifestyle® a más de 50 millones de clientes a través de nuestros servicios innovadores y de banda ancha de alta velocidad. Nuestro propósito es construir las autopistas digitales que conectan personas, mejoran la calidad de vida y fomentan el desarrollo de nuestras comunidades. Y nuestra misión es proporcionar las autopistas digitales más rápidas y seguras para convertirnos en la primera opción de los clientes en todos nuestros mercados. Las acciones de Millicom se cotizan en la bolsa de valores de Estocolmo (Nasdaq Stockholm) como recibos de depósito suecos y en el mercado de valores Nasdaq en Estados Unidos desde el 9 de enero de 2019.

Hemos publicado un informe LED anual desde 2015 por dos motivos principales:

1. Para informar de manera más transparente a las partes interesadas sobre cómo manejamos las solicitudes gubernamentales
2. Para explicar de forma más clara los contextos en los que las empresas de telecomunicaciones reciben solicitudes de los gobiernos y las consideraciones que influyen en las decisiones en relación con estas situaciones

Como operador enfocado exclusivamente en mercados emergentes, nos esforzamos por encontrar el equilibrio adecuado entre proporcionar altos niveles de transparencia, cumplir con las leyes aplicables y proteger a nuestro personal y nuestros activos en el terreno. En algunos de los mercados donde operamos, la ley nos prohíbe divulgar las solicitudes de ayuda de las autoridades judiciales. En otros casos, la divulgación puede poner en riesgo la seguridad de nuestro personal y nuestros activos. Con estas consideraciones en mente, subdividimos nuestros informes en dos regiones, América Central y América del Sur, para proporcionar información más detallada y minuciosa. Dada nuestra presencia reducida en África, donde ahora operamos solo en Tanzania y Ghana, este informe LED solo cubre acontecimientos importantes[1] y solicitudes relacionados con la COVID-19 en la región de África.

Sobre qué estamos informando

Damos a conocer el tipo y la cantidad de solicitudes que recibimos de las autoridades judiciales. Más importante aún, también describimos el contexto general y las tendencias reflejadas en las solicitudes que recibimos. En casos específicos y significativos, lo que llamamos acontecimientos importantes, el contexto sirve para resaltar los desafíos prácticos que encontramos en nuestras interacciones con las autoridades judiciales.

Describimos varios de estos acontecimientos importantes y, siempre que sea posible, revelamos los países en los que se desarrollaron.

Divulgamos información acerca de políticas, procesos y controles internos que protegen la privacidad de nuestros clientes cuando manejamos solicitudes de las autoridades judiciales. Este informe también describe cómo buscamos minimizar los efectos injustificados en la libertad de expresión y la privacidad de nuestros clientes.

Además, incluimos información sobre los diversos servicios de comunicaciones que brindamos, así como la cantidad de clientes y nuestra posición en el mercado en cada país. Estos detalles afectan la cantidad de solicitudes que recibimos y se deben tener en cuenta al evaluar el alcance de las actividades gubernamentales.

Sobre qué no estamos informando

En su mayor parte, este informe describe nuestro compromiso en términos amplios en lugar de detallar acontecimientos específicos. Las solicitudes de las autoridades judiciales son de carácter delicado. En muchos casos, se relacionan con procedimientos judiciales confidenciales y con situaciones de seguridad nacional y de emergencia en las que la vida humana está en peligro.

Las solicitudes de las autoridades judiciales vienen acompañadas de estrictos requisitos de confidencialidad. A menudo, la ley nos prohíbe revelar detalles acerca de las solicitudes que recibimos.

El incumplimiento de estos requisitos puede generar sanciones graves para nuestra empresa y nuestro personal local, incluida la detención.

Tenemos una capacidad limitada para discutir públicamente sobre cómo nos relacionamos con las agencias a cargo del cumplimiento de la ley o con otras autoridades cuando recibimos solicitudes, o las formas en que cuestionamos su enfoque. Hacerlo afectaría nuestra capacidad de comprometernos con esas autoridades en el futuro y, en algunos casos, podría poner en riesgo al personal. A veces, estas limitaciones son una causa de frustración, ya que pueden llevar a percepciones incorrectas de inacción de nuestra parte.

A diferencia de algunos de nuestros colegas, que tienen un área geográfica de operación diferente, no revelamos el número de solicitudes gubernamentales por país. Una razón importante para no hacerlo es que varios de los países donde operamos prohíben dicha divulgación. En

[1] Los acontecimientos importantes incluyen, entre otros, las solicitudes con motivos políticos claros como cortes de servicios de nuestra red, denegación o restricción de servicio, eliminación o bloqueo dirigido de contenido, denegación de acceso para personas específicas con la intención de limitar la libertad de expresión, cambios operativos significativos relacionados con las técnicas de vigilancia, cambios significativos en leyes locales relacionadas con poderes gubernamentales de vigilancia o retención de datos o solicitudes para enviar mensajes con motivaciones políticas a los clientes en nombre del gobierno.

cambio, dividimos América Latina en América Central y América del Sur, lo que permite mayores detalles en las cifras. Por lo general, la ley no es clara con respecto a si podemos publicar el número de solicitudes recibidas o si se prohíbe explícitamente la publicación.

Hemos realizado un análisis considerable de riesgos internos y un debate sobre la publicación de cifras específicas de cada país. Operamos en algunos países donde la divulgación pública de dichas cifras puede poner en riesgo la seguridad de nuestros empleados. Esto no es necesariamente un riesgo de acción del gobierno; podría provenir de entidades delictivas a las que hacen referencia las solicitudes. En algunos países, incluso iniciar conversaciones con las autoridades con respecto a la divulgación de las cifras, según nuestra evaluación de riesgo/beneficio, podría generar resultados negativos para nuestras operaciones y nuestra capacidad de promover prácticas más respetuosas de los derechos.

En informes anteriores, divulgamos información específica relacionada con una de nuestras operaciones para proporcionar datos a un nivel más detallado. Esa sección ha sido reemplazada en el informe de este año por dos razones: este país (Colombia) ahora está produciendo esta información en su propio informe de transparencia local, y en su lugar hemos incluido una sección específica sobre el tema más pertinente de la COVID-19.

Hemos trabajado con nuestros colegas anteriores del TID y con el bufete de abogados Hogan Lovells para crear un recurso de marcos legales (https://globalnetworkinitiative.org/policy-issues/legal-frameworks/) que detalla los poderes de vigilancia gubernamentales en nuestros mercados. Por esta razón, no describimos leyes específicas por país en este informe.

Definiciones de solicitudes

La industria de la información, comunicación y tecnología (ICT) no tiene definiciones ni clasificaciones acordadas de las solicitudes de las autoridades judiciales. La creación de definiciones estándar es un desafío, dadas las múltiples jurisdicciones y modelos de negocio en nuestro sector más amplio. En Millicom, clasificamos las solicitudes de las autoridades judiciales en tres categorías: interceptación, metadatos de clientes y datos financieros de clientes (relacionados con los servicios de dinero móvil o servicios financieros móviles [Mobile Financial Services, MFS] que proporcionamos). Algunos de nuestros colegas de la industria presentan informes en categorías similares.

Estas tres categorías abarcan la gran mayoría de las solicitudes que recibimos. Informamos todas las demás solicitudes que permanecen fuera de las definiciones que figuran a continuación, como acontecimientos importantes. No informamos específicamente sobre solicitudes de retiro de contenido, ya que son poco frecuentes en nuestros mercados, con la excepción de la eliminación por mandato legal del acceso a contenido de abuso sexual infantil. Sin embargo, hemos visto un aumento de propuestas legislativas para ordenar o solicitar la eliminación de contenido ilegal en línea en los últimos años. Este contenido a menudo no está bajo nuestro control y solo puede ser eliminado por el proveedor de contenido. Cuando corresponda, contabilizamos las solicitudes de eliminación de contenido en la sección Acontecimientos importantes de este informe.

Cómo obtenemos el material sobre el que presentamos informes

La información sobre el número de solicitudes que recibimos de las autoridades judiciales nos la envían los departamentos legales y regulatorios en cada una de nuestras operaciones locales. Como se indica en nuestras **Directrices sobre acontecimientos importantes y asistencia a autoridades judiciales,** estos departamentos reciben todas las solicitudes y revisan su legalidad antes de ejecutarlas.

Nuestros departamentos registran cada solicitud por fecha, tipo (ver tabla 1) y autoridad solicitante. Una vez que una solicitud está legalmente justificada, proporcionamos la información a las autoridades o emprendemos las acciones necesarias.

La información sobre interceptación, metadatos y solicitudes relacionadas con

dinero móvil se recopila durante nuestro proceso anual de informes de responsabilidad corporativa a través de

Enablon, una herramienta dedicada en la que los equipos jurídicos locales ingresan las cifras totales de solicitudes, así como evidencia de sus cifras totales.

Presentamos la información relacionada con los acontecimientos importantes de conformidad con un mecanismo escalado definido en nuestras **Directrices sobre acontecimientos importantes y asistencia a autoridades judiciales.**

El equipo de Asuntos Externos Globales mantiene un registro de información sobre todos los acontecimientos importantes que se revisan en nuestro Comité multidisciplinario de LED, compuesto por personal de alto nivel de Asuntos Externos. Este incluye las funciones de responsabilidad corporativa, seguridad, asuntos jurídicos, ética y cumplimiento. Los servicios de certificación y verificación de ERM (ERM Certification and Verification Services, ERM CVS) han evaluado la información numérica de Millicom relacionada con las solicitudes de autoridades judiciales como parte de nuestro proceso de aseguramiento limitado de informes de responsabilidad corporativa, como se revela en las páginas 28 a 60 de nuestro informe anual.

Comentarios

Estamos interesados en escuchar las opiniones o trabajar con quien quiera promover el acceso abierto y procesos transparentes y responsables de vigilancia y seguridad. También agradecemos los comentarios sobre este informe o acerca de cuestiones de privacidad y libertad de expresión en general. Comuníquese con CR@millicom.com o encuentre nuestros datos completos de contacto en www.millicom.com.

Tabla 1
Categorías de solicitud

Interceptación	Interceptación de voz, mensajes de texto (short message service, SMS), fax y tráfico de datos (interceptación legal) en tiempo real; es decir, vigilancia en vivo.
Metadatos de clientes	Metadatos como registros de datos de llamadas, direcciones de protocolos de Internet (Internet Protocol, IP), SMS, tráfico de correo electrónico e información sobre el tráfico de Internet, documentos de servicios en la nube y solicitudes de información de localización (estación física/base o información de satélite de posicionamiento global [global positioning satellite, GPS]).
Datos relacionados con servicios de dinero móvil	Información relacionada con nuestros servicios financieros móviles (MFS), como datos de transacciones, confirmación de que una persona es un cliente de dinero móvil y otra actividad de la cuenta. Estas solicitudes no siempre se relacionan con un delito financiero.

3. Nuestra gobernanza y compromiso

Hace tiempo que reconocemos la necesidad de involucrar a la sociedad civil, las ONG, los inversores, los clientes, los académicos y los expertos en la materia, en los asuntos sobre la privacidad y la libertad de expresión, para mejorar nuestra comprensión de los riesgos de derechos humanos relacionados con nuestras operaciones, y promulgar procesos para gestionar esos riesgos.

Nuestras acciones para minimizar los riesgos, en la medida de lo posible, incluyen monitorear la efectividad de las directrices de Millicom, agregar controles y mejorar la preparación de los equipos locales y globales para manejar todos los acontecimientos importantes, así como los asuntos de derechos humanos y reputación que plantean dichos acontecimientos. Inicialmente, nos enfocamos en mejorar procesos locales al brindar apoyo a la administración local y a los equipos que manejan las relaciones con las autoridades judiciales. Desde entonces, hemos progresado significativamente, inculcado una cultura de respeto por la privacidad y los derechos de libertad de expresión en todo nuestro negocio y actuado como líder de pensamiento en los mercados emergentes en estos temas.

En 2018, comenzamos nuestro primer proceso externo de evaluación de la GNI (analizado con más detalle en nuestro informe de LED de 2019). También revisamos y reforzamos continuamente nuestro marco de políticas existente, creado en 2015, y realizamos actualizaciones en línea con los avances tecnológicos, las nuevas normas y las mejores prácticas; y la evolución de los entornos políticos y de seguridad en nuestras operaciones. Por último, nuestra **Política de privacidad global** aborda los derechos de privacidad de los clientes.

Impacto y riesgos sobre los derechos humanos

En 2017, el primer año de nuestra membresía en la GNI, llevamos a cabo una evaluación global de los riesgos de derechos humanos en nuestro entorno operativo para medir el nivel de riesgo de acontecimientos importantes o de otras solicitudes que puedan representar una amenaza para los derechos de nuestros clientes. Derivamos los riesgos destacados y materiales planteados por cada país a partir de los índices de riesgo de Verisk Maplecroft.[2]

Como parte de esta evaluación de riesgos, contratamos el apoyo de expertos externos para evaluar todas nuestras políticas, prácticas y recursos con el fin de comprender mejor nuestros riesgos potenciales y nuestras oportunidades para mejorar.

La importante presencia de Millicom en el área en nuestros mercados nos brinda una comprensión sólida de las situaciones de riesgo potencial y de los niveles de riesgo. Intentamos formalizar esta evaluación y ampliar nuestro análisis a través de la interacción con grupos de partes interesadas externas e internas para crear una herramienta dinámica que pudiéramos actualizar y consultar regularmente. En el 2018, trabajamos con la empresa líder en sustentabilidad Business for Social Responsibility (BSR) para crear un conjunto de herramientas de evaluación de impacto en los derechos humanos (Human Rights Impact Assessment, HRIA), que implementamos en nuestras operaciones en América del Sur en 2019. Continuamos implementando esta evaluación en nuestras operaciones en América Central y hemos incluido un resumen ejecutivo de los resultados de América del Sur en este informe.

BSR también nos apoyó en nuestra evaluación de materialidad más reciente, al convocar entrevistas internas y externas con las partes interesadas para ayudar a definir las prioridades de Millicom en el espacio de responsabilidad corporativa. Naturalmente, la privacidad y la libertad de expresión fueron áreas de enfoque claves durante esta evaluación.

Gobernanza y vigilancia de los derechos humanos

La responsabilidad corporativa es una función central dentro de nuestro equipo de Asuntos Externos. La Junta Directiva (Board of Directors, BoD) de Millicom y nuestro Equipo Ejecutivo (Executive Team, ET), que incluye al Vicepresidente Ejecutivo de Asuntos Externos, supervisan nuestra estrategia y actividades de responsabilidad corporativa. La Junta recibe actualizaciones periódicas sobre temas de responsabilidad corporativa, y el Director Ejecutivo, el Vicepresidente Ejecutivo de Asuntos Externos y el Vicepresidente de Cumplimiento y Asuntos Jurídicos de Millicom asisten a las reuniones de la Junta Directiva. El Vicepresidente Ejecutivo de Asuntos Externos también informa al Equipo Ejecutivo de manera mensual, mientras que el Director de Responsabilidad Corporativa de Millicom es responsable de la gestión continua de los asuntos de derechos humanos en la empresa.

Nuestra Junta Directiva recibe actualizaciones periódicas sobre asuntos de derechos humanos y ha ordenado a la administración que continúe con su firme enfoque proactivo, lo que incluye la profundización de las relaciones con la sociedad civil a nivel nacional y global. Durante el 2019 y el 2020, la Junta Directiva recibió, de parte del Vicepresidente Ejecutivo de Asuntos Externos de la empresa, actualizaciones sobre la implementación por parte de Millicom de los principios de la GNI y nuestra gestión de riesgos relacionados con la privacidad y la libertad de expresión. El Comité de Cumplimiento y Conducta Empresarial de la Junta Directiva brindó supervisión adicional.

En enero de 2014, cuando Millicom comenzó su proceso de escalado para solicitudes gubernamentales, establecimos un Comité de Divulgación a las Autoridades Judiciales (Comité LED) interdisciplinario

[2] https://maplecroft.com

para coordinar mejor la gestión de riesgos. Este comité está presidido por el Vicepresidente Ejecutivo de Asuntos Externos. Incluye al Director de Responsabilidad Corporativa, Vicepresidente de Asuntos Jurídicos y de Cumplimiento, Vicepresidente Ejecutivo de Ética y Cumplimiento, Director de Seguridad de la Información, Vicepresidente de Asesoría Jurídica Corporativa General y Director de Privacidad Global y a nuestros Directores de Asuntos Regulativos. Los miembros del Comité de LED preparan y aprueban conjuntamente las políticas y procesos, revisan nuestras **Directrices sobre acontecimientos importantes y asistencia a autoridades judiciales** y los riesgos relacionados, y aprueban los informes y el compromiso de Millicom relacionados con la privacidad y la libertad de expresión. El Comité de LED se comunica con frecuencia y se reunió en varias ocasiones en 2020 para revisar los riesgos y las acciones relacionadas con la libertad de expresión y la privacidad. Estas reuniones brindaron una oportunidad para informar a los nuevos miembros del equipo sobre nuestro trabajo en curso respecto a estos temas, así como para ayudar a evaluar y definir los "acontecimientos importantes" en nuestros mercados. Este Comité también proporciona orientación e información sobre la manera en la que Millicom puede abordar mejor estos asuntos de forma respetuosa de los derechos y apegada a la ley.

Completamos nuestro marco de **Política de privacidad global** en 2018 y continuamos ejecutándolo durante 2019-20. Además, hemos aprobado amplios principios de privacidad, directrices y compromisos para la empresa. A nivel global, nuestra Oficina de Privacidad está dirigida por nuestro Director de Privacidad Global. A nivel local, todas las operaciones de Tigo tienen un Director de Privacidad Local responsable de la administración de asuntos de privacidad y capacitación local. Nuestros sitios web de Millicom y Tigo brindan información a nuestros clientes sobre nuestra **Política de privacidad global** y los Avisos de Privacidad de Tigo, incluida la forma en que usamos, procesamos y protegemos los datos del cliente. Nuestros sitios web también ofrecen canales y puntos de contacto para que nuestros clientes planteen inquietudes sobre nuestra política o su privacidad.

Nuestro Vicepresidente Ejecutivo de Asuntos Externos, Vicepresidente de Ética y Cumplimiento, Vicepresidente de Información y Tecnología, Vicepresidente de Asuntos Jurídicos y Cumplimiento, Vicepresidente de Asesoría Jurídica Corporativa General y Director de Privacidad Global supervisan los esfuerzos de desarrollo del marco de privacidad. Continuamos implementando este marco de forma interna y externa junto con los compromisos de privacidad y los Principios Rectores de Millicom. Toda la información relevante está disponible en nuestra política de privacidad en línea en http://www.millicom.com/privacy-policy/.

Compromiso

Trabajamos con una amplia gama de actores para mitigar riesgos e impactos en los derechos humanos relacionados con las solicitudes de las autoridades judiciales.

Millicom es un miembro fundador del grupo de Diálogo de la Industria de las Telecomunicaciones sobre Libertad de Expresión y Privacidad; nos unimos a la Iniciativa de Red Global (GNI) como miembro de pleno derecho en 2017. También nos comprometemos con muchas organizaciones internacionales al participar en varios eventos y contribuir con el debate en curso sobre libertad de expresión y privacidad, en el contexto de un panorama tecnológico que cambia rápidamente. Desarrollamos y ampliamos nuestras relaciones con actores de la sociedad civil a través de nuestra membresía en la GNI durante 2020, al participar en su Comité de Políticas y el Comité de Aprendizaje para promover intereses mutuos en defensa de la libertad de expresión y los derechos de privacidad. Además, nos comprometemos tanto como sea posible con los gobiernos y otras partes interesadas de los países, en temas de privacidad y libertad de expresión. En 2020, nos comprometimos ampliamente con las ONG de Nicaragua, Panamá, Paraguay y Colombia en relación con la evaluación de nuestra política y prácticas de privacidad. Buscamos mejorar el entendimiento de los gobiernos sobre nuestras obligaciones fuera de sus países. También buscamos resaltar los riesgos de una actuación gubernamental desproporcionada, especialmente para la reputación de los gobiernos y las posibilidades de inversión extranjera, y discutimos estos temas con representantes diplomáticos relevantes.

llevamos a cabo conversaciones y capacitaciones similares con los miembros de nuestro personal local que se involucran con estos temas en el área.

Un entorno tecnológico que cambia rápidamente y las altas demandas de seguridad pública pueden complicar nuestro proceso de toma de decisiones a medida que nos esforzamos por cumplir con las obligaciones legales y proteger la libertad de expresión y la privacidad de los usuarios. Brindamos capacitación presencial anual sobre estos temas con nuestro personal local en las cumbres regionales, así como a través de sesiones de capacitación específicas en diferentes operaciones según sea necesario.

Políticas, directrices y controles

Nuestro compromiso con la Carta Internacional de Derechos Humanos y los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos se incluye en el **Código de Conducta de Millicom**.

Además, estamos comprometidos a implementar los Principios sobre libertad de expresión y privacidad del TID para el sector de las telecomunicaciones, con base en nuestra membresía en el TID. Los informes LED de Millicom comenzaron como una contabilidad pública de nuestro compromiso. Ahora nos adherimos a los principios de la GNI sobre libertad de expresión y privacidad, e informamos con mayor amplitud sobre estos compromisos después de nuestro primer proceso de evaluación de la GNI.

Durante 2018, el Comité de LED finalizó y aprobó las actualizaciones de las **Directrices del Grupo Millicom sobre acontecimientos importantes y asistencia a autoridades judiciales (Law Enforcement Assistance, LEA)**, que comprenden una versión racionalizada y consolidada de nuestras diversas políticas internas y trabajo en esta área. Estas directrices resumen:

- Nuestras obligaciones dentro de los estándares y marcos internacionales
- Funciones y responsabilidades de cada departamento

- Evaluaciones a realizar a medida que se reciben las solicitudes
- Cómo manejar solicitudes urgentes y no escritas
- Cómo registrar las solicitudes y nuestras respuestas
- Cómo proteger los datos del cliente durante todo el proceso de recuperación de información
- Cómo entregar la información de manera segura

Una versión abreviada de estas directrices está disponible en https://www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf.

Revisamos y modificamos estas directrices de forma continua. También capacitamos constantemente a nuestro personal en implementación y desarrollo.

El Vicepresidente Ejecutivo de Asuntos Externos y el Vicepresidente de Asuntos Jurídicos y de Cumplimiento, que trabajan con los miembros principales de los equipos de Responsabilidad Corporativa y Jurídica, Ética y Cumplimiento, son los responsables finales de la implementación de los principios de la GNI por parte de la empresa, en relación con los derechos de privacidad y libertad de expresión.

Nuestro **proceso de control interno** evalúa el grado de aplicación y cumplimiento de las diferentes políticas y controles globales por parte de nuestras operaciones locales. En 2015, agregamos dos controles relacionados con la implementación de las Directrices de LEA originales. El primer control verifica que todas las solicitudes sean evaluadas por el equipo jurídico antes de la ejecución y que se conserve en los archivos una copia escrita de la solicitud original. El segundo control se relaciona con limitar y hacer un registro de acceso a los datos del cliente al ejecutar la solicitud. Nuestras operaciones evalúan su alineación o nivel de madurez de forma anual, con estos controles. Todas las operaciones han logrado mejoras sustanciales en el nivel de madurez de sus controles de las directrices LEA desde 2015.

El Comité LED aprobó las **Directrices sobre acontecimientos importantes** en 2015. Estas directrices definen los pasos a seguir en caso de un acontecimiento importante, incluido un proceso de escalado a nivel regional y global, así como sugerencias prácticas para establecer relaciones con las autoridades gubernamentales para limitar la responsabilidad o el plazo de un acontecimiento importante. En 2020, nos basamos en trabajos anteriores para evaluar cómo racionalizar la comunicación de estas políticas, directrices y controles internos a nuestro personal local.

Después de realizar una evaluación comparativa externa de cómo se hace esto en la industria y de decidir crear un documento autoritario, las **Directrices sobre acontecimientos importantes y asistencia a autoridades judiciales**, discutimos y revisamos la naturaleza evolutiva de las solicitudes y la posible necesidad de actualizar nuestras definiciones y directrices, para reflejar estas evoluciones.

Hacemos esto para garantizar que nuestros recursos internos se entiendan fácilmente y para que sigan siendo relevantes en un entorno de constante evolución. Capacitamos a los miembros del personal sobre estos temas regularmente. Esperamos finalizar actualizaciones menores de nuestro marco de políticas durante 2021.

Seguridad de la información

Millicom, al igual que todas las operaciones de Tigo, protege nuestras redes y clientes como una de nuestras mayores prioridades. Millicom cuenta con un Director Global de Seguridad de la Información dedicado, cuyo equipo supervisa la estrategia y la dirección de todos los activos relacionados con la seguridad en toda la empresa. Nuestro programa global de seguridad de la información proporciona políticas y estándares, gestión de vulnerabilidades y gestión de riesgos de terceros. El programa también supervisa la implementación de soluciones técnicas en toda la empresa. El Director Global de Seguridad de la Información (Global Chief Information Security Officer, CISO) informa periódicamente sobre iniciativas tecnológicas y riesgos nuevos y en evolución a la Junta Directiva de Millicom. Dado que operamos en muchos países de todo el mundo, es primordial desarrollar un marco de riesgo que pueda abordar las diversas necesidades de informes jurídicos y reglamentarios, así como los desafíos únicos a los que se enfrenta cada país. Millicom ha implementado un marco de riesgo que se basa en una combinación del Marco de Ciberseguridad (Cybersecurity Framework, CSF) del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) y la ISO/IEC 27001:2013. Este enfoque mixto permite a cada país dirigirse a los reguladores locales en el formato que prefieran, a la vez que proporciona una medición común de riesgos y madurez en toda nuestra empresa.

4. Evaluación de impacto en los derechos humanos (HRIA)

Panorama general del proyecto

Millicom trabajó con BSR para realizar evaluaciones de impacto en los derechos humanos (HRIA) de las operaciones de la empresa en Colombia, Bolivia y Paraguay. Buscamos:

- **Identificar y priorizar los impactos reales y potenciales sobre los derechos humanos**, incluidos los riesgos y las oportunidades relacionados con las operaciones, relaciones comerciales, productos y servicios de la empresa
- **Alinear las políticas y prácticas de la empresa con los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos (UN Guiding Principles on Business and Human Rights, UNGP)**, teniendo en cuenta su presencia geográfica, escala y recursos
- **Crear un plan de acción** para abordar los impactos; evitar, prevenir o mitigar los riesgos, y maximizar las oportunidades
- **Desarrollar la capacidad del personal pertinente** para dirigir un diálogo constructivo con los titulares de derechos y las partes interesadas
- **Identificar las mejores prácticas** para la gobernanza y la gestión de los derechos humanos

Resumen de riesgos y oportunidades en materia de derechos humanos

- **Riesgos causados por extralimitaciones gubernamentales y solicitudes excesivas:** el sector de las telecomunicaciones está muy regulado y, a menudo, está sujeto a leyes y condiciones de licencias de espectro que exigen que las autoridades judiciales tengan acceso directo y permitan amplias solicitudes de datos de clientes, que pueden dar lugar a violaciones de los derechos humanos.
- **Riesgos relacionados con las operaciones directas de Millicom:** Millicom también tiene riesgos potenciales en materia de derechos humanos relacionados con sus operaciones. Entre ellos se encuentran los derechos laborales de sus empleados y contratistas, los riesgos para la salud y la seguridad asociados a la construcción y el mantenimiento de las infraestructuras de telecomunicaciones, y las repercusiones sobre los derechos humanos que podrían derivarse de las infracciones éticas y la corrupción.
- **Riesgos causados por el mal uso y el abuso de los servicios de Millicom:** los clientes pueden utilizar los servicios de telecomunicaciones e Internet ofrecidos por Millicom de manera que perjudiquen los derechos de los demás.
- A continuación, se presenta un resumen de los riesgos y oportunidades en materia de derechos humanos identificados en esta HRIA. Los riesgos se desglosan en amplias categorías de derechos. Debido a los contextos similares y a la naturaleza de los servicios de Millicom en Colombia, Paraguay y Bolivia, la mayoría de los riesgos y oportunidades son relevantes para los tres países.
- Es importante señalar que los riesgos para los derechos humanos identificados en esta evaluación son posibles impactos adversos sobre los derechos humanos, que pueden ocurrir en el futuro; esta no es una lista de los impactos adversos reales sobre los derechos humanos, que ocurren en la actualidad. Además, estos riesgos no son exclusivos de Millicom o de los mercados de Colombia, Paraguay y Bolivia; más bien, se encuentran comúnmente en la industria de las telecomunicaciones.
- **Privacidad y seguridad de los datos:** Millicom posee un gran volumen de datos de clientes y, por lo tanto, es importante garantizar que los datos de los usuarios no estén sujetos a un acceso indebido o un uso inadecuado, ya sea por parte de empleados, socios, proveedores o mediante ciberataques de terceros. También es importante abordar los riesgos jurídicos potenciales, como las amplias solicitudes gubernamentales de datos y el abuso gubernamental del acceso directo a las redes móviles.
- **Libertad de expresión y asociación:** como proveedor de servicios de telecomunicaciones e Internet, Millicom es parte de un ecosistema de actores que permite a las personas ejercer sus derechos a la libre expresión, acceso a la información y asociación. Para evitar los riesgos para estos derechos, es importante abordar la posibilidad de que las autoridades gubernamentales ordenen a Millicom eliminar o bloquear el acceso a contenidos legítimos y cerrar parte o la totalidad de su red.
- **Ética y corrupción:** las infracciones éticas y la corrupción pueden afectar o agravar los impactos negativos sobre los derechos humanos al impedir que las personas ejerzan sus derechos. La corrupción y las infracciones también pueden afectar la disponibilidad, calidad y accesibilidad de los servicios y recursos de los que dependen las personas. Los grupos vulnerables que ya tienen opciones limitadas pueden verse especialmente afectados por la corrupción. Millicom tiene sólidas políticas de ética global y es parte de un ecosistema de actores en el mercado. Para hacer su parte, Millicom debe continuar con sus sólidas políticas de ética global.
- **Servicios de seguridad:** Millicom contrata servicios de seguridad para proteger su infraestructura de telecomunicaciones. Es importante garantizar que el personal de seguridad defienda los derechos de seguridad corporal de los demás, si se encuentran con enfrentamientos físicos. Del mismo modo, es importante garantizar que los derechos de seguridad corporal del personal de seguridad estén a su vez salvaguardados de los daños causados por otros. Estos riesgos aumentan en áreas afectadas por conflictos y áreas con altas tasas de criminalidad.
- **Discurso de odio y no discriminación:** estos son riesgos potenciales tanto en las operaciones directas de Millicom como en el uso de los servicios de Millicom por parte de los clientes. Es importante garantizar que las oficinas de los países respeten el código de conducta de los empleados y otras políticas relevantes, así como fomentar una cultura corporativa sólida, para defender el derecho de los empleados a la no discriminación. El discurso de odio y los

contenidos que pretenden acosar a los usuarios son un riesgo de cualquier presencia en las redes sociales.

- **Derechos del niño:** los derechos del niño corren un riesgo especial, debido al uso indebido de las tecnologías de la información y la comunicación (Information and Communication Technologies, ICT). Los niños pueden estar expuestos a contenido inapropiado en línea y las personas pueden utilizar Internet para explotarlos; por ejemplo, compartiendo material sobre abuso sexual infantil. Es importante que Millicom continúe haciendo su parte en la promoción de un entorno en línea seguro para los niños, a través de programas educativos y de divulgación. También es importante proteger los derechos de los niños, al asegurarse de que los proveedores y contratistas no incurran en la explotación de menores u otras prácticas comerciales que puedan perjudicar a los niños.
- **Estándares laborales:** para proteger los derechos laborales tanto de los empleados de Millicom como de los empleados de los proveedores y contratistas, es importante garantizar el cumplimiento de los requisitos de salud y seguridad, evitar que las personas trabajen demasiadas horas y garantizar que los empleados reciban un salario digno, de acuerdo con las leyes y prácticas locales. Millicom y sus proveedores tienen la oportunidad de mejorar los estándares laborales, a través de oportunidades de empleo que brinden un nivel de vida digno.
- **Derechos territoriales y derechos territoriales indígenas:** la infraestructura de Millicom, ya sea propia o arrendada, requiere el uso de terreno y, por lo tanto, es importante garantizar que se respeten los derechos sobre el mismo durante la construcción y el mantenimiento de la red. Esto es especialmente importante para los derechos de territorios históricos de las comunidades indígenas.
- **Uso de las ICT para acceder a la cultura y los servicios públicos:** los servicios de telecomunicaciones e Internet de Millicom permiten a las personas acceder a los servicios públicos y a la educación y ejercer su derecho a participar en la cultura. Es importante continuar apoyando estos derechos al ampliar la cobertura de la red a áreas desatendidas, en la medida en que sea técnica y financieramente viable, al mantener la calidad del servicio y al garantizar que el marketing y las comunicaciones sean inclusivos.

Conclusiones clave

- Los riesgos de derechos humanos más importantes para las operaciones de Millicom en los tres países están relacionados con la privacidad y la seguridad de los datos, la libertad de expresión, la seguridad infantil en línea, y la ética y la corrupción.
- El acceso directo de las agencias a cargo del cumplimiento de la ley a las redes de telecomunicaciones es una preocupación importante en materia de derechos humanos a nivel mundial y está aumentando en América del Sur. Aunque el acceso directo es, a menudo, si no siempre, una condición de las licencias de espectro o de la legislación local, reduce considerablemente la influencia de Millicom para proteger los derechos humanos de los usuarios.
- La tensión política, que puede dar lugar a disturbios sociales, amerita un seguimiento cercano y puede desencadenar la reevaluación de los riesgos relacionados con los derechos humanos.
- Millicom cuenta con políticas sólidas en todas las áreas temáticas, tanto a nivel corporativo como nacional. Estas políticas están diseñadas para prevenir y mitigar los problemas de derechos humanos que se plantean en esta evaluación. Esto se ha documentado en el reciente proceso de evaluación de la GNI de Millicom.
- BSR ha proporcionado varias recomendaciones para mejorar las medidas de mitigación de Millicom para los riesgos de privacidad y libertad de expresión relacionados con la aplicación de la ley. Sin embargo, es imposible mitigar a la perfección todos los riesgos relacionados con los derechos humanos, y una implementación y supervisión sólidas a nivel local resultan particularmente importantes.

Recomendaciones para Millicom

A corto plazo

1. **Colaborar con los gobiernos en las relaciones con las autoridades judiciales, las solicitudes de datos y la vigilancia.** Esto puede llevarse a cabo en colaboración con iniciativas de múltiples partes interesadas. La colaboración debe diseñarse para aumentar la transparencia en las relaciones con las autoridades judiciales y abogar por un enfoque que respete los derechos humanos en las solicitudes de datos y la vigilancia. Esto es particularmente importante dada la creciente tendencia al acceso directo de las autoridades judiciales. La colaboración gubernamental es una de las únicas vías disponibles para que Millicom evite el abuso del acceso directo para una vigilancia inadecuada.
2. **Colaborar con los gobiernos en el bloqueo de contenido, las solicitudes de eliminación y los cortes de Internet.** Millicom ya lo hace para los contenidos de abuso sexual infantil, pero la colaboración podría ampliarse. Esto puede llevarse a cabo en colaboración con iniciativas de múltiples partes interesadas y debe diseñarse para aumentar la transparencia en torno al proceso, para establecer las solicitudes de bloqueo y eliminación de contenidos por parte del gobierno, en la medida en que lo permita la ley.
3. **Ayudar a los agentes gubernamentales a aprender las mejores prácticas.** Emprender un aprendizaje y un diálogo compartidos con los funcionarios del gobierno, los jueces y las agencias a cargo del cumplimiento de la ley sobre las mejores prácticas en materia de libertad de expresión y privacidad. Esto es especialmente importante para hacer frente a posibles abusos de las autoridades judiciales relacionados con el acceso directo.
4. **Reforzar la privacidad y la seguridad de los datos.** Continuar fortaleciendo las políticas y prácticas de seguridad de datos y privacidad de Millicom en relación con las autoridades judiciales, los clientes y los socios, de conformidad con las leyes aplicables.

4. Evaluación de impacto en los derechos humanos (HRIA)—continuado

5. **Seguir reforzando las políticas y prácticas de ética y contra la corrupción.** Abordar cómo se aplican las políticas y las prácticas. Revisar las políticas de manera continua para asegurarse de que estén funcionando y resaltar las áreas que se deben mejorar.
6. **Aplicar las mitigaciones de riesgo de derechos humanos pertinentes en todos los países.** Comparar las medidas de mitigación de riesgos de derechos humanos existentes en todos los países para identificar y aplicar las mejores prácticas.

A medio plazo

7. **Continuar mejorando los procesos y controles de solicitudes gubernamentales.** Esto debe incluir garantizar que los nuevos miembros del equipo estén capacitados adecuadamente en procesos y controles.
8. **Realizar esfuerzos para reducir el riesgo de discriminación en Millicom.** Se recomienda la formación en materia de concienciación sobre la discriminación y los prejuicios inconscientes.
9. **Apoyar los esfuerzos para proteger a los grupos vulnerables.** Promover aún más los enfoques de múltiples partes interesadas para proteger y apoyar a los grupos vulnerables, como los niños, el colectivo LGBTI+, las mujeres y las personas con discapacidad.
10. **Integrar los derechos humanos en la formación existente sobre ética, privacidad y seguridad de los datos.** Esto podría incluir una introducción básica a la empresa y los derechos humanos y un resumen de los compromisos de Millicom en materia de derechos humanos.

A largo plazo

11. **Continuar apoyando el avance de las mujeres en funciones técnicas.** Continuar con los programas que crean una cantera de mujeres en los campos técnicos y apoyan su avance.
12. **Buscar formas de ampliar el acceso a la banda ancha móvil en áreas desatendidas.** Colaborar con los gobiernos nacionales y locales para ampliar el acceso a la banda ancha móvil en zonas remotas y rurales.
13. **Implementar las directrices de publicidad responsable existentes de Millicom con las oficinas locales.** Adaptar las directrices según sea necesario para ajustarse a las normas y reglamentos locales.
14. **Capacitar al personal sobre cómo lidiar con el contenido inapropiado de las cuentas de redes sociales de las operaciones de Millicom en los países.** Esto puede incluir los comentarios publicados en las páginas de redes sociales de Tigo.
15. **Continuar promoviendo el uso seguro de Internet para los niños,** incluso a través de programas como Contigo Conectados y Conéctate Segur@.
16. **Compartir los conocimientos de esta evaluación de impacto sobre los derechos humanos** con las partes interesadas comerciales y no comerciales.
17. **Establecer requisitos con base en los derechos humanos para los proveedores que utilizan servicios de seguridad física para el mantenimiento y la expansión de la red.** Esto debería dar prioridad a los proveedores que operan en entornos difíciles y afectados por conflictos.
18. **Respaldar los estándares sólidos de salud, seguridad y protección y el cumplimiento en la construcción y el mantenimiento de redes** en toda la industria de las telecomunicaciones.

5. América del Sur

Panorama general

Millicom ha operado redes de comunicaciones en América del Sur por más de 25 años. Ofrecemos una amplia gama de servicios, incluidos servicios de datos de alta velocidad, televisión por cable, voz y SMS, servicios financieros móviles (MFS) y soluciones empresariales en tres países de América del Sur. Durante 2020, invertimos un total de 941 millones de dólares estadounidenses en las regiones de América Central y América del Sur, para desarrollar aún más nuestras redes de comunicaciones móviles y fijas. Estas inversiones garantizan un mejor ancho de banda y una mejor calidad de la experiencia en Internet. También permiten construir más servicios e innovación, además del acceso que brindamos.

Mantenemos la posición de mercado más alta en servicios móviles de negocio a consumidor (business-to-consumer, B2C), hogar B2C y MFS en Paraguay, y generalmente estamos clasificados entre los tres principales proveedores de esos servicios en Colombia y Bolivia. Somos un contribuyente importante a nuestros mercados en términos de inversión, impuestos pagados[3] y el empleo y los servicios que brindamos. Para obtener más detalles, consulte las tablas a la derecha.

Tabla 2
América del Sur (Bolivia, Colombia y Paraguay)

Clientes de telefonía móvil totales '000	Relaciones con los clientes[4] '000	Clientes de MFS '000
17.563	2.756	2.389

Tabla 3

País	Clientes de telefonía móvil '000	Fuerza de trabajo[5]	Población[6] '000
Bolivia	3.920	2.716	11.513
Colombia	10.025	3.985	50.339
Paraguay	3.618	5.050	7.044

Marcos jurídicos

En Bolivia y Paraguay existen procesos y requisitos claros para supervisión judicial sobre interceptación y solicitudes de metadatos de los clientes. En Colombia, debido en gran parte a los conflictos internos de larga data y a la guerra contra las drogas, los procesos son significativamente más complejos. Sin embargo, existe supervisión judicial para el inicio de la interceptación.

La información sobre las leyes y procedimientos en Colombia se publica en detalle en https://globalnetworkinitiative.org/policy-issues/legal-frameworks/.

En Bolivia, el uso de la interceptación se limita a circunstancias excepcionales, como el tráfico de drogas y la trata de personas, en las que recibiríamos órdenes judiciales para activar las líneas. Tenemos conversaciones en curso con las autoridades sobre la implementación de técnicas de interceptación.

Los procedimientos en Colombia nos obligan a proporcionar acceso directo a nuestra red móvil a las autoridades. Las auditorías periódicas aseguran que no obtengamos información sobre la interceptación que se está llevando a cabo.

Estamos sujetos a fuertes sanciones, incluidas multas, si las autoridades descubren que hemos obtenido dicha información. Como resultado, no contamos con información con respecto a la frecuencia y durante qué períodos se interceptan las comunicaciones en nuestras redes móviles en Colombia. También tenemos un importante negocio de redes fijas en Colombia; para estas líneas, recibimos órdenes judiciales que revisamos y evaluamos antes de abrir la línea para que se efectúe la interceptación. La duración de la interceptación está limitada por la ley a un máximo de seis meses.

En Paraguay, al igual que en Colombia, las autoridades ordenan que proporcionemos acceso directo a nuestra red móvil. Los procedimientos nos permiten ver la orden judicial requerida para que las autoridades inicien la interceptación, y somos conscientes de cuándo ocurre la misma. Podemos presentar una queja ante la Corte Suprema de Justicia si consideramos que la orden o la interceptación no cumplen con los requisitos legales.

Para las solicitudes de metadatos de los clientes, recibimos pedidos por escrito en los tres países. Evaluamos la legalidad de estas solicitudes antes de proporcionar a las autoridades la información solicitada.

[3] Consulte la página 130 de nuestro informe anual.
[4] Número total de hogares con servicio activo.
[5] La fuerza de trabajo representa empleados contratados directamente por Millicom.
[6] Estadísticas de población según el Banco Mundial (2019).

Solicitudes de las autoridades judiciales en 2020

La tabla 5 muestra una disminución en las solicitudes recibidas por parte de las autoridades judiciales en nuestros mercados en América del Sur. Esto refleja un nivel reducido de actividad criminal y policial debido a los estrictos cierres durante 2020 como resultado de la COVID-19.

Esto se puede ver más claramente en la notable disminución del número de solicitudes de metadatos, el tipo más común de solicitud de aplicación de la ley a las empresas de telecomunicaciones.

Varios países en la región tienen acceso directo a nuestras redes. Dependiendo del tipo de acceso directo en cuestión, esto puede significar que no se nos notifica de todos los casos en los que se intercepta la comunicación del cliente. La solicitud escrita real recibida por una operación cuenta como una solicitud en las tablas de datos. Una solicitud puede buscar información sobre varias personas o dispositivos. Por lo tanto, las solicitudes no son iguales en magnitud.

La gran mayoría de las solicitudes pertenecen a la categoría de metadatos del cliente. La mayoría de estas solicitudes, a su vez, buscan confirmar la identidad que está detrás de números de teléfono específicos. Algunas solicitudes pueden solicitar información acerca de más de uno de los registros de telefonía móvil de un cliente (p. ej., llamadas entrantes y salientes desde el teléfono, ubicación de la torre celular, durante un período específico o dentro de un área geográfica específica).

La cantidad de solicitudes que reciben nuestras operaciones locales también depende de cuántos clientes tengamos y de nuestra posición en el mercado. En América del Sur, el porcentaje de solicitudes de metadatos recibidas por cliente en 2020 fue del 0,110 %, una ligera disminución con respecto a la cifra de 2019.

Tabla 4

	Autoridades que pueden solicitar interceptación o metadatos	Autoridades que pueden emitir órdenes de interceptación
Bolivia	Fiscales, Unidad de Investigaciones Financieras	Autoridades judiciales
Colombia	El ejército, la policía, el fiscal general, los funcionarios públicos con funciones judiciales o de supervisión, el contralor general, el procurador general, los alcaldes y el Instituto Nacional Penitenciario y Carcelario (INPEC)	Oficina del Procurador General y jueces
Paraguay	Oficina de la Fiscalía Pública, tribunales penales	Tribunales penales

Tabla 5

América del Sur	Interceptación	MFS	Metadatos	Solicitudes de metadatos por cliente
2020	749	177	19.333	0,110 %
2019	732	239	24.864	0,157 %
2018	583	190	22.590	0,154 %
2017	38	21	21.492	0,150 %
2016	111	73	22.521	0,103 %
2015	184	104	24.447	0,115 %

6. América Central

Panorama general

Millicom ha operado en la región de América Central por más de 25 años. Ofrecemos una amplia gama de servicios, incluidos datos de alta velocidad, televisión por cable, voz y SMS, servicios financieros móviles (MFS) y soluciones empresariales en seis mercados diferentes. Durante 2020, Millicom invirtió un total de 941 millones de dólares estadounidenses en las regiones de América Central y América del Sur para desarrollar aún más nuestras redes de comunicaciones móviles y fijas. Estas inversiones garantizan un mejor ancho de banda y una mejor calidad de la experiencia en Internet. También permiten construir más servicios e innovación además del acceso que brindamos.

Mantenemos la primera posición de mercado para muchos servicios en toda la región. Además, somos un contribuyente importante a nuestros mercados en términos de inversión, impuestos pagados[7] y el empleo y los servicios que brindamos.

Ahora estamos informando sobre toda nuestra presencia en la región (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá) después de varias adquisiciones en los últimos años. Anteriormente solo habíamos atendido a clientes empresariales, y un número muy pequeño de clientes de televisión por cable y domésticos (Direct-To-Home, DTH) en Nicaragua hasta mediados de 2019, cuando cerramos una transacción para la adquisición de la empresa de telefonía móvil Telefónica en el país. También completamos la adquisición de los activos de Cable Onda y Telefónica en Panamá en diciembre de 2018 y septiembre de 2019, respectivamente. Todos los números relacionados con estas empresas ahora están incluidos por completo en nuestros informes.

Tabla 6
América Central (Costa Rica, El Salvador, Guatemala, Nicaragua, Honduras y Panamá)

Clientes de telefonía móvil totales '000	Relaciones con los clientes[8] '000	Clientes de MFS '000
24.172	1.789	2.556

Tabla 7

País	Clientes de telefonía móvil '000	Fuerza de trabajo[9]	Población[10] '000
Costa Rica	N/A[11]	468	5.047
El Salvador	2.685	622	6.453
Guatemala	11.416	3.201	16.604
Nicaragua	3.493	393	6.545
Honduras	4.620	965	9.746
Panamá	1.957	2.623	4.246

Marcos jurídicos

Debido a los entornos de seguridad desafiantes, que incluyen los altos niveles de crimen organizado y violencia relacionada con el narcotráfico, los gobiernos de América Central han promulgado algunas de las leyes y requisitos técnicos más desarrollados para la vigilancia. En Costa Rica, donde operamos únicamente con redes fijas, el número de solicitudes de las autoridades judiciales es significativamente menor que en otros mercados de América Central.

En Honduras y El Salvador, la ley exige que las autoridades accedan directamente a nuestras redes. Sin embargo, las leyes de ambos países especifican cuáles autoridades pueden solicitar la interceptación y que las órdenes de interceptación solo pueden ser dictadas por los tribunales (ver tabla 8). Como estos son regímenes de acceso directo, no recibimos estas órdenes ni tenemos visibilidad sobre la frecuencia o el período en el que se produce la interceptación. En El Salvador, la ley también enumera los tipos de delitos específicos a los que se puede aplicar la interceptación, además de otros requisitos. En Guatemala y Panamá, la interceptación también se lleva a cabo por órdenes judiciales, que recibimos y revisamos antes de abrir la línea por el período especificado. En Nicaragua, no existe un sistema de interceptación en vivo. Para metadatos de los clientes, se requieren órdenes judiciales de los mismos tribunales en todos nuestros mercados en América Central. Recibimos y revisamos estas solicitudes antes de proporcionar a las autoridades la información solicitada.

[7] Consulte la página 130 de nuestro informe anual.
[8] Número total de hogares con servicio activo.
[9] La fuerza de trabajo representa empleados contratados directamente por Millicom.
[10] Estadísticas de población según el Banco Mundial (2019).
[11] Millicom no tiene operaciones móviles en Costa Rica, pero brinda servicios B2C residencial y B2B, en los cuales es el líder del mercado.

En El Salvador y Honduras, leyes especiales obligan a los operadores de telecomunicaciones a bloquear las señales dentro y fuera de las cárceles. Leyes similares habían existido anteriormente en Guatemala, mientras que Costa Rica recientemente introdujo una legislación en esta área. Consulte la sección 8 para obtener una descripción más amplia del bloqueo de señales en las cárceles de la región.

No se nos compensa por los recursos necesarios para evaluar y procesar las solicitudes de las autoridades judiciales en ninguno de nuestros mercados. Dada la desafiante situación de seguridad en numerosos países de América Central, estos recursos son amplios y deben estar disponibles para responder a las solicitudes en todo momento.

Solicitudes de las autoridades judiciales en 2020

Las autoridades judiciales en todos nuestros mercados en América Central continúan combatiendo el crimen y la violencia en la región. Estos países se encuentran entre los más violentos del mundo. Las notorias pandillas criminales transnacionales involucradas en actividades que van desde contrabando de drogas hasta tráfico de personas son, en gran parte, responsables de la violencia que afecta a estos países. La vigilancia y solicitudes de datos de los clientes respaldan los esfuerzos de las autoridades judiciales para combatir estos graves desafíos de la delincuencia organizada. Las diferencias en las poblaciones de nuestros mercados de América Central y América del Sur contribuyen a dificultar las comparaciones directas de una región a otra. Además, como se mencionó anteriormente, las solicitudes de las autoridades judiciales no son todas iguales en magnitud, lo que complica aún más cualquier intento de hacer comparaciones directas.

Como se muestra en la tabla 9, los tipos de solicitudes han aumentado gradualmente a lo largo de los años. Dicho esto, las adquisiciones recientes dificultan las comparaciones directas con años anteriores. Ciertas solicitudes pueden involucrar una gran cantidad de registros de metadatos, lo que puede sesgar los números. Este año, como en América del Sur, las solicitudes de metadatos cayeron respecto a años anteriores (por las razones antes mencionadas vinculadas al COVID-19) si no fuera por nuestros activos recién adquiridos.

Tabla 8

	Autoridades que pueden solicitar interceptación o metadatos	**Autoridades que pueden emitir órdenes de interceptación**
Costa Rica	Oficina de la Fiscalía, Jueces y Autoridades Fiscales	Jueces en Tribunales Penales
El Salvador	Oficina del Procurador General	Tribunal de Primera Instancia de San Salvador
Guatemala	Oficina de la Fiscalía	Jueces de Primera Instancia en Materia Penal
Honduras	Oficina de la Fiscalía, Procurador General, Oficina Nacional de Investigación e Inteligencia	Tribunal Penal
Nicaragua	Tribunales Penales, Oficina de la Fiscalía, Policía, Oficina de Análisis Financiero, TELCOR	Jueces de Tribunales Penales, Procurador General, Director General de TELCOR
Panamá	Oficina del Procurador General	Rama Judicial

Tabla 9

América Central	Interceptación	MFS	Metadatos	Solicitudes de metadatos por cliente
2020	1.555	323	14.870	0,058 %
2019	1.389	275	12.633	0,072 %
2018	1.533	333	11.278	0,064 %
2017	933	160	10.848	0,060 %
2016	816	194	16.758	0,099 %
2015	0	158	8.653	0,052 %

7. COVID-19

Desde 2017, hemos estado ofreciendo detalles más específicos sobre los tipos y fuentes de solicitudes recibidas en un país no identificado. Desde entonces, este país (Colombia) viene elaborando su propio informe de transparencia con estos detalles. Por lo tanto, ya no replicaremos esta información en nuestro informe LED. Este año, en cambio, hemos decidido incluir una sección específica relacionada con la COVID-19, dada la pertinencia del tema y su correspondiente impacto en nuestro compromiso con la aplicación de la ley.

Tipos de solicitudes relacionadas con la COVID-19

Fuimos testigos de una amplia gama de solicitudes de los gobiernos para ayudar a abordar los desafíos de salud pública relacionados con la COVID-19 (consulte la tabla 10 para obtener más detalles). Entre ellas, las notificaciones automáticas por SMS y el uso de medios y espacios publicitarios para mensajes de salud pública; y solicitudes de apoyo en los esfuerzos relacionados con el rastreo de contactos y la identificación de poblaciones vulnerables para la distribución de fondos de ayuda. Aunque los objetivos y motivos detrás de los últimos tipos de solicitudes posiblemente los hicieron lógicos, pragmáticos y comprensibles, nos vimos obligados a oponernos en circunstancias en las que creíamos que las protecciones para la privacidad y seguridad de nuestros clientes podrían verse socavadas a largo plazo.

No fueron decisiones fáciles, y a menudo nos arriesgamos a dañar las relaciones con nuestras partes interesadas en el gobierno, que buscaban desesperadamente soluciones para hacer frente a una crisis como ninguna otra experimentada en nuestra vida. Ofrecimos nuestros servicios y apoyo de muchas otras formas (por ejemplo, mediante el uso de nuestra plataforma de servicios financieros móviles para distribuir fondos a poblaciones vulnerables), pero no pudimos aceptar entregar nuestra base de datos de clientes a otros gobiernos que necesitaban identificar correctamente qué partes de la población necesitaban esos fondos con mayor urgencia. Esperamos que esta información ayude a proporcionar algunos detalles sobre esta clase de desafíos y mejore la comprensión de los tipos de situaciones que se enfrentan durante esta pandemia. Al igual que nuestra decisión de no publicar los datos a nivel de país para nuestras solicitudes de las autoridades judiciales, hemos optado por mantener esta división a nivel regional para estas solicitudes, dada la sensibilidad de algunos casos. Describimos algunos de estos casos en nuestra sección de Acontecimientos importantes.

Tabla 10

	Notificaciones por SMS	Espacio para medios de comunicación/ publicidad	Solicitudes de geolocalización	Solicitudes de bases de datos de clientes
América Central	86	10	2	1
América del Sur	15	5	3	1
África	4	—	—	—

8. Acontecimientos importantes en 2020

Los acontecimientos importantes son solicitudes que no encajan dentro de los tres tipos de solicitudes de asistencia de las autoridades judiciales cubiertas en las secciones anteriores de este informe. Todas las operaciones locales deben escalar estos eventos a la administración global y tomar medidas para minimizar el efecto de dichos acontecimientos en nuestros servicios y en los derechos de los clientes a la libertad de expresión y la privacidad. Los acontecimientos descritos en esta sección se presentaron en la sede mundial en 2020.

Tomar la decisión de impugnar un acontecimiento importante rara vez es simple. Estas solicitudes a menudo tienen una base legal, aunque los acontecimientos con frecuencia provienen de amplios poderes relacionados con la seguridad nacional.

Los acontecimientos importantes incluyen:

- Solicitudes de cierre de sitios específicos de estaciones base, áreas geográficas o una red completa
- Denegación o restricción del servicio (SMS, Internet móvil o fijo, canales de redes sociales)
- Solicitudes de interceptación fuera del debido proceso
- Bloqueos o retiros de contenidos específicos[12]
- Denegación de acceso a personas determinadas
- Cambios significativos relacionados con técnicas de vigilancia o procesos operativos (cómo se implementan las leyes de vigilancia locales en la práctica)
- Cambios significativos en las leyes locales relacionadas con los poderes gubernamentales de vigilancia o retención de datos
- Solicitudes para enviar mensajes por motivos políticos a clientes en nombre del gobierno

En 2020, registramos 15 acontecimientos importantes, un aumento en comparación con 2019, pero en gran medida acorde al rango observado en años anteriores, como se muestra en la tabla 11. Once de los acontecimientos se produjeron en África, tres en América Central y uno en América del Sur.

Las comparaciones de año a año de nuestros acontecimientos importantes son difíciles, dado que nos hemos desviado de una serie de operaciones en África al tiempo que reorientamos nuestro capital y nuestros esfuerzos en los mercados existentes y nuevos en América Latina. Sin embargo, dada la proporción significativa de acontecimientos importantes en la región de África, hemos optado por incluir esos acontecimientos en esta sección.

Al igual que con las solicitudes de las autoridades judiciales, el sector de las ICT no tiene definiciones aceptadas o estandarizadas para los diferentes tipos de acontecimientos importantes ni cómo contabilizarlos.

Millicom cuenta la cantidad de solicitudes que nos hacen directamente, así como los acontecimientos que tienen consecuencias o implicaciones para nuestros servicios y los derechos de nuestros clientes.

Contamos el acontecimiento independientemente de si nuestro compromiso fue exitoso o no en prevenirlo. Una solicitud puede incluir el corte de varios servicios diferentes o partes de la red en varias zonas geográficas. Si recibimos una solicitud para extender un corte anterior, contamos esto como un nuevo acontecimiento.

Por ejemplo, en el caso de una solicitud para cerrar torres de telefonía móvil alrededor de las cárceles en América Central, contamos una solicitud por país en lugar del número de cárceles o torres de telefonía móvil involucradas. En el caso de cortes en cárceles que estén en curso, sin cambios significativos en términos de obligaciones o requisitos, no lo contamos como un acontecimiento adicional. Para 2020, no registramos acontecimientos importantes en esta área. Si bien no informamos sobre el bloqueo continuo de señales en cárceles (o nuevas medidas de bloqueo que no afectan directamente nuestro negocio) como un acontecimiento importante, consideramos que este es un asunto significativo y continuamos brindando detalles sobre sus implicaciones y nuestro trabajo para mitigar riesgos y amenazas a la libertad de expresión.

Tenemos directrices claras para nuestras subsidiarias sobre el manejo de acontecimientos importantes, además de escalar la información al equipo global para obtener asistencia. Para algunos de los acontecimientos a continuación, no podemos describir cómo reducimos el impacto de esos eventos en la privacidad o en la libertad de expresión de nuestros clientes. Sin embargo, hemos compartido dicha información en diferentes foros de múltiples partes interesadas, como la GNI.

Tabla 11
Tipo de acontecimiento importante

	2015	2016	2017	2018	2019	2020
Corte o restricción de servicios	8	8	2	7	8	8
Propuesta de cambios significativos en leyes locales	3	5	4	5	1	2
Propuesta de cambios significativos en procedimientos técnicos u operativos	3	2	1	2	1	0
Solicitudes desproporcionadas de datos de clientes o interceptación	2	1	2	2	0	3
Mensajes con motivos políticos	2	1	0	1	0	0
Otros	2	1	5	3	0	2
TOTAL	**20**	**18**	**14**	**20**	**10**	**15**

[12] Con la excepción del bloqueo de contenido de abuso sexual infantil.

Cortes o restricciones de servicios

Cuando recibimos solicitudes de cortes o de restricción de servicios, debemos considerar las consecuencias directas para nuestra operación y gestión local, si se aplican sanciones definidas por la ley. Las sanciones pueden incluir multas, encarcelamiento o revocación de una licencia para operar redes de comunicaciones.

Las solicitudes de cortes o restricciones de servicios se producen durante un momento particularmente volátil, lo que significa que también debemos considerar la seguridad de nuestro personal, así como las posibles represalias del público en general contra nuestra empresa y nuestros activos visibles, como tiendas y estaciones base.

África

Aunque no hemos recibido ninguna orden de corte de Internet en África, seguimos ocupándonos de la eliminación de contenidos. En la medida de lo posible, siempre hemos revisado y analizado cuidadosamente las solicitudes de eliminación que no están relacionadas con el contenido de abuso sexual infantil. Constantemente hemos marcado tales acontecimientos y los hemos enviado a través de nuestro sólido proceso de escalamiento. Esto demuestra cuán seriamente nuestro personal se adhiere a las directrices internas de Millicom.

Durante un año electoral delicado en Tanzania, experimentamos una serie de solicitudes extraordinarias de las autoridades. Como se informó ampliamente en la prensa,[13] varios servicios fueron bloqueados o regulados en el periodo previo a la votación y cesaron varios días después de que se anunciaran los resultados de las elecciones. Muchos de estos servicios no son de nuestra competencia, y las autoridades suelen poder actuar con independencia de las empresas de telecomunicaciones en este ámbito.

Aviso de cortes de servicio a los clientes

En nuestros mercados, los servicios móviles son principalmente de prepago y nuestros clientes interactúan con una gran base de distribución que consta de emprendedores individuales y pequeñas tiendas de conveniencia. Nos reunimos con nuestra fuerza de ventas diariamente para informarles de nuevas promociones, productos u otros asuntos relevantes. Esto nos permite transmitir mensajes a los clientes a través de nuestra fuerza de ventas, incluso cuando nuestros servicios se ven afectados.

En el caso de una interrupción del servicio ordenada por el gobierno, hacemos todo lo posible para notificar a clientes que estamos enfrentando una situación fuera de nuestro control. En la mayoría de los casos, nuestros clientes saben por qué los servicios no están disponibles.

Corte continuo de servicios en cárceles en América Central

Desde 2014, las autoridades de El Salvador y Honduras han promulgado leyes que obligan a todos los operadores de telecomunicaciones a cortar los servicios o a reducir la capacidad de la señal en las cárceles y sus alrededores, cuando las autoridades sospechan que bandas criminales siguen operando mediante el uso de teléfonos celulares de contrabando. Guatemala promulgó leyes similares en 2014, pero la legislación pertinente fue anulada en la Corte Suprema en 2015. Costa Rica también introdujo nuevas medidas de bloqueo de señal en 2018, pero no tenemos operaciones móviles en el país. Hemos ayudado con el trabajo de supervisión y defensa realizado por organizaciones como GSMA y ASIET, y continuaremos trabajando con estas organizaciones en estos temas.

En América Central, donde las cárceles a menudo se encuentran en áreas urbanas, acciones como quitar antenas, cerrar torres de estaciones base e instalar bloqueadores de señales pueden afectar el servicio móvil para las personas que viven cerca de las instalaciones correccionales. Por ejemplo, el uso del cajero automático puede verse interrumpido. Las sanciones por incumplimiento de estas órdenes legales incluyen multas sustanciales y la posible revocación de licencias.

Continuamos colaborando con las autoridades locales y colegas de la industria para encontrar formas alternativas de abordar el bloqueo de señales en las cárceles y sus alrededores, que no afecten a los residentes cercanos. Estas alternativas incluyen nuevos diseños de cobertura de red alrededor de las cárceles, soluciones de terceros que bloquean las señales en áreas físicas específicas y la reubicación de las cárceles a áreas menos densamente pobladas.

Millicom se sometió a una evaluación externa de nuestro caso de estudio sobre el bloqueo de la señal de las cárceles en la región de América Central, como parte del proceso de evaluación de la GNI. El Informe de Evaluación Pública de la GNI incluye una descripción de este caso de estudio.

El Salvador

El Salvador aprobó una Ley contra la extorsión en abril de 2015, que prohíbe cualquier señal de telecomunicaciones dentro de una cárcel. Esta legislación establece multas diarias de hasta 900.000 dólares estadounidenses por incumplimiento y autorizó al gobierno a revocar la licencia de cualquier operador de telecomunicaciones que reciba cinco multas dentro de un año.

Cuando la violencia en el país alcanzó su punto máximo a principios de 2016, el Congreso Nacional aprobó una ley que permitía al gobierno tomar medidas específicas y drásticas relacionadas con al menos siete cárceles, si los operadores de telecomunicaciones no bloqueaban sus señales en las cercanías. En el 2018, la Comisión de Seguridad de la Asamblea Legislativa reformó la "Ley Penitenciaria" para hacer del bloqueo de señal un mecanismo permanente. Debido a esta legislación, Millicom y otros operadores tuvieron que cerrar torres de estaciones base, no solo cerca de las cárceles, sino también en las áreas circundantes, dejando a una parte de la población sin servicio. Desde entonces, nuestra empresa ha reducido el alcance de nuestras medidas de bloqueo para ayudar a mitigar los impactos en la libertad de expresión de los clientes cercanos.

Inmediatamente después de que el gobierno aplicó estas medidas extraordinarias, les informamos a nuestros clientes sobre los cierres y sus posibles implicaciones en nuestros servicios y les explicamos que estamos obligados a cumplir con las medidas relacionadas con los esfuerzos de seguridad nacional.

[13] https://qz.com/africa/1923616/tanzanias-magufuli-blocks-twitter-facebook-sms-on-election-eve/

Los operadores de telecomunicaciones en El Salvador continúan trabajando con las nuevas autoridades gubernamentales, que cambiaron en junio de 2019 cuando el presidente Bukele asumió el cargo, para reducir y minimizar los impactos en el servicio. Se ha establecido un grupo de trabajo conjunto con las autoridades para supervisar el progreso y el funcionamiento de los bloqueadores en las cárceles. Los operadores también están donando equipos adicionales para monitorear y ubicar dispositivos dentro de las cárceles.

Honduras

En enero de 2014, el Congreso Nacional de Honduras aprobó una ley que obliga a los operadores a bloquear cualquier señal de telecomunicaciones que llegue a las cárceles del país.

La sanción por incumplimiento es de aproximadamente 420.000 dólares estadounidenses para la primera instancia y aproximadamente 840.000 dólares estadounidenses para la segunda, mientras que una tercera infracción puede resultar en la terminación de la licencia. En 2014, los operadores apagaron varias antenas para cumplir con la ley, dejando a algunos usuarios en las grandes ciudades sin servicio. Los operadores aún no han encontrado una solución de bloqueo que limite los efectos en las personas que se encuentran fuera las cárceles, pero tampoco permita que los guardias de la cárcel apaguen los bloqueadores.

En 2016, tuvimos que ampliar el bloqueo de la señal a otras tres cárceles y mejorar la eficacia de los bloqueadores instalados anteriormente. La Comisión Nacional de Telecomunicaciones (CONATEL), el regulador de telecomunicaciones hondureño, envió una notificación por escrito acerca de un proceso de sanciones después de realizar pruebas en una de las cárceles, en la que se había detectado una señal que permitía realizar llamadas salientes. En enero de 2017, tanto Tigo como el otro gran operador del país, Claro, recibieron sanciones por llamadas salientes. Todavía estamos disputando esta sanción en los tribunales. La situación se ha mantenido prácticamente igual durante los últimos años.

Solicitudes desproporcionadas de datos de clientes o interceptación

Como se describe en la sección anterior sobre solicitudes por la COVID-19, experimentamos algunas solicitudes extraordinarias relacionadas con los esfuerzos para abordar la crisis de salud pública. Estas incluyeron solicitudes de ciertos gobiernos para acceder a nuestras bases de datos de clientes, con el fin de comprender mejor a sus poblaciones y distribuir los fondos de ayuda de manera más efectiva. En Colombia, todos los operadores importantes recibieron una solicitud como esta del Departamento Administrativo Nacional de Estadística (DANE), la agencia de estadísticas del gobierno, a través de la Cámara de Telecomunicaciones local Asomovil.

Enviamos una carta al DANE como Asomovil, GSMA, y por separado como TIGO, describiendo nuestras razones para no cumplir con esta solicitud. Estas incluyeron preocupaciones de privacidad y la falta de jurisdicción legal del DANE para solicitar los datos. El DANE respondió reiterando la necesidad de cumplir, pero nos mantuvimos firmes en no brindar esta información.

Propuestas de cambios significativos en procedimientos operativos o en leyes locales

Las leyes locales prohíben estrictamente a Millicom revelar detalles de los cambios propuestos en los procedimientos de aplicación de la ley, tales como los cambios en los procedimientos operativos de asistencia a las autoridades judiciales. Estos procedimientos definen cómo se implementan en la práctica las leyes locales con respecto a dicha asistencia y detallan cómo se realizan y se manejan las solicitudes diarias de las autoridades judiciales.

Los reguladores y legisladores continúan analizando los marcos legales locales y los procedimientos operativos en muchos de nuestros mercados actuales. Partiendo de una tendencia anterior, los principales acontecimientos que registramos durante 2020 involucraron un nuevo proyecto de ley de delitos informáticos en Nicaragua y regulaciones de contenido en Tanzania.

Nos comprometemos con las autoridades locales para desarrollar leyes a través de un proceso abierto y consultivo. Nuestra solicitud más frecuente a los legisladores es que establezcan supervisión judicial, promuevan medidas proporcionadas y necesarias, y sean lo más específicos, claros y detallados posible con respecto a qué autoridades pueden realizar solicitudes conforme a la ley y cómo la ley nos exige que respondamos. A menudo encontramos que los legisladores tienen dificultades para comprender los roles y las limitaciones de los diferentes actores en el ecosistema de las ICT. Como resultado, los legisladores a menudo imponen requisitos a las empresas de telecomunicaciones que solo pueden ser realizados por proveedores de servicios específicos.

Tampoco estamos de acuerdo en que los operadores de telecomunicaciones deban asumir el costo de implementar medidas técnicas y operativas para la interceptación, como proponen con frecuencia los gobiernos. En nuestra opinión, compartir estos costos ayudará a fomentar el uso proporcional de tales poderes.

Nicaragua

A fines de 2020, la asamblea nacional controlada por el Frente Sandinista de Liberación Nacional (FSLN) aprobó una ley que hace que la difusión de noticias falsas a través de "tecnologías de la información y la comunicación" sea punible con hasta cuatro años de prisión.

Sigue a otros proyectos de ley, como la "ley de agentes extranjeros" y la "ley de cadena perpetua", así como las medidas contra varios medios de comunicación.

La ley Ciberdelitos tiene el objetivo declarado de "brindar un marco legal para la prevención, investigación, enjuiciamiento y sanción de los delitos cometidos a través de las tecnologías de la información y la comunicación". Según el proyecto de ley, las personas condenadas por delitos como fraude, ciberespionaje o uso de Internet para corromper a menores, o por pornografía infantil, se enfrentarían a penas de dos a 10 años de prisión.

La disposición que ha atraído una cobertura mediática significativa es el Artículo 30, que permitiría condenas de dos a cuatro años por "la publicación o difusión de información falsa (o) distorsionada que produzca alarma, miedo o angustia entre el público".

Tanzania

En julio, el gobierno publicó nuevas reglamentaciones sobre contenidos en línea que se aplica a los proveedores de servicios de contenidos en línea, los proveedores de servicios de Internet, los titulares de licencias de servicios de aplicaciones, los usuarios de contenidos en línea y cualquier otro contenido en línea relacionado. Las reglamentaciones incluyen normas generales que cubren:

- Categorías de licencia
- Procedimiento de solicitud de licencia
- Obligaciones de los proveedores de servicios de contenido en línea
- Usuarios y anfitriones de contenido en línea
- Contenido prohibido
- Quejas y sanciones

Las obligaciones generales para los titulares de licencias incluyen, entre otras:

- Obligación de utilizar herramientas de moderación para filtrar los contenidos prohibidos, identificar el origen de los mismos y tomar medidas correctivas
- Al recibir la orden de la Autoridad Reguladora de las Comunicaciones de Tanzania (Tanzania Communications Regulatory Authority, TCRA), la obligación de eliminar de inmediato el contenido prohibido (en el caso de que la TCRA decida solicitar la eliminación en lugar de realizar la eliminación por sí misma)
- Obligación de abstenerse de acceder, almacenar, conservar, publicar, circular o difundir cualquier contenido prohibido

9. Tendencias y prioridades para el 2021

Tendencias en nuestro entorno operativo

Como se señaló anteriormente, la cantidad de acontecimientos importantes en nuestros mercados aumentó en 2020. Los cambios significativos en nuestro negocio en los últimos años, como salir y consolidar varias operaciones en África mientras nos expandimos en América Latina, dificultan el análisis de tendencias de año en año. Continuamos experimentando una gran mayoría de acontecimientos importantes en la región de África durante 2020, impulsados por un año electoral polémico. Permanecemos atentos a los numerosos problemas de seguridad y desafíos políticos en los países donde operamos. Seguimos trabajando con las autoridades locales para mejorar la transparencia y la rendición de cuentas, así como para educar a las autoridades sobre la necesidad de una actuación proporcionada.

Continuaron surgiendo nuevos marcos relacionados con la regulación del contenido y el delito cibernético, tendencias destacadas en nuestros informes de LED anteriores. Es probable que estos tipos de eventos aumenten a medida que los gobiernos busquen comprender cómo las nuevas tecnologías pueden ayudarlos en sus esfuerzos de seguridad nacional.

Desafortunadamente, a veces vemos propuestas legislativas copiadas directamente de otras jurisdicciones, sin una consulta adecuada en un foro de múltiples partes interesadas. A través de nuestro trabajo con la GNI pretendemos demostrar que este tipo de interacción, con todos los actores que trabajan en soluciones conjuntas, es la manera más efectiva de comprender y satisfacer demandas y deseos, tanto de la población como de los gobiernos.

Los cortes en las cárceles siguen siendo un desafío importante en la región de América Central. Aunque no tuvimos acontecimientos importantes relacionados con este tema en los últimos años, las medidas de bloqueo de señal en América Central continúan siendo un foco para los esfuerzos de defensa de la industria, con nuevas medidas en discusión ahora también en Panamá.

Nuestro objetivo es redoblar nuestros esfuerzos con otras partes interesadas de la sociedad civil, para seguir llamando la atención internacional sobre los problemas de bloqueo de señales. Hemos discutido este tema y compartido las mejores prácticas con nuestros colegas de la industria en varias ocasiones. También hemos continuado nuestro trabajo sobre este tema como un área de enfoque de políticas para la GNI, y nos sentimos alentados por el potencial de este grupo para ayudar a abordar el problema. Millicom apoyó a la GNI en su trabajo para producir una guía de una página para legisladores y funcionarios del gobierno, con el fin de garantizar que entiendan completamente las consecuencias de los cortes de la red. La campaña #KeepItOn de Access Now también sigue desempeñando un papel importante al resaltar estos acontecimientos, agregar información sobre los cortes y crear conciencia.

Capacidad de las autoridades judiciales locales

La mayoría de las solicitudes que recibimos fuera del proceso legal establecido tienden a derivarse de la falta de comprensión de las leyes u operaciones técnicas por parte de ciertos funcionarios a cargo del cumplimiento de la ley. En nuestra opinión, algunas autoridades policiales locales también carecen de la capacidad, los recursos y el conocimiento para comprender el ecosistema de las ICT. Este déficit, junto con el acceso inadecuado a los métodos de investigación cibernética más recientes, puede dar lugar a solicitudes que no podemos llevar a cabo o que son desproporcionadas para el problema que las autoridades están tratando de abordar.

Un ejemplo común es cuando las autoridades emiten una solicitud relacionada con contenido que no tenemos, como contenido en servicios de redes sociales como YouTube, WhatsApp o Facebook. Dichos datos se mantienen fuera de la jurisdicción que los solicita, y los complejos tratados de asistencia legal mutua hacen que sea muy difícil para las agencias locales a cargo del cumplimiento de la ley, recuperarlos rápidamente.

Nos reunimos regularmente con agencias a cargo del cumplimiento de la ley con respecto a solicitudes y propuestas desproporcionadas o excesivas, para ayudar a educarlas sobre las complejidades involucradas. Siempre trabajamos para proporcionar las mejores prácticas de otros países en los que hemos negociado garantías en los procesos de interceptación con éxito. Los ejemplos incluyen supervisión independiente, órdenes limitadas y enfocadas solo para fines legítimos, límites de tiempo estrictos y la capacidad de verificar que el individuo o el equipo autorizado correcto estén llevando a cabo la solicitud.

Abogar por leyes claras

Las leyes y los procesos claros relacionados al respeto de la privacidad y la libertad de expresión de nuestros clientes son cruciales para las compañías de telecomunicaciones. Operamos subsidiarias locales que están sujetas a las leyes locales y no tenemos la opción de seleccionar las leyes que cumpliremos. Por lo tanto, abogamos por leyes más claras, que respeten las convenciones internacionales y definan de manera restringida quién, cómo y bajo qué circunstancias se pueden realizar las solicitudes de las autoridades judiciales, incluso cuando pueda llevar más tiempo alcanzar el resultado final deseado. Consideramos que esa claridad es un instrumento central para promover el uso proporcional de los poderes de las autoridades judiciales. Las leyes claras también nos ayudan a evaluar con mayor facilidad la legalidad de las solicitudes, lo que beneficia tanto a la privacidad como a los derechos de libertad de expresión de los ciudadanos. Además, la claridad ayuda a que los procesos de aplicación de la ley

sean más eficientes y nos permite impugnar con éxito las solicitudes que no cumplan con la ley correspondiente.

Agradecemos la asistencia técnica adicional de la comunidad internacional y otras fuentes, mientras nos esforzamos por incluir consideraciones de derechos humanos en las investigaciones cibernéticas. La asistencia de estas partes interesadas también ayuda a diseñar leyes transparentes y claras en torno a la vigilancia que incorporen principios internacionales de derechos humanos.

Prioridades para 2021

Continuaremos nuestros esfuerzos de compromiso con todos los grupos de partes interesadas, en torno a temas de libertad de expresión y privacidad. Además, promoveremos más la orientación interna relacionada al monitorear continuamente la efectividad de nuestras directrices y procedimientos existentes, en relación con la asistencia a las autoridades judiciales. Continuamos revisando y actualizando nuestra guía para las operaciones locales, como las sesiones de capacitación presencial que tuvieron lugar en países específicos a lo largo de 2020. Realizamos dos sesiones de capacitación en Panamá, primero con el nuevo equipo de Cable Onda y luego en una sesión conjunta con los equipos de Cable Onda y Telefónica, que ahora trabajan juntos después de nuestras adquisiciones. También celebramos una sesión similar con empleados nuevos y existentes en Nicaragua, luego de la adquisición de los activos de Telefónica en este país. Asimismo, realizamos una sesión de capacitación con un nuevo miembro de alto nivel del equipo en Bolivia.

Nos tomamos en serio el cumplimiento de nuestros procedimientos internos; en raras ocasiones hemos sancionado a los empleados que no siguieron nuestras directrices y controles. Esto refleja la evolución natural de nuestro proceso de madurez y nuestro robusto marco para proteger la privacidad y la libertad de expresión

Continuamos asistiendo a los principales eventos de la sociedad civil y promoviendo la necesidad de mayores garantías sobre los derechos humanos en ayuda internacional para el desarrollo y asistencia financiera. También continuamos promoviendo la necesidad de un apoyo técnico con base en los derechos humanos para los legisladores y las agencias de cumplimiento de la ley en nuestras regiones. Lo más importante es que continuamos dialogando directamente con las agencias gubernamentales pertinentes siempre que sea posible.

Esperamos aprovechar nuestras interacciones con las múltiples partes interesadas para continuar nuestro importante trabajo en cuestiones de libertad de expresión y privacidad, que siguen estando en la vanguardia de los debates sobre derechos humanos y seguridad en todo el mundo. A través del diálogo entre las distintas partes interesadas, hemos ganado socios para el aprendizaje compartido y hemos recibido comentarios cruciales de asesores expertos sobre la efectividad de nuestras políticas y procesos.

Nuestros puntos focales con los actores externos incluyen ayudar a definir leyes de vigilancia claras, transparentes y efectivas que incorporen garantías adecuadas. A medida que los países continúan revisando su legislación relacionada con la vigilancia y la interceptación, creemos que todos los interesados en esta área necesitan una definición más clara de cómo deben ser las buenas leyes de vigilancia.

Durante 2021, continuaremos implementando las HRIA en operaciones locales seleccionadas. Estamos aprendiendo mucho acerca de nuestros riesgos y oportunidades en las áreas de derechos humanos, libertad de expresión y privacidad a través del proceso de HRIA. Esto ha permitido un mayor intercambio de ideas de las mejores prácticas y estándares entre nuestras operaciones locales.

Por último, hemos puesto en marcha un marco de política de privacidad según la legislación vigente y una plataforma interna para los empleados. También hemos lanzado una sección de privacidad en nuestro sitio web externo, que continuaremos desarrollando para que todos los usuarios puedan consultar todas nuestras políticas y compromisos relacionados con la privacidad junto con materiales relacionados y herramientas interactivas.