

¿QUIÉN DEFIENDE TUS DATOS?

PANAMÁ 2021





Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0):
<https://creativecommons.org/licenses/by-sa/4.0/>

Edición: Migdalia Díaz S.
Diagramación: Juan Pablo Hoyos C.
Coordinación: Abdías Zambrano, Veridiana Alimonti y Lia Hernández
Investigación: Gabriel Cajiga

JUNIO 2022

PANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

IPANDETEC Centroamérica es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

ELECTRONIC FRONTIER FOUNDATION EFF

¿Quién defiende tus datos? Panamá es un proyecto realizado con el apoyo de la Electronic Frontier Foundation (EFF).

¿QUIÉN DEFIENDE TUS DATOS? PANAMÁ 2021.

Desde 2011, la Electronic Frontier Foundation (EFF) empezó a publicar una evaluación anual titulada “Who has your back?” para evaluar las políticas de protección de datos de las principales compañías de telecomunicaciones e Internet en Estados Unidos, con el objetivo de incrementar la protección de los datos personales y la privacidad por parte de las empresas, frente a las solicitudes de información realizadas por el Estado.

Actualmente, la EFF apoya a diversas organizaciones en la región iberoamericana para la realización de proyectos parecidos titulados “¿Quién defiende tus datos?” o ¿Dónde están mis datos? en Argentina, Brasil, Chile, Colombia, México, Nicaragua, Paraguay, Perú y España hasta la fecha.

Durante el desarrollo de este reporte, IPANDETEC, organización sin fines de lucro que promueve el uso y regulación de las Tecnologías de la Información y Comunicación (TIC) y la defensa de los Derechos Humanos en el entorno digital en Centroamérica, como encargada del estudio para Panamá, ha evaluado una serie de criterios que se desarrollarán a continuación con base en la información públicamente disponible en los sitios web de las empresas proveedoras de servicio de telefonía móvil. Se incluyen las políticas de protección de datos, contratos y otra información relevante.

CONTEXTO NACIONAL

Las empresas seleccionadas para esta tercera edición fueron las cuatro actuales operadoras de telefonía móvil en el mercado de telecomunicaciones panameño: Claro, Digicel, Más Móvil y Tigo.

CLARO PANAMÁ: Claro Panamá es una marca de la subsidiaria Claro de la empresa América Móvil SAB de C.V. La marca está en Panamá desde marzo de 2009, convirtiéndose en la cuarta operadora de telefonía móvil en el país hasta el momento. En septiembre del 2021 se anunció que América Móvil firmó un acuerdo con Cable & Wireless Communications Limited, subsidiaria del grupo Liberty Latin America, por la venta del 100% de sus acciones de Claro Panamá. Esta transacción fue demandada por Digicel, pero tanto la Autoridad de Protección al Consumidor (ACODECO) como la Autoridad de los Servicios Públicos (ASEP) aprobaron la venta. Por el momento, Claro Panamá opera de forma independiente, cuenta con líneas fijas y ofrece los servicios de telefonía móvil, internet móvil y fijo y televisión satelital. Durante 2020 lograron modernizar 500 radiobases dotándolas de tecnología LTE.¹

Digicel, cuyo dueño es Digicel (Panamá), S.A., es una filial perteneciente a Digicel Group que opera en la República de Panamá desde el año 2008 ofreciendo servicios de telefonía móvil. En el año 2018 invirtió más de 100 millones de dólares en la incorporación de tecnología LTE Pro y hasta la fecha, Digicel ha invertido 575 millones de dólares. Como consecuencia a la aprobación de la ASEP sobre la venta de Claro Panamá, Digicel solicitó el 6 de abril del 2022 su liquidación voluntaria expresando que dicha fusión hace insostenible que Digicel opere en Panamá además de representar el fin de la libre competencia.² A finales del mismo mes, el Gobierno Nacional comunica que ha tomado el control de Digicel para evitar su liquidación.

Más Móvil es la filial para los servicios de telefonía móvil de la empresa Cable & Wireless Panamá, S.A., fundada en 1997 después de que el Instituto Nacional de Telecomunicaciones (INTEL) vendiera acciones a la empresa privada. Es propiedad conjunta del Estado Panameño que posee el 49% de las acciones de Cable & Wireless Communications Limited, subsidiaria del grupo Liberty Latin América con un 49% de las acciones y de los colaboradores

1. Revista Martes Financiero Panamá, Claro dinamiza la era digital en Panamá y amplía su infraestructura tecnológica, 2022, Disponible en: <https://www.martesfinanciero.com/portada/claro-dinamiza-la-era-digital-en-panama-y-amplia-su-infraestructura-tecnologica/>

2. Revista Martes Financiero Panamá, Digicel solicita al Órgano Judicial liquidación voluntaria para salir del mercado panameño, 2022, Disponible en: <https://www.martesfinanciero.com/actualidad-empresarial/digicel-solicita-al-organo-judicial-liquidacion-voluntaria-para-salir-del-mercado-panameño/>

activos de la empresa con contrato por tiempo indefinido y de los que se hubiesen jubilado a partir del 29 de mayo de 1997, con una participación accionaria del 2% de las acciones de la compañía. Actualmente, cuenta con líneas activas y ofrece servicios de línea fija, móvil, banda ancha, servicios corporativos y televisión pagada. Más Móvil incursionó por primera vez en el mercado panameño en el año 1998, siendo la primera compañía de telefonía móvil en tener 1 millón de líneas activas.

Tigo es una marca de Cable Onda, S.A., afiliada de Millicom International Cellular. El día 29 de agosto de 2019, Millicom International Cellular, a través de su afiliada Cable Onda, S.A., adquirió el 100% de las acciones de Telefónica Móviles Panamá, S.A., la cual se encontraba representada por la marca Movistar. A partir del día 28 de julio de 2020 se formalizó el cambio de razón social de la empresa telefónica Móviles Panamá, S.A. Actualmente, se denomina Grupo de Comunicaciones Digitales S.A., y está representada por la marca Tigo, la cual ha reemplazado a la marca Movistar; cuenta con líneas activas y ofrece servicios de línea móvil y servicios corporativos.

METODOLOGÍA DE EVALUACIÓN

CRITERIOS Y PARÁMETROS

La investigación desde nuestra primera edición en el 2019 se desarrolla con el objeto de analizar y evaluar una serie de criterios con perspectiva de Derechos Humanos. En la primera edición, una de nuestras principales conclusiones fue que “a la industria de las telecomunicaciones le preocupaba poco o muy poco la protección de datos y la privacidad de los usuarios”³, considerando la información disponible en los sitios web de las empresas existentes en el 2019 en Panamá

En nuestra edición del 2020 se revisó más allá de los datos disponibles en sus sitios web y se notó poco avance, teniendo como principal conclusión que “las empresas de telefonía móvil no incluyen políticas de protección integral de los datos personales de sus clientes en el conjunto de su prestación de servicio”.⁴

3. ¿Quién Defiende Tus Datos? Panamá 2019, Disponible en: https://www.ipandetec.org/wp-content/uploads/2019/08/QDTD_Panam%C3%A1_1ra-edici%C3%B3n-2.pdf

4. ¿Quién Defiende Tus Datos? Panamá 2020, Disponible en: https://www.ipandetec.org/wp-content/uploads/2020/11/QDTD_2020.pdf

En esta tercera edición, se ha decidido mantener como base los criterios utilizados en los reportes anteriores considerando que se siguen manteniendo vigentes dentro del catálogo de instrumentos, resoluciones e informes elaborados por organismos regionales e internacionales. No obstante, se ha incluido parámetros nuevos y explicado extensamente otros para aclarar el objetivo de dichos parámetros, impulsar la publicidad del cómo se defiende los datos en las empresas y reflejar la perspectiva de la legislación local.

Como consecuencia, los criterios utilizados en esta edición 2021 del reporte son desarrollados a continuación:

1. POLÍTICA DE PROTECCIÓN DE DATOS

La política de protección de datos se refiere al documento que contiene una declaración—adecuada al marco legal del país—en la que la empresa informa sobre los mecanismos que utiliza para la recolección, utilización, divulgación y gestión de los datos personales de clientes en el conjunto de su prestación de servicio. En Panamá, la Ley No. 81 del 2019 sobre la Protección de Datos Personales, la Constitución Política, la Ley de Acceso a la Información Pública⁵ y la Ley No. 33 de 23 de abril 2013 que crea la Autoridad de Transparencia y Acceso a la Información Pública (ANTAI)⁶ son los textos legales que contienen los principales mecanismos de protección de la privacidad y datos personales de los ciudadanos.

Se destaca en comparación con los reportes anteriores que la Ley de Protección de Datos Personales entró en vigencia en marzo del 2021, después de dos años en vacatio legis y fue reglamentada por el Decreto Ejecutivo 285 del 28 de mayo de 2021.

Esta ley protege los datos personales de todos los panameños y extranjeros, siempre y cuando el tratamiento de datos se realice en el territorio panameño y faculta a la ANTAI, para que con ayuda de la Autoridad para la Innovación Gubernamental (AIG), reglamente la ley y la haga cumplir, convirtiéndola en la autoridad encargada de la protección de datos personales.⁷ La ley define los tipos de datos en Panamá; los actores involucrados en la protección de datos personales; los requisitos para su recolección, tratamiento y transferencia de datos; los derechos que tienen los titulares de los datos; y la responsabilidad legal por infracciones a la ley.

Por su parte, el Decreto Ejecutivo 285 del 28 de mayo de 2021 reglamenta con más detalle los principios generales para el tratamiento de datos mencionados en la Ley 81, la relación de la información entre el titular y responsable del tratamiento, los derechos de los titulares, las condiciones de licitud para el tratamiento, la seguridad de los datos y las medidas y mecanismos para hacer cumplir la ley.

5. Ley No. 6 del 22 de enero de 2002 de Transparencia y Acceso Información Pública, Disponible: <http://www.mef.gob.pa/es/transparencia/Documents/Ley%20No%206%20de%2022%20enero%20de%202002.pdf>

6. Ley No. 33 de 25 de abril de 2013, Que crea la “Autoridad Nacional de Transparencia y Acceso a la Información”. Disponible en: <http://www.antai.gob.pa/wp-content/uploads/2015/04/ley33-25-abril-2013.pdf>

7. Ley No. 81 de 26 de marzo de 2019 “sobre Protección de Datos Personales.” Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/72148.pdf

Sin embargo, existen legislaciones especiales para el tratamiento de datos crediticios, médicos y del sector de las telecomunicaciones, dejando a la Ley de Datos Personales con carácter supletorio para llenar vacíos legales y establecer los mínimos de protección de datos personales. De estas leyes especiales se pueden mencionar:

La Ley No. 51 de 18 de septiembre de 2009⁸, en su artículo 1, 2 y 6, dispone que las empresas de telecomunicaciones, entre otros, deben conservar los datos necesarios para identificar al usuario (datos para rastrear e identificar el origen de la comunicación, para identificar el destino de la comunicación, para determinar fecha, hora y duración de la comunicación, para identificar el tipo de comunicación, para identificar el equipo de comunicación, y para identificar geográficamente el lugar donde se inicia la comunicación) y el tiempo a almacenar los mismos (las empresas de telecomunicaciones están obligadas a conservar los datos por 6 meses, ampliables a 6 meses más, desde el momento en que se generó la comunicación). La Ley No. 13 de 20 de febrero de 2018 que adiciona artículos a la Ley No. 51 de 2009 establece la obligatoriedad de las empresas de telecomunicaciones de registrar los datos de los usuarios prepago.⁹

Ambas leyes mencionadas no hacen mayor mención los derechos que pueda tener un usuario; sin embargo, todo usuario que desee ejercer sus derechos en virtud de la Ley 81 de 2019 debe dirigirse primeramente a la Autoridad de Servicios Públicos (ASEP), ente regulador de empresas de telecomunicaciones y de no obtener respuesta, deberá dirigirse a la ANTAI. Esto fue el criterio planteado en una consulta elevada por el Administrador General de la ASEP hacia la Procuraduría General de la Administración publicada en abril del 2022.¹⁰ Con esta opinión legal se confirma que la Ley 51 del 2009 es la principal de alcance sectorial para empresas de telecomunicación con respecto a la conservación y suministro de datos de los usuarios, mientras que la Ley 81 del 2019 queda con carácter general, desarrollando el núcleo esencial del derecho a la privacidad y, para efectos prácticos, atendiendo reclamos de manera subsidiaria.

La Ley No. 33 del 23 de abril de 2013, que crea la Autoridad Nacional de Transparencia y Acceso a la Información, define los datos personales en su artículo 5, numeral 5, como información confidencial, además de domicilio, número telefónico y correo electrónico personal; a su vez información confidencial se define en el mismo artículo, numeral 11, como “todo tipo de información en manos de agentes del Estado o de cualquiera institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual,

8. Ley No. 51 de 18 de septiembre de 2009, “que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones.” Disponible en: <https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf>

9. Ley No 13 de 20 de febrero de 2018, “que adiciona artículos a la Ley 51 d 2009, que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones.” Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/28469_B/66177.pdf

10. Procuraduría de la Administración, Consulta C-039-22. Disponible en: <http://vocc.procuraduria-admon.gob.pa/content/c-039-22>

correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad”.

También se considera como confidencial la información contenida en los registros individuales o expedientes del personal o de recursos humanos de los funcionarios.

Como consecuencia, en este proyecto se evalúa si las empresas están comprometidas con la privacidad y protección de los datos personales de sus usuarios en la prestación de los servicios, yendo más allá del marco jurídico actual, desarrollando una política de protección de datos transparente en un lenguaje claro y sencillo, además de publicarla en su sitio web en un lugar accesible al público. Se aclara que al hacer referencia a la publicidad de la política de protección de datos en el sitio web, solo se considerarán aquellas que contengan las reglas de protección de datos aplicables a la prestación de los servicios y no a la política de privacidad del sitio web.

Es una buena práctica que facilita a los usuarios entender las condiciones en las que se realiza el tratamiento de sus datos personales. Las políticas deben determinar qué información es recopilada y almacenada, así como el plazo y objeto.

Sobre los derechos de los titulares también conocidos como derechos ARCO, el Decreto Ejecutivo 285 del 2021 los define como “derechos irrenunciables básicos de los titulares de datos personales, e identificados como derechos de acceso, rectificación, cancelación y oposición”. Por tal razón las políticas de protección de datos deben mencionar estos derechos a sus usuarios y los mecanismos claros para que puedan ser ejercidos.

PARÁMETROS

- La política es clara y de fácil acceso a los usuarios.
- La política establece cuáles datos son recopilados.
- La política establece el plazo de retención de los datos de los usuarios.
- La política menciona y explica los derechos ARCO y cómo pueden ser ejercidos.

2. INFORMES DE TRANSPARENCIA

Los informes de transparencia se refieren a la publicación periódica en su sitio web del número de solicitudes de información personal de sus clientes realizadas por autoridades competentes, indicando la cantidad de solicitudes aceptadas y rechazadas, relacionadas a las medidas de conservación y suministro de datos de usuarios de las telecomunicaciones.

Estos reportes o informes de transparencia son cada vez más frecuentes entre las empresas de tecnología y de telecomunicaciones alrededor del mundo, ya que son una buena práctica que están adoptando las empresas que permite que los usuarios conozcan la cantidad y alcance de las solicitudes de datos que realiza el Estado. Las solicitudes de datos pueden ir desde la interceptación telefónica, registro de llamadas, número IP hasta la geolocalización en tiempo real del cliente.

PARÁMETROS

- La empresa pública da informes de transparencia.
- Los informes están fácilmente accesibles a sus usuarios.
- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.

3. NOTIFICACIÓN AL USUARIO

La notificación al usuario consiste en una de las garantías de la protección del derecho a la privacidad. Se refiere a la notificación que se realiza a la persona para informarle que sus comunicaciones o datos sobre la comunicación fueron entregados al Estado, con el tiempo y la información suficiente para que el usuario pueda impugnar la decisión o buscar otras soluciones, mientras no ponga en serio peligro la finalidad para la que se autoriza el acceso a datos.

En un primer análisis, no se encontró ninguna prohibición legal en Panamá para que las empresas notifiquen a sus usuarios sobre pedidos de acceso a datos por autoridades de investigación. La Ley 51 en su artículo 10 dispone que: “los datos conservados y la información suministrada con arreglo a lo dispuesto en esta Ley tienen el carácter de información confidencial y solo podrán ser proveídos de conformidad con lo establecido en la Constitución, la presente Ley y sus reglamentaciones.”

Esta redacción del artículo pudiera invitar a concluir que el usuario no puede ser notificado de una solicitud de entrega de sus datos al Estado porque es confidencial; sin embargo, esta interpretación estricta restringe el derecho a la privacidad y no debiera sostenerse por varias razones.

Primeramente, el artículo citado menciona que son confidenciales “los datos conservados y la información suministrada”. El uso de la conjunción “y” dentro de una interpretación estricta de esta ley significaría que los titulares de los datos no pudieran ejercer sus derechos ARCO sobre los datos conservados porque estos son igualmente confidenciales. Es decir, se estaría yendo en contra de la Constitución de Panamá que en su artículo 42 establece como garantía fundamental el derecho que tiene toda persona a acceder, rectificar y oponerse de su información personal.

Segundo, tanto en la Constitución de Panamá como en el Código Procesal Penal no encontramos una prohibición expresa que impida la notificación al usuario en tiempo, pero sí en contenido. El artículo 29 de la Constitución que esboza un derecho de privacidad no menciona que las solicitudes de información de la autoridad competente con mandato judicial excluyan al titular.¹¹ El artículo 311 del Código Procesal Penal sobre interceptaciones de comunicaciones menciona que, “a quien se le encomiende interceptar y grabar la comunicación o quien la escriba tendrá la obligación de guardar secreto sobre su contenido...”. Este artículo limita a que se conozca el contenido de la comunicación grabada, también para que terceros no la accedan, mas no impide que la empresa pueda dar a conocer al titular que una autoridad competente por mandato judicial ha requerido información suya, especialmente después que la medida ha sido concluida.

Tercero, la ley 51 no prohíbe directamente que el titular sea excluido del conocimiento de la solicitud. La Ley 51 no define el término “confidencial”, de forma que se debe utilizar supletoriamente a la Ley 81 de 2019 para obtener su definición. Esta define los datos confidenciales como: “aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados...”. El titular de los datos no puede ser considerado un tercero o parte del público porque los datos le pertenecen y forman parte de su ser.

Con este breve análisis se considera que las empresas no están impedidas legalmente de notificar en algún momento a un usuario sobre el hecho de que una autoridad de investigación ha solicitado información suya.

PARÁMETROS

- La empresa se compromete a notificar al usuario sobre la información solicitada en el primer momento permitido por ley.

4. AUTORIZACIÓN JUDICIAL

Las normas para acceder a los datos de las comunicaciones deben ser realizadas en el marco de una investigación con las suficientes salvaguardas del debido proceso. El abuso de funcionarios públicos, a cargo de mecanismos de acceso a datos, es un riesgo inminente para los ciudadanos; como consecuencia, las empresas únicamente deben atender las solicitudes de entrega de información personal de sus usuarios emitidas por autoridades competentes.

El artículo 29 de la Constitución Nacional señala que las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial. Al respecto, una Sentencia de la Corte Suprema de Justicia de Panamá deja claro que la autoridad judicial solo son aquellos jueces y encargados de administrar justicia dentro del Órgano Judicial, del cual no forma parte el Ministerio Público ni sus agentes; esto deja claro que se necesita mandato de autoridad judicial para interceptar llamadas telefónicas.¹² De igual forma, la Ley No. 121 de 31 de diciembre de 2013,¹³ que reforma el Código Procesal Penal, en su Sección No.5 explica que solamente el juez de Garantías puede autorizar la interceptación de comunicaciones o incautación de correspondencia, a razón de petición del fiscal de la causa en resolución motivada. El tiempo de interceptación es de 3 meses, prorrogables por el mismo periodo.

A su vez, la Ley No. 51 de 18 de octubre de 2009 dicta las medidas y normas para la conservación, la protección y suministro de datos de las comunicaciones que incluye datos del suscriptor, los metadatos y datos de localización de usuarios de los servicios de telecomunicaciones; en sus artículos 11, 12, 13 y 14 explica que los datos retenidos van a ser suministrados al Ministerio Público o la autoridad judicial para la investigación de delitos, detención y enjuiciamiento de personas vinculadas con la comisión de dichos delitos.

Los datos requeridos también podrán ser solicitados directamente por el Ministerio Público mediante Resolución motivada con base del principio de proporcionalidad y excepcionalidad, la que será luego sujeta de control posterior por la autoridad judicial. El artículo 7 de la Ley 51 aclara que en ningún momento la conservación será del contenido de las comunicaciones.

Con relación a las reglas para el acceso a los datos retenidos, la legislación panameña no cumple con los estándares de independencia e imparcialidad mediante el cual la autoridad que autoriza el acceso a los datos no es separada ni independiente de la autoridad que conduce la investigación.

12. Sentencia del Pleno de la Corte Suprema de Justicia del 28 de enero de 2010. Disponible en: https://vlex.com.pa/vid/solicitud-pleno-suprema-sala-198250047?_ga=2.243494855.370176048.1551118645-1758111339.1550249042

13. Ley No. 121 de 31 de diciembre de 2013, "que reforma el Código Penal, Judicial, Procesal Penal y adopta medidas contra las actividades relacionadas con el delito de delincuencia organizada." Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/27446_B/44985.pdf

PARÁMETROS

- La empresa promete en sus contratos, políticas o términos de servicio a exigir a las autoridades una autorización judicial antes de suministrar el contenido de las comunicaciones de sus clientes.
- La empresa se compromete a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales.

5. DEFENSA DE LOS DERECHOS HUMANOS

Este criterio se refiere a la participación proactiva de las empresas en relación a la promoción y defensa de los derechos humanos de sus usuarios, especialmente los relacionados a la privacidad de las comunicaciones y protección de datos personales. La promoción se puede realizar por medio de campañas publicitarias, participación en discusiones de proyectos legislativos o en foros con enfoque multisectorial sobre tecnologías y derechos humanos.

Las empresas deben expresar su compromiso con el respeto de los derechos de sus usuarios, haciendo incidencia a nivel de legislación y políticas públicas o litigio estratégico para la protección de los derechos humanos a través de posiciones legales pro-privacidad adoptadas. Además, expresar rechazos contra medidas de vigilancia sin las salvaguardas necesarias que pueden afectar la privacidad de sus usuarios, es una acción positiva que genera confianza.

Dado los riesgos de abuso que conlleva la utilización de una facultad de acceso a datos en donde la persona afectada no tiene conocimiento de ello, resulta indispensable la participación previa de un juez que pueda verificar la protección de los intereses de la persona afectada y el cumplimiento de la ley en cada requerimiento.

La Corte Interamericana de Derechos Humanos ha reconocido que los datos que identifican una comunicación, también conocidos como metadatos, se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones privadas y, por tanto, también es necesaria autorización judicial para que una autoridad competente pueda tener acceso.¹⁴ Por ello, como principio, las empresas deberían exigir que las autoridades que le solicitan información presenten una autorización judicial. Lo anterior es exigido además por la Constitución, incluyendo el derecho internacional de los derechos humanos.

14. Ver sentencia de la Corte Interamericana de Derechos Humanos. Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 114. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

Sin embargo, la Ley 51 de 18 de septiembre de 2009: “dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones”, estaría en violación de los estándares internacionales por permitir el suministro de metadatos directamente al Ministerio Público, sin una orden judicial previa. Delante de tal incumplimiento, las empresas podrían iniciar litigio estratégico de ser factible o incidencia en políticas públicas sobre la necesidad de una autorización judicial previa o inmediata cuando les sea solicitado el acceso o la colaboración para obtener los metadatos de las comunicaciones de un usuario.

PARÁMETROS

- La empresa promueve a través de campañas o actividades la importancia de la privacidad y protección de datos de sus usuarios.
- La empresa promueve iniciativas de ley, litigio estratégico, o de políticas públicas para la protección de la privacidad y la protección de datos de sus usuarios.
- La empresa participa en mecanismos o procesos multisectoriales para la promoción de los Derechos Humanos en el marco de sus responsabilidades empresariales.

6. SEGURIDAD DIGITAL

Las empresas poseen sitios web con toda la información relevante sobre los servicios que prestan, incluso una plataforma de pagos en línea, lo cual facilita que los usuarios realicen los pagos correspondientes a los servicios que utilizan. Como consecuencia, es importante analizar el compromiso de las empresas con la seguridad de los datos que sus usuarios ingresan en sus sitios web.

Sin embargo, las brechas de seguridad digital generan que los datos personales de los usuarios sean susceptibles a ataques o incluso robos. El Decreto Ejecutivo 238 de 2021 entiende que una violación de seguridad es cualquier daño, pérdida, alteración, destrucción, acceso o cualquier uso ilícito no autorizado de datos personales que haya ocurrido aun de forma accidental.

Como consecuencia, el compromiso de la empresa en promover e incentivar una cultura de seguridad digital entre sus usuarios es importante. Además, la mitigación de estos ataques o filtraciones de datos conlleva a que una empresa deba tener protocolos para notificar a sus usuarios cuando ha sido vulnerada para minimizar el alcance de la violación de seguridad. El plazo establecido en el mencionado decreto es de setenta y dos horas desde que se tenga conocimiento de la violación de seguridad.

PARÁMETROS

- La empresa utiliza el protocolo HTTPS para navegar en su página web.
- La empresa utiliza el protocolo HTTPS inclusive a la hora de hacer pagos en línea.
- La empresa publica o pone a disposición de sus clientes información o contenidos sobre seguridad digital.
- La empresa mantiene un protocolo para informar a sus usuarios sobre filtraciones de datos.

7. GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD

Importa verificar si las empresas publican guías en las que se establece el procedimiento de colaboración con las autoridades de investigación con detalles sobre los datos que entrega, así como requerimientos legales y requisitos que exige para entregar la información de sus usuarios, teniendo en cuenta el marco legal local.

Se distingue este parámetro 7 del parámetro 2 sobre la publicación de los informes de transparencia, toda vez que aquel parámetro es un informe estadístico, mientras este se refiere a guías que informen públicamente las políticas adoptadas por las empresas frente a solicitudes de información de sus usuarios por las autoridades. Con esto es posible a los usuarios conocer más qué información está disponible para la aplicación de la ley y sus protecciones, de manera que las autoridades mantengan sus solicitudes fundamentadas y específicas.

PARÁMETROS

- La empresa cuenta con una guía para el requerimiento de la información personal de sus clientes por parte de la autoridad que sea públicamente accesible y tenga en cuenta el marco legal local.

PARÁMETROS DE LAS RESPUESTAS

1. POLÍTICA DE PROTECCIÓN DE DATOS

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa cuenta con una política de protección de datos, aplicada a sus servicios de telecomunicaciones, publicada en su sitio web.
- La política es clara y de fácil acceso a los usuarios.
- La política establece cuáles datos son recopilados.
- La política establece el plazo de retención de los datos de los usuarios.
- La política menciona y explica los derechos ARCO y cómo pueden ser ejercidos.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con al menos cuatro de los parámetros de evaluación.
- La empresa obtiene ½ estrella si cumple con al menos tres de los parámetros de evaluación.
- La empresa obtiene ¼ de estrella si cumple con al menos uno de los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

2. INFORMES DE TRANSPARENCIA

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa pública informes de transparencia.
- Los informes están fácilmente accesibles a sus usuarios.
- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.
- La empresa obtiene ½ estrella si cumple al menos con la mitad de los parámetros de evaluación.
- La empresa obtiene ¼ de estrella si cumple con al menos uno de los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

3. NOTIFICACIÓN AL USUARIO

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa se compromete a notificar al usuario sobre la información solicitada en el primer momento permitido por ley.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

4. AUTORIZACIÓN JUDICIAL

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa se compromete en sus contratos, políticas o términos de servicio a exigir a las autoridades una autorización judicial antes de suministrar el contenido de las comunicaciones de sus clientes.
- La empresa se compromete a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.
- La empresa obtiene ½ estrella si cumple con la mitad de los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

5. DEFENSA DE LOS DERECHOS HUMANOS

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa promueve a través de campañas o actividades la importancia de la privacidad y protección de datos de sus usuarios.
- La empresa promueve iniciativas de ley, litigio estratégico, o de políticas públicas para la protección de la privacidad y la protección de datos de sus usuarios.
- La empresa participa en mecanismos o procesos multisectoriales para la promoción de los derechos humanos en el marco de sus responsabilidades empresariales.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.
- La empresa obtiene ½ estrella si cumple con dos de los parámetros de evaluación.
- La empresa obtiene ¼ de estrella si cumple con al menos uno de los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

6. SEGURIDAD DIGITAL

PARÁMETROS

LOS PARÁMETROS EVALUADOS PARA ESE CRITERIO SON:

- La empresa utiliza el protocolo HTTPS para navegar en su página web.
- La empresa utiliza el protocolo HTTPS inclusive a la hora de hacer pagos en línea.
- La empresa pública o pone a disposición de sus clientes información o contenidos sobre seguridad digital.
- La empresa mantiene un protocolo para informar a sus usuarios sobre filtraciones de datos.

EVALUACIÓN

- La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.
- La empresa obtiene ½ estrella si cumple con dos de los parámetros de evaluación.
- La empresa obtiene ¼ de estrella si cumple con al menos uno de los parámetros de evaluación.
- La empresa no obtiene estrella si no cumple con ninguno de los parámetros de evaluación.

EVALUACIÓN DE LAS PRÁCTICAS

EMPRESA EVALUADA: **CLARO PANAMÁ**

1. POLÍTICA DE PROTECCIÓN DE DATOS

- **LA EMPRESA CUENTA CON UNA POLÍTICA DE PROTECCIÓN DE DATOS, APLICADA A SUS SERVICIOS DE TELECOMUNICACIONES, PUBLICADA EN SU SITIO WEB.**

Claro cuenta con una política de privacidad publicada en su [sitio web](#) que después de ser evaluada detenidamente puede interpretarse como aplicada a sus servicios.

La política en su primer párrafo expresa directamente que la empresa se compromete a proteger la privacidad de sus usuarios en las páginas de Claro y a facilitar la tecnología necesaria para que el usuario pueda disfrutar de los servicios de forma segura y eficaz. Seguidamente, la política establece que la misma se aplica a Claro y sus subsidiarias y que contempla la recopilación y tratamiento de datos personales y servicios de dichos sitios. Sin embargo, no resulta claro si la política al referirse por “sitios” quiere entender por sitios web o sitios de las subsidiarias. Igualmente cuando la política se refiere a la recopilación de los datos, esta empieza diciendo que Claro recopila y trata los datos personales en algunos sitios web de Claro.

Por otro lado, lo que lleva a concluir que la política de protección se refiere al servicio es que en la propia sección de recopilación de los datos se incluyen casos en los que Claro recopila y trata datos. Entre esos casos se menciona aquellos datos propios y relacionados con la prestación de servicios de Claro. Adicionalmente, cuando la política hace mención a la finalidad del tratamiento de los datos, esta explica que la finalidad dependerá del: **“Servicio contratado o a contratar, los requerimientos del Usuario y de la interacción del Usuario en las Páginas o sitios web y Apps Claro”** Esta interpretación de la política se reitera a lo largo del texto. Por ejemplo, Claro añade una sección en la que explica que entre las consecuencias de no brindar los datos o revocar el consentimiento para el tratamiento significa que Claro no podrá prestar adecuadamente los servicios requeridos por el usuario.

- **LA POLÍTICA ES CLARA Y DE FÁCIL ACCESO A LOS USUARIOS.**

Se considera que la política no es lo suficientemente clara para que un usuario pueda determinar inmediatamente si la política se refiere a los datos recopilados en el sitio web o si la política además se aplica en todos los productos y/o servicios de Claro. Falta una mayor claridad.

Por otro lado, la política de privacidad es de notorio fácil acceso. El sitio web de Claro posee en la página principal una sección específica llamada “Claro Transparente” y otra “Protección de Datos Personales” que hacen imposible que pase desapercibida por cualquier usuario. De esta forma, se innova y se reta el usual estándar de colocar las políticas de privacidad en la parte inferior del sitio web y en letra pequeña.

A pesar de esta innovación, se considera que la empresa no cumple con el parámetro puesto que no vemos congruente que exista un fácil acceso a una política que no es clara.

- **LA POLÍTICA ESTABLECE CUÁLES DATOS SON RECOPIRADOS**

La política establece claramente siete literales en los que mencionan los datos que se recopilan y el escenario en el que esto ocurre. Especifican que pueden recabar nombre, apellidos, domicilio, correo electrónico, teléfono; cualquier información proporcionada en la relación contractual; la información técnica relativa al acceso y uso de los servicios, así como el número IMEI del equipo; e incluyen la posibilidad de recopilar datos de forma automática del hardware o software del equipo, como la dirección IP y sitios web visitados.

- **LA POLÍTICA ESTABLECE EL PLAZO DE RETENCIÓN DE LOS DATOS DE LOS USUARIOS**

Claro no establece el plazo por el cual retendrá los datos de los usuarios. No obstante, sí especifica que cuando Claro realice gestiones con terceros proveedores de servicios y deba transferirles datos, Claro suscribirá acuerdos para garantizar la eliminación de los datos al finalizar el plazo de prestación del servicio, así como garantizar su protección.

- **LA POLÍTICA MENCIONA Y EXPLICA LOS DERECHOS ARCO Y CÓMO PUEDEN SER EJERCIDOS.**

La política ofrece una sección específica sobre “Derechos del Usuario” en la que menciona que Claro vela por la autodeterminación informativa de sus usuarios, por lo que ellos pueden ejercer sus derechos ARCO (acceso, rectificación, cancelación, oposición y/o portabilidad) a través de diversos canales. Los usuarios pueden acudir en persona a un centro de atención al cliente, enviar mensajes a través de Whatsapp, llamar al Call Center o al teléfono fijo, escribir por Instagram o por correo electrónico.

CALIFICACIÓN: CLARO PANAMÁ RECIBE ½ DE ESTRELLA AL CUMPLIR CON TRES DE LOS CINCO PARÁMETROS..

2. INFORMES DE TRANSPARENCIA

- **LA EMPRESA PUBLICA INFORMES DE TRANSPARENCIA.**

La empresa no publica informes de transparencia directamente en su sitio web. Sin embargo, al momento de hacer la investigación se pudo contar con la colaboración de **Claro Panamá**, quienes indicaron que la empresa, siendo parte del grupo **América Móvil**, facilita información para la confección del Informe de Transparencia de América Móvil encontrado dentro de los [Reportes de Sustentabilidad](#) del grupo publicados en la página web de América Móvil.

Se resalta que, a diferencia de los años anteriores, la edición 2020 del reporte muestra el número de órdenes de autoridad recibidas, requiriendo información de usuarios por región y el número de las que fueron procesadas. El reporte, como se mencionó, ofrece un link que redirige al [Informe de Transparencia en las Comunicaciones 2020](#).

En este informe de transparencia, América Móvil entra a detallar cada región y país en cuanto a la información que deben ofrecer por ley a las autoridades competentes, la legislación aplicable y cuál es la autoridad competente por cada país. **Sin embargo, en ambos los informes los datos estadísticos de solicitudes recibidas por la autoridad están especificados por región, y no por país.** Por parte de la región centroamericana, se reporta que se entregó la información en un 96.7% de las 40,500 solicitadas. Cuando no fueron procesadas, el informe explica que se debió a que no provenían de autoridades competentes o no cumplía con los requisitos establecidos en la ley.

La región centroamericana incluye solicitudes recibidas en Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá. Aunque América Móvil haya avanzado en su compromiso con la transparencia al publicar datos estadísticos de solicitudes recibidas y rechazadas, la empresa debe considerar hacerlo por país en sus futuros informes. Esto es fundamental para brindar la transparencia adecuada a las solicitudes de acceso a datos de los usuarios por parte de autoridades gubernamentales.

- **LOS INFORMES ESTÁN FÁCILMENTE ACCESIBLES A SUS USUARIOS.**

El informe no se encuentra en la página web de **Claro Panamá** y no hay indicaciones sobre cómo encontrarlo. Por tales razones, no es intuitivo para un usuario que el informe de transparencia se encuentre en un link en la página 95 del reporte de sustentabilidad de publicado en la página web de **América Móvil**.

- **LOS INFORMES CONTIENEN DATOS RELACIONADOS AL NÚMERO DE SOLICITUDES RECIBIDAS, CUMPLIDAS Y EL TIPO DE SOLICITUD.**

El reporte de sustentabilidad y el informe de transparencia de las comunicaciones sí contiene el número de solicitudes recibidas y las que fueron cumplidas, pero por región y no por país. Además, no se muestra cuantificada los tipos de solicitud aunque sí se identifican de manera general. Para Panamá, el reporte indica que por ley la empresa está obligada a entregar datos conservados, proveer localización geográfica en tiempo real, intervenir comunicaciones privadas, suspender servicios de telecomunicaciones y bloquear líneas de comunicación que participen en la comisión de delitos.

CALIFICACIÓN: CLARO PANAMÁ RECIBE ½ DE ESTRELLA AL CUMPLIR CON AL MENOS DOS DE LOS TRES PARÁMETROS DE EVALUACIÓN.

3. NOTIFICACIÓN AL USUARIO

- **LA EMPRESA SE COMPROMETE A NOTIFICAR AL USUARIO SOBRE LA INFORMACIÓN SOLICITADA EN EL PRIMER MOMENTO PERMITIDO POR LEY.**

Claro Panamá no mantiene este compromiso con sus usuarios, pero sí aclaran al usuario que no pueden notificar en virtud de la legislación panameña que mandata que la solicitud de información sea confidencial. Se considera que esta interpretación es muy restrictiva por las razones expuestas en la metodología de evaluación.

CALIFICACIÓN: CLARO PANAMÁ LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON EL PARÁMETRO DE EVALUACIÓN.

4. AUTORIZACIÓN JUDICIAL

- **LA EMPRESA PROMETE EN SUS CONTRATOS, POLÍTICAS O TÉRMINOS DE SERVICIO EXIGIR A LAS AUTORIDADES UNA AUTORIZACIÓN JUDICIAL ANTES DE SUMINISTRAR EL CONTENIDO DE LAS COMUNICACIONES DE SUS CLIENTES.**

La empresa en reiteradas ocasiones menciona en su política de transparencia que deberá transmitir la información requerida por autoridades judiciales o administrativas competentes para cumplir con la obligación legal. Este compromiso se refuerza en los informes de sustentabilidad y en especial en los Informes de Transparencia en las Comunicaciones del grupo América Móvil.

Sin embargo, el apartado que detalla el marco legal aplicable en Panamá no remarca el requisito de previa autorización judicial para la intervención de las comunicaciones. El informe describe lo siguiente en cuanto a las autoridades competentes para emitir solicitudes relativas a las comunicaciones de los usuarios: **“Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente.”**¹⁵

La necesidad de previa orden judicial para la interceptación del contenido de las comunicaciones está presente en la Constitución de Panamá y en el Código Procesal Penal. A diferencia de otros marcos legales nacionales mencionados en el informe de transparencia, el apartado de Panamá no especifica esta distinción para la intervención de las comunicaciones.

- **LA EMPRESA SE COMPROMETE A RECHAZAR REQUERIMIENTOS DE ENTREGA DE INFORMACIÓN EN CASOS QUE INCUMPLAN REQUISITOS LEGALES.**

La empresa afirma que **“solo se permite la entrega de información a las autoridades competentes, previa solicitud mediante un mandamiento o requerimiento (escrito o por medio electrónico), debidamente fundado y motivado, de la autoridad competente y/o mediante resolución judicial en los términos que establezcan las leyes vigentes en los países donde operamos”**.¹⁶ Aunque no exprese directamente que se compromete a rechazar requerimientos de información que incumplan los requisitos legales, esto puede entenderse como su compromiso de solo entregar datos cuando tales requisitos sean cumplidos.

CALIFICACIÓN: CLARO PANAMÁ RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

15. América Móvil, Informe de Transparencia en las Comunicaciones 2020, p. 9. Disponible en: <http://img1.telcel.com/amx/informe-transparencia-comunicaciones.pdf>

16. América Móvil, Informe de Sustentabilidad 2020, p. 94. Disponible en: https://s22.q4cdn.com/604986553/files/doc_downloads/2021/05/Informe-de-Sustentabilidad-2020.pdf Nótese que en su Informe de Transparencia afirma también que la entrega de la información “solamente será exigible previo requerimiento escrito, debidamente fundamentado y motivado por la autoridad competente”. Disponible en: <http://img1.telcel.com/amx/informe-transparencia-comunicaciones.pdf>

5. DEFENSA DE DERECHOS HUMANOS

- **LA EMPRESA PROMUEVE A TRAVÉS DE CAMPAÑAS O ACTIVIDADES LA IMPORTANCIA DE LA PRIVACIDAD Y PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve en sus redes sociales (Twitter e Instagram) y/o sitio web campañas o actividades sobre privacidad y protección de datos personales.

- **LA EMPRESA PROMUEVE INICIATIVAS DE LEY, LITIGIO ESTRATÉGICO, O DE POLÍTICAS PÚBLICAS PARA LA PROTECCIÓN DE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve o ejecuta iniciativas de ley, litigio estratégico o de políticas públicas para la privacidad y protección de datos personales.

- **LA EMPRESA PARTICIPA EN MECANISMOS O PROCESOS MULTISECTORIALES PARA LA PROMOCIÓN DE LOS DERECHOS HUMANOS EN EL MARCO DE SUS RESPONSABILIDADES EMPRESARIALES.**

La empresa no ha participado en mecanismos o procesos multisectoriales de promoción de derechos humanos. No se encuentra información referente a este parámetro en su sitio web o en sus redes sociales (Twitter e Instagram).

Cabe mencionar que la empresa se comprometió el año pasado con el Plan Educativo Solidario y Plan de Telecomunicaciones Solidario para brindar internet móvil gratis a estudiantes y a aquellas personas afectadas por la pandemia; sin embargo, no se pudo encontrar información sobre el avance o implementación del mismo. En el Reporte de Sustentabilidad publicado en América Móvil se menciona que América Móvil ofrece navegación gratuita en la plataforma App-Prende de la Fundación Carlos Slim.

Por otro lado, en el mismo reporte, se menciona que en seguimiento a la participación de América Móvil en el programa “Nos Importa” del GSMA, su subsidiaria en Panamá ha participado en campañas para implementar reciclaje de dispositivos móviles, actividades de reforestación, protección ambiental y la eliminación de dispositivos robados a través de la identificación del número IMEI.

CALIFICACIÓN: CLARO PANAMÁ RECIBE ¼ DE ESTRELLA AL CUMPLIR CON AL MENOS UNO DE LOS PARÁMETROS DE EVALUACIÓN.

6. SEGURIDAD DIGITAL

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS PARA NAVEGAR EN SU PÁGINA WEB.**

La empresa mantiene el protocolo HTTPS al momento de navegar en todas sus páginas web.

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS INCLUSIVE A LA HORA DE HACER PAGOS EN LÍNEA.**

La empresa mantiene el protocolo HTTPS al momento de realizar pagos en su página web.

- **LA EMPRESA PUBLICA O PONE A DISPOSICIÓN DE SUS CLIENTES INFORMACIÓN O CONTENIDOS SOBRE SEGURIDAD DIGITAL.**

La empresa no promueve, publica o pone a disposición en sus redes sociales (Twitter e Instagram) y/o sitio web contenidos sobre seguridad digital para sus usuarios. Aunque este tipo de contenido esté disponible para los colaboradores de Claro Panamá, tal como informó la empresa, lo que se busca evaluar con este parámetro es la información que se brinda a sus usuarios con el objetivo de sensibilizar y educar en materia de seguridad digital.

- **LA EMPRESA MANTIENE UN PROTOCOLO PARA INFORMAR A SUS USUARIOS SOBRE FILTRACIONES DE DATOS.**

La empresa cuenta con una guía para el requerimiento de la información personal de sus clientes por parte de la autoridad que sea públicamente accesible y tenga en cuenta el

CALIFICACIÓN: CLARO PANAMÁ RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

7. GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD

- **LA EMPRESA CUENTA CON UNA GUÍA PARA EL REQUERIMIENTO DE LA INFORMACIÓN PERSONAL DE SUS CLIENTES POR PARTE DE LA AUTORIDAD QUE SEA PÚBLICAMENTE ACCESIBLE Y TENGA EN CUENTA EL MARCO LEGAL LOCAL.**

La empresa no mantiene este tipo de guía en su sitio web; sin embargo, sí está disponible en idioma español como una sección dentro del Informe de Transparencia en las Comunicaciones 2020 llamada “Proceso de atención y respuesta a solicitudes de autoridad competente en Centroamérica”.

La guía explica que el procedimiento para cada solicitud en Centroamérica comienza con el análisis legal de las órdenes de la autoridad competente, con el objetivo de validar las facultades y procedencia. En caso de que esta solicitud cumpla con la ley vigente, se obtiene y procesa la información para luego elaborar la contestación oficial a la autoridad competente.

Por último, se envía la información requerida a la autoridad competente a través de mecanismos que garanticen la inalterabilidad y confidencialidad de la información.

Si bien la sección es para la región centroamericana, la guía obtiene sentido local pues aparece después de la descripción legal aplicable en requerimientos de información en cada país de Centroamérica, incluyendo Panamá.

Sin embargo, el apartado sobre la legislación de Panamá todavía puede avanzar en detallar las autoridades competentes para los distintos tipos de solicitud de datos y los requisitos analizados por la empresa en las solicitudes recibidas.¹⁷ De manera que se pueda reconocer la relevancia de la información publicada por la empresa en su informe, pero apuntar que todavía se puede avanzar en la transparencia de su política de entrega de datos a la autoridad, se brindó puntaje parcial para este criterio.

CALIFICACIÓN: CLARO PANAMÁ RECIBE ½ DE ESTRELLA AL CUMPLIR PARCIALMENTE CON EL PARÁMETRO DE EVALUACIÓN.

EMPRESA EVALUADA: DIGICEL

1. POLÍTICA DE PROTECCIÓN DE DATOS

- **LA EMPRESA CUENTA CON UNA POLÍTICA DE PROTECCIÓN DE DATOS, APLICADA A SUS SERVICIOS DE TELECOMUNICACIONES, PUBLICADA EN SU SITIO WEB**

Digicel Panamá cuenta con una política de protección de datos. La búsqueda en internet de “Digicel Panamá” arroja como primer resultado <https://www.digicelgroup.com/pa/>, pero igualmente muestra la página [digicel.com.pa](https://www.digicel.com.pa/).

Al ingresar a la primera, el usuario deberá dirigirse a la sección de “Legal” encontrada en la parte inferior del sitio web. Esta sección enumera distintos productos con sus términos y condiciones. En el numeral 5 del listado, Digicel muestra su Política de Privacidad a la que también llama **“Declaración sobre Privacidad de los Datos”**. En el segundo sitio web llamado **“Digicel eShop”**, Digicel también cuenta con una política de privacidad dentro de Términos y Condiciones ubicada en la parte inferior del sitio.

Sobre la vinculación de la política de protección de datos con la prestación del servicio, el primer sitio web explica que el usuario:

“Debe leer esta notificación, conjuntamente con los Términos y Condiciones de uso de nuestros sitios web, aplicaciones y de nuestros productos y servicios. Esta Declaración sobre Privacidad cubre todos los negocios y entidades de Digicel en todos los países en los que opera”.

No obstante, la política de privacidad del segundo sitio web es únicamente para su página web y no contempla la prestación del servicio. Se pudiera considerar que Digicel ha cumplido con este parámetro si se interpreta que la página de Digicel Group es a la que más acceso tendrían los usuarios panameños con el cambio de nombre del sitio web de Digicel en Panamá a **“Digicel eShop”**.

Hay que considerar también que el sitio de Digicel Group contiene una sección específica para Panamá. De todas maneras, la empresa debería publicar también en el sitio web relativo a **“Digicel eShop”** la política de privacidad aplicable a sus servicios.

- **LA POLÍTICA ES CLARA Y DE FÁCIL ACCESO A LOS USUARIOS.**

La política es clara y su lenguaje está orientado a ser lo suficientemente general para ser usada indistintamente en las aplicaciones, sitios web y servicios de Digicel.

Sin embargo, Digicel no muestra fácilmente su política de protección de datos en su página principal, como se ha señalado en reportes anteriores. Su acceso es difícil para el público porque esta se encuentra dentro de la sección “Legal” que no resalta y pareciera estar aparte de los demás enlaces de interés. Además, la política forma parte de un listado de otros temas que impiden que un usuario pueda encontrarla fácilmente.

- **LA POLÍTICA ESTABLECE CUÁLES DATOS SON RECOPIRADOS.**

La política establece de manera enunciativa y sin limitaciones cuáles son los datos recopilados a través de sus aplicaciones, sitios web y servicios de Digicel.

Estos son: **información de contacto** (como nombre, dirección, dirección de correo electrónico y número de teléfono); **información de identificación** (como número de pasaporte, número de registro impositivo o número de seguro social, licencia de conducir, fecha de nacimiento); **información demográfica** (como rango de edad, estado civil, género); **fotografías como las que puede enviar para concursos o competencias con premios**; **información específica sobre productos** (como preferencia, grupo cerrado de usuarios, familiares o amigos incluidos en el plan de servicio, límite de crédito); **información bancaria** (como transacciones bancarias de débito directas o de pago de facturas relacionadas); **e información de la cuenta de servicio** (como uso de llamadas, saldos de cuenta, historial de transacciones, información crediticia, facturación, puntos de lealtad acumulados).

- **LA POLÍTICA ESTABLECE EL PLAZO DE RETENCIÓN DE LOS DATOS DE LOS USUARIOS.**

Digicel cuenta con una sección en su política de “retención de datos” en la que explica que serán retenidos por el tiempo específico necesario, dependiendo de la ley de cada país.

Al ser la política suficientemente amplia como para poder ser homogénea en distintos países y no necesitar ser modificada por leyes o reglamentos, esta no establece un plazo de retención específico. Esto demuestra que más allá de una política de protección general aplicable a todas sus subsidiarias, Digicel debería publicar una política de protección de datos relativa a sus servicios adaptada a Panamá.

- **LA POLÍTICA MENCIONA Y EXPLICA LOS DERECHOS ARCO Y CÓMO PUEDEN SER EJERCIDOS.**

La política no menciona o explica los derechos ARCO ni cómo pueden ser ejercidos. En este punto se señala que para el ejercicio de derechos, la política se limita a ofrecer un correo no específico para Panamá y una línea telefónica estadounidense. Estos puntos dificultan que el público panameño pueda ejercer sus derechos ARCO.

CALIFICACIÓN: DIGICEL RECIBE ¼ DE ESTRELLA AL CUMPLIR CON AL MENOS UNO DE LOS PARÁMETROS DE EVALUACIÓN.

2. INFORMES DE TRANSPARENCIA

- **LA EMPRESA PUBLICA INFORMES DE TRANSPARENCIA.**

La empresa no publica informes de transparencia en su página web. Este punto fue señalado en el reporte anterior y no se visibilizan avances en este parámetro.

- **LOS INFORMES ESTÁN FÁCILMENTE ACCESIBLES A SUS USUARIOS.**

La empresa no publica informes de transparencia y, por lo tanto, no puede puntuar en este parámetro.

- **LOS INFORMES CONTIENEN DATOS RELACIONADOS AL NÚMERO DE SOLICITUDES RECIBIDAS, CUMPLIDAS Y EL TIPO DE SOLICITUD.**

Los usuarios de Digicel no tienen forma de conocer el número de veces que las autoridades competentes han solicitado información a Digicel y cuántas veces estas han sido aceptadas o rechazadas.

CALIFICACIÓN: DIGICEL LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON EL PARÁMETRO DE EVALUACIÓN.

3. NOTIFICACIÓN AL USUARIO

- **LA EMPRESA SE COMPROMETE A NOTIFICAR AL USUARIO SOBRE LA INFORMACIÓN SOLICITADA EN EL PRIMER MOMENTO PERMITIDO POR LEY.**

Digicel no mantiene este compromiso con sus usuarios. Según la política de privacidad, el compromiso de Digicel se limita a no vender, intercambiar, transferir información personal, a menos que esta sea requerida por “autoridad competente, para fines investigativos y expresamente configurados dentro del marco legal”.

CALIFICACIÓN: DIGICEL LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

4. AUTORIZACIÓN JUDICIAL

- **LA EMPRESA PROMETE EN SUS CONTRATOS, POLÍTICAS O TÉRMINOS DE SERVICIO A EXIGIR A LAS AUTORIDADES UNA AUTORIZACIÓN JUDICIAL ANTES DE SUMINISTRAR EL CONTENIDO DE LAS COMUNICACIONES DE SUS CLIENTES.**

La empresa no mantiene este tipo de compromiso expresamente en su sitio web. Digicel opta por mencionar que no van a transferir o compartir de ninguna manera información personal, excepto a la autoridad competente y para fines expresamente configurados dentro del marco legal.

- **LA EMPRESA SE COMPROMETE A RECHAZAR REQUERIMIENTOS DE ENTREGA DE INFORMACIÓN EN CASOS QUE INCUMPLAN REQUISITOS LEGALES.**

La empresa afirma en su política que “no vende, intercambia, transfiere o de ninguna otra manera comparte su información personal, a excepción de requerimiento de autoridad competente, para fines investigativos y expresamente configurados dentro del marco legal”. Esto puede implicar una afirmación de la empresa de que solo comparte la información personal de sus clientes a partir de un requerimiento de la autoridad competente para “**fines (...) expresamente configurados dentro del marco legal**”. A diferencia de Claro, la sentencia anterior es una expresión más genérica que no remarca la necesidad de requerimiento debidamente fundado y motivado o la verificación de que dicho requerimiento cumple los términos legales que autorizan el acceso a los datos de los usuarios.

Por otro lado, al ser la redacción muy genérica y hasta cierto punto ambigua deja a interpretación si para Digicel el fin investigativo y los demás fines que tenga la autoridad competente sobre infracciones penales, son suficientes para transferir información personal o si le exigirá los requerimientos legales que debe seguir la autoridad competente para perseguir sus fines.

Se considera que el progreso de Digicel en este tema es positivo en comparación al reporte anterior por lo que se toma en consideración en esta edición del reporte.

CALIFICACIÓN: DIGICEL RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

5. DEFENSA DE DERECHOS HUMANOS

- **LA EMPRESA PROMUEVE A TRAVÉS DE CAMPAÑAS O ACTIVIDADES LA IMPORTANCIA DE LA PRIVACIDAD Y PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve en sus redes sociales (Twitter e Instagram) y/o sitio web campañas o actividades sobre privacidad y protección de datos personales.

- **LA EMPRESA PROMUEVE INICIATIVAS DE LEY, LITIGIO ESTRATÉGICO, O DE POLÍTICAS PÚBLICAS PARA LA PROTECCIÓN DE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve o ejecuta iniciativas de ley, litigio estratégico o de políticas públicas para la privacidad y protección de datos personales.

- **LA EMPRESA PARTICIPA EN MECANISMOS O PROCESOS MULTISECTORIALES PARA LA PROMOCIÓN DE LOS DERECHOS HUMANOS EN EL MARCO DE SUS RESPONSABILIDADES EMPRESARIALES.**

La empresa no participa en mecanismos o procesos multisectoriales de promoción de derechos humanos. No se encontró información referente a este parámetro en su sitio web o en sus redes sociales (Twitter e Instagram).

Cabe mencionar que la empresa sí ha tenido una constante participación social. En seguimiento al acuerdo Plan Educativo Solidario y Plan de Telecomunicaciones Solidario firmado en el 2020 para brindar internet móvil gratis a estudiantes y a aquellas personas afectadas por la pandemia, respectivamente, Digicel lanzó el plan del 15 de marzo 2021 al 15 junio 2021.

Igualmente, **Digicel Panamá** fue reconocida en los [Latin American SABRE Awards 2021](#) por la mejor campaña comunicacional de Centroamérica que permitió la donación de más de 2 millones de insumos médicos a 14 centros hospitalarios durante la pandemia.¹⁸ En esta misma línea, Digicel lanzó el proyecto **“Conexión de Amor”** como parte de su iniciativa **“Somos una red humana”**.¹⁹ Dicho proyecto busca que personas de tercera edad en asilos u hogares tengan la oportunidad de interactuar y compartir sus historias virtualmente con voluntarios.

CALIFICACIÓN: DIGICEL RECIBE ¼ DE ESTRELLA AL CUMPLIR CON AL MENOS UNO DE LOS PARÁMETROS DE EVALUACIÓN.

18. Digicel, 'Juntos Somos Héroes' de Digicel Panamá gana premio internacional, 2021. Disponible en:

<https://www.prnewswire.com/news-releases/-juntos-somos-heroes-de-digicel-panama-gana-premio-internacional-875097728.html>

19. El Capital Financiero, Campaña “Somos una red humana” apoya conectividad de casas hogar de adultos mayores, 2021. Disponible en: <https://elcapitalfinanciero.com/campana-somos-una-red-humana-apoya-conectividad-de-casas-hogar-de-adultos-mayores/>

6. SEGURIDAD DIGITAL

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS PARA NAVEGAR EN SU PÁGINA WEB.**

La empresa mantiene el protocolo HTTPS al momento de navegar en todas sus páginas web.

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS INCLUSIVE A LA HORA DE HACER PAGOS EN LÍNEA.**

La empresa mantiene el protocolo HTTPS al momento de realizar pagos en su página web, Digicel eShop.

- **LA EMPRESA PUBLICA O PONE A DISPOSICIÓN DE SUS CLIENTES INFORMACIÓN O CONTENIDOS SOBRE SEGURIDAD DIGITAL.SOBRE SEGURIDAD DIGITAL.**

La empresa no promueve, publica o pone a disposición en sus redes sociales (Twitter e Instagram) y/o sitio web contenidos sobre seguridad digital de forma regular y continua. Este tipo de contenido sí se distingue en su sitio de Digicel Group aunque en idioma inglés si se selecciona otro país.

- **LA EMPRESA MANTIENE UN PROTOCOLO PARA INFORMAR A SUS USUARIOS SOBRE FILTRACIONES DE DATOS.**

La empresa no mantiene público un protocolo para informar a sus usuarios sobre filtraciones de datos. Este punto no se menciona en sus políticas de privacidad.

CALIFICACIÓN: DIGICEL RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

7. GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD

- **LA EMPRESA CUENTA CON UNA GUÍA PARA EL REQUERIMIENTO DE LA INFORMACIÓN PERSONAL DE SUS CLIENTES POR PARTE DE LA AUTORIDAD QUE SEA PÚBLICAMENTE ACCESIBLE Y TENGA EN CUENTA EL MARCO LEGAL LOCAL.**

La empresa no mantiene este tipo de guía en su sitio web panameño. En el sitio internacional de la empresa tampoco se encontró este documento o alguno parecido.

CALIFICACIÓN: DIGICEL LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

EMPRESA EVALUADA: MÁS MÓVIL

1. POLÍTICA DE PROTECCIÓN DE DATOS

- **LA EMPRESA CUENTA CON UNA POLÍTICA DE PROTECCIÓN DE DATOS, APLICADA A SUS SERVICIOS DE TELECOMUNICACIONES, PUBLICADA EN SU SITIO WEB**

Más Móvil cuenta con una política de protección de datos publicada en su [sitio web](#), la cual expresamente menciona que esta describe **“cómo obtenemos y procesamos tu información personal cuando usas y cuando te proveemos de nuestros productos y servicios”**.

La política en su párrafo introductorio explica que la política rige la manera en la que **Cable & Wireless Panamá, S.A. (CWP)**, empresa dueña de Más Móvil, administra la información personal. Además, al leerla se nota que esta política no se limita únicamente a ser una política de protección de datos del sitio web, sino que al leerla se puede fácilmente señalar que +Móvil la enfoca hacia la prestación de servicios. Se reconoce a la empresa este sustancial avance en comparación con los reportes que se han publicado hasta la fecha.

- **LA POLÍTICA ES CLARA Y DE FÁCIL ACCESO A LOS USUARIOS.**

La política es clara y no deja lugar a dudas que la política será utilizada para la prestación de servicios y que el usuario debe revisarla periódicamente, ya que está sujeta a cambios periódicos. Además, cabe resaltar que la política plantea sus diversas secciones en forma de preguntas empezando por: **“¿Qué debemos entender por información personal?”**

Con respecto a su acceso, este puede ser ingresado desde la página principal, aunque puede no ser intuitivo para el público porque se encuentra en un cintillo bajo un color oscuro, tipografía distinta y tamaño de letra pequeña. Esta no resalta y pudiera pasar desapercibida para un usuario.

Siguiendo el mismo análisis con otras empresas, la empresa no cumple con el parámetro porque se considera que pierde congruencia que una política muy bien diseñada y redactada sea de difícil acceso.

- **LA POLÍTICA ESTABLECE CUÁLES DATOS SON RECOPIRADOS.**

La política establece que se van a conservar datos, considerando la naturaleza de los productos y servicios que ofrece Más Móvil. De ahí, la política didácticamente desarrolla 5 instancias en las que obtiene diversos tipos de datos y aporta ejemplos para que el usuario entienda cada escenario en el cual la empresa recabará sus datos.

Por la extensión, no se mencionarán los ejemplos, pero sí los escenarios. La política menciona que pudiera conservar: información de contacto que les permite identificar al usuario; información de la cuenta cuando se instala el servicio; información cuando se ingresa en una promoción o para conocer sobre los productos o servicios; información necesaria para entregarte nuestros servicios; información de uso general que permite saber cómo están siendo usados los productos y servicios, sin necesariamente identificar al usuario; y otra información personal que **Cable & Wireless Panamá** podría obtener desde fuentes públicas disponibles, de acuerdo a las leyes aplicables.

- **LA POLÍTICA ESTABLECE EL PLAZO DE RETENCIÓN DE LOS DATOS DE LOS USUARIOS.**

La política no establece un plazo determinado. La política le informa al usuario que la información personal se retendrá dependiendo del propósito por el cual se usa y se mantendrá por el tiempo que sea necesario para cumplir con ese propósito siempre que las leyes aplicables no digan algo distinto. Se considera que este tipo de redacción es laxa porque eventualmente conlleva a que el usuario siempre desconocerá el plazo de retención.

- **LA POLÍTICA MENCIONA Y EXPLICA LOS DERECHOS ARCO Y CÓMO PUEDEN SER EJERCIDOS.**

La política menciona directamente que el usuario tiene derecho al Acceso, Rectificación, Cancelación, Oposición y Portabilidad de la información personal siguiendo el marco de la Ley 81 del 2019 sobre Protección de Datos Personales.

Agregado a esto, la política plantea escenarios en los que los derechos puedan ser ejercidos y cómo pueden ser ejercidos, dándole especial énfasis al derecho de acceso. La política desarrolla que para ese derecho el usuario deberá presentarse a una sucursal de **+Móvil** y llenar el formulario de **“Solicitud de Acceso de Datos de Clientes”**, la cual será respondida en los siguientes 10 días hábiles por correo electrónico. Con respecto a los demás derechos, se da a entender que se debe contactar a la empresa a través del correo: privacidad@cwpanama.com.

CALIFICACIÓN: MÁS MÓVIL RECIBE ½ DE ESTRELLA AL CUMPLIR CON TRES DE LOS CINCO PARÁMETROS..

2. INFORMES DE TRANSPARENCIA

- **LA EMPRESA PUBLICA INFORMES DE TRANSPARENCIA.**

La empresa no publica informes de transparencia en su página web. Este punto fue señalado en el reporte anterior y no se visibilizan avances en este parámetro. Se intentó buscar los reportes en la página de **Liberty Latin America**, pero no pudimos encontrarlos.

- **LOS INFORMES ESTÁN FÁCILMENTE ACCESIBLES A SUS USUARIOS.**

La empresa no publica informes de transparencia y, por lo tanto, no puede puntuar en este parámetro.

- **LOS INFORMES CONTIENEN DATOS RELACIONADOS AL NÚMERO DE SOLICITUDES RECIBIDAS, CUMPLIDAS Y EL TIPO DE SOLICITUD.**

Los usuarios de **Más Móvil** no tienen forma de conocer el número de veces que las autoridades competentes han solicitado información a Digicel y cuántas veces estas han sido aceptadas o rechazadas.

CALIFICACIÓN: MÁS MÓVIL LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON EL PARÁMETRO DE EVALUACIÓN.

3. NOTIFICACIÓN AL USUARIO

- **LA EMPRESA SE COMPROMETE A NOTIFICAR AL USUARIO SOBRE LA INFORMACIÓN SOLICITADA EN EL PRIMER MOMENTO PERMITIDO POR LEY.**

Más Móvil no mantiene este compromiso claramente con sus usuarios. En la política de privacidad, la empresa explica detalladamente que utilizarán y revelarán la información personal de usuarios para cumplir obligaciones legales.

Textualmente explican que las divulgaciones podrán “**ser hechas con o sin tu consentimiento y conocimiento, y con o sin aviso, en cumplimiento de los términos de un proceso legal, de conformidad a los procesos establecidos en la Ley 51, del 18 de septiembre de 2009.**”

La política no explica lo resalta de cuando se hace con aviso y cuáles son las consideraciones que sopesan para tomar esa decisión. Esta deficiencia puede llevar a que la divulgación de la información personal se dé siempre sin aviso. No obstante, se resalta que empiece a retarse el status quo de que el usuario no será notificado en ningún momento.

Más Móvil presenta que existe la posibilidad de que haya un aviso y se resalta el avance con calificación parcial.

CALIFICACIÓN: MÁS MÓVIL RECIBE ¼ DE ESTRELLA AL CUMPLIR PARCIALMENTE CON EL PARÁMETRO DE EVALUACIÓN.

4. AUTORIZACIÓN JUDICIAL

- **LA EMPRESA PROMETE EN SUS CONTRATOS, POLÍTICAS O TÉRMINOS DE SERVICIO A EXIGIR A LAS AUTORIDADES UNA AUTORIZACIÓN JUDICIAL ANTES DE SUMINISTRAR EL CONTENIDO DE LAS COMUNICACIONES DE SUS CLIENTES.**

En la política de privacidad, **Más Móvil** señala directamente que **Cable & Wireless Panamá**, empresa dueña de la marca, se reserva el derecho de cuestionar el acceso a información personal a las autoridades. Sin embargo, no hay mención a las autoridades competentes para emitir tales solicitudes, tampoco el compromiso expreso con la necesidad de autorización judicial para el suministro del contenido de las comunicaciones de sus usuarios.

- **LA EMPRESA SE COMPROMETE A RECHAZAR REQUERIMIENTOS DE ENTREGA DE INFORMACIÓN EN CASOS QUE INCUMPLAN REQUISITOS LEGALES.**

La empresa menciona expresamente en más de una ocasión, que revelarán información personal a autoridades o terceras partes siempre de acorde a la ley y que se reservan el derecho de cuestionar las solicitudes recibidas.

Aunque no expresen directamente un compromiso de rechazar las solicitudes que incumplan requisitos legales, la política refleja un avance en demostrar un compromiso con el análisis de solicitudes de información bajo las garantías legales y con la posibilidad de cuestionarlas cuando estas garantías no se cumplan. Si bien la empresa puede todavía perfeccionar este compromiso para dejarlo más claro y robusto, se considera el avance en esta edición en comparación a la edición 2020 para brindarle puntaje.

CALIFICACIÓN: MÁS MÓVIL RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

5. DEFENSA DE DERECHOS HUMANOS

- **LA EMPRESA PROMUEVE A TRAVÉS DE CAMPAÑAS O ACTIVIDADES LA IMPORTANCIA DE LA PRIVACIDAD Y PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve en sus redes sociales (Twitter e Instagram) y/o sitio web campañas o actividades sobre privacidad y protección de datos personales.

- **LA EMPRESA PROMUEVE INICIATIVAS DE LEY, LITIGIO ESTRATÉGICO, O DE POLÍTICAS PÚBLICAS PARA LA PROTECCIÓN DE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS DE SUS USUARIOS.**

La empresa no promueve o ejecuta iniciativas de ley, litigio estratégico o de políticas públicas para la privacidad y protección de datos personales.

- **LA EMPRESA PARTICIPA EN MECANISMOS O PROCESOS MULTISECTORIALES PARA LA PROMOCIÓN DE LOS DERECHOS HUMANOS EN EL MARCO DE SUS RESPONSABILIDADES EMPRESARIALES.**

+**Móvil**, por medio de Cable Wireless Panamá, participa del [Pacto Mundial de las Naciones Unidas](#) desde el 2006 y se ha mantenido publicando reportes de su avance cada año. Este pacto tiene como finalidad transformar el mercado global, potenciando un sector privado sostenible y responsable sobre la base de 10 principios, comprendiendo los 17 Objetivos del Desarrollo Sostenible (ODS) en áreas relacionadas con los derechos humanos, el trabajo, el medio ambiente y la corrupción.

En su reporte de avance del 2021, **Cable & Wireless** menciona que se enfocó en apoyar la conectividad, la salud comunitaria, la reducción de la brecha digital, el equilibrio económico, la calidad de la educación y la conservación del ambiente.²⁰

A lo largo del reporte, **Cable & Wireless** da muestras de las diversas actividades y proyectos que ha ejecutado durante el 2021. Entre los ejemplos a destacar está su respaldo al Plan Educativo Solidario para brindar internet móvil a estudiantes, el acceso gratuito a sitios web oficiales del gobierno y la eliminación el consumo de datos móviles de aplicaciones de comunicación como Telegram o Signal.

Aunado a lo anterior, **Más Móvil**, a través de la Fundación Cable & Wireless (**FCWP**), firmó un convenio de cooperación con el Ministerio de Desarrollo Social con una duración de tres años prorrogables con el objetivo de contribuir a la formación profesional de los jóvenes.²¹

Igualmente, **FCWP** renovó su compromiso con la Fundación Ayudinga para impulsar proyectos de educación por medio de la tecnología y plataformas virtuales de estudio.²²

CALIFICACIÓN: MÁS MÓVIL RECIBE ¼ DE ESTRELLA AL CUMPLIR CON AL MENOS UNO DE LOS PARÁMETROS DE EVALUACIÓN.

6. SEGURIDAD DIGITAL

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS PARA NAVEGAR EN SU PÁGINA WEB.**

La empresa mantiene el protocolo HTTPS al momento de navegar en todas sus páginas web.

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS INCLUSIVE A LA HORA DE HACER PAGOS EN LÍNEA.**

La empresa mantiene el protocolo HTTPS al momento de realizar pagos en su página web.

20. Cable & Wireless Panamá, REPORTE ACTUALIZADO DE PROGRESO AL PACTO GLOBAL 2021. Disponible para descarga en: <https://www.unglobalcompact.org/what-is-gc/participants/1592-Cable-Wireless-Panama-S-A->

21. Ministerio de Desarrollo Social, MIDES y Fundación Cable & Wireless Panamá entablan acuerdo para apoyar a la juventud, 2021. Disponible en: <https://www.mides.gob.pa/2021/08/13/mides-y-fundacion-cable-wireless-panama-entablan-acuerdo-para-apoyar-a-la-juventud/>

22. Comunicado de Prensa Más Móvil Panamá, Fundación CWP firma convenio con Fundación Ayudinga, para seguir apoyándoles con servicios de tecnología en sus plataformas de enseñanza aprendizaje, 2021. Disponible en: <https://www.masmovilpanama.com/fundacion-cwp-firma>

- **LA EMPRESA PUBLICA O PONE A DISPOSICIÓN DE SUS CLIENTES INFORMACIÓN O CONTENIDOS SOBRE SEGURIDAD DIGITAL.SOBRE SEGURIDAD DIGITAL.**

La empresa no promueve, publica o pone a disposición en sus redes sociales (Twitter e Instagram) y/o sitio web contenidos sobre seguridad digital de forma regular y continua. De la búsqueda realizada durante el 2021, solo se pudo notar una publicación en la que se hace referencia al Día de la Internet Segura.

- **LA EMPRESA MANTIENE UN PROTOCOLO PARA INFORMAR A SUS USUARIOS SOBRE FILTRACIONES DE DATOS.**

La empresa no mantiene público un protocolo para informar a sus usuarios sobre filtraciones de datos. Este punto no se menciona en sus políticas de privacidad.

CALIFICACIÓN: MÁS MÓVIL RECIBE ½ DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

7. GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD

- **LA EMPRESA CUENTA CON UNA GUÍA PARA EL REQUERIMIENTO DE LA INFORMACIÓN PERSONAL DE SUS CLIENTES POR PARTE DE LA AUTORIDAD QUE SEA PÚBLICAMENTE ACCESIBLE Y TENGA EN CUENTA EL MARCO LEGAL LOCAL.**

La empresa no mantiene este tipo de guía en su sitio web panameño. En el sitio internacional de la empresa tampoco se encontró este documento o alguno parecido.

CALIFICACIÓN: MÁS MÓVIL LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

EMPRESA EVALUADA: MÁS MÓVIL

1. POLÍTICA DE PROTECCIÓN DE DATOS

- **LA EMPRESA CUENTA CON UNA POLÍTICA DE PROTECCIÓN DE DATOS, APLICADA A SUS SERVICIOS DE TELECOMUNICACIONES, PUBLICADA EN SU SITIO WEB**

La empresa cuenta con una política de protección de datos en su [sitio web](#) para Panamá. No obstante, siguiendo el mismo análisis realizado el año pasado, Tigo enfoca las políticas de privacidad a su sitio web, el Portal Tigo, la App Mi Tigo Online y a Tigo Business Online. En nuestro reporte del 2020, se había inferido que de esta política de privacidad “pareciese ser aplicable para todo dato personal de los clientes recabado por la empresa”. Habiendo analizado la política en esta versión del reporte se nota que los Términos y Condiciones del sitio web explican que se debe entender que la Políticas de Privacidad es parte de los Términos y Condiciones y que estos Términos no se aplican a la contratación de servicios. Específicamente, se lee:

“Los datos personales obtenidos a través de la contratación y uso de Servicios de TIGO son tratados en base a términos y condiciones, y cláusulas de privacidad, adicionales y distintos al presente”.

Por tal razón, se da a entender que los usuarios que deseen conocer la política de privacidad de Tigo deben entablar una relación contractual. A primera vista, no son accesibles al público. A pesar de ello, Tigo pone a disposición del público una lista actualizada del 2021 de los contratos que puede tener con sus clientes. Al analizar estos contratos, no se hace mención de que Tigo posea una política de privacidad en la prestación del servicio. En su contrato de “Nuevos Servicios de Tigo”, se establece únicamente que:

“EL CLIENTE autoriza a TIGO a tratar sus datos personales para fines promocionales, manejo de relaciones con nuestras afiliadas y subsidiarias, para el cumplimiento de requerimientos legales y para la adecuada prestación de los servicios contratados”.

A menos que esta exista bajo un documento aparte que se le presenta al usuario contratante, se puede concluir que Tigo no posee una política de protección de datos aplicable a sus servicios en Panamá. Sin embargo, Grupo Millicom sí cuenta con una política de privacidad en su [sitio web](#) aplicable a los servicios de todas sus empresas afiliadas, lo que incluye Cable Onda, S.A.

- **LA POLÍTICA ES CLARA Y DE FÁCIL ACCESO A LOS USUARIOS.**

La política de privacidad del sitio web es clara en su lenguaje, llegando a explicar con detalle los datos que se recaban, cómo se recopilan los datos, la finalidad de estos, el plazo de retención y cómo se pueden aplicar los derechos de Acceso y Rectificación. Adicional, se distingue y se encuentra con facilidad al final del sitio web.

Sin embargo, esta política no puede ser calificada porque se refiere a los datos recabados en el sitio web de la empresa, no en los datos relativos a la prestación del servicio.

- **LA POLÍTICA ESTABLECE CUÁLES DATOS SON RECOPIRADOS.**

Esta política no puede ser calificada porque se refiere a los datos recabados en el sitio web de la empresa, no en los datos relativos a la prestación del servicio.

- **LA POLÍTICA ESTABLECE EL PLAZO DE RETENCIÓN DE LOS DATOS DE LOS USUARIOS.**

Esta política no puede ser calificada porque se refiere a los datos recabados en el sitio web de la empresa, no en los datos relativos a la prestación del servicio.

- **LA POLÍTICA MENCIONA Y EXPLICA LOS DERECHOS ARCO Y CÓMO PUEDEN SER EJERCIDOS.**

La política menciona la forma y la información de contacto para poder ejercer el acceso o rectificación de los datos que se recaben a través del Portal Tigo, la App Mi Tigo Online y Tigo Business Online.

Por otro lado, esta política no puede ser calificada porque se refiere a los datos recabados en el sitio web de la empresa, no en los datos relativos a la prestación del servicio.

CALIFICACIÓN: TIGO LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

2. INFORMES DE TRANSPARENCIA

- **LA EMPRESA PUBLICA INFORMES DE TRANSPARENCIA.**

Tigo no publica informes de transparencia en su sitio web panameño. Sin embargo, Grupo Millicom, dueño de Tigo, sí publica anualmente el Informe sobre Divulgación a las Autoridades Judiciales (LED) en su [sitio web](#).

El año pasado, se señaló que hubo un retroceso por parte de Tigo en su buena práctica de transparencia ya que Panamá no fue incluido en el reporte por el proceso de compra en el que se encontraba Millicom con la empresa Telefónica. En esta edición de nuestro reporte se señaló que Panamá aparece en el reporte a lo que Tigo resalta mencionando: **“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”**.

Considerando este avance, se aclara que los informes de transparencia de Grupo Millicom muestran el número de solicitudes de las autoridades judiciales de forma regional y no por cada país. El informe de transparencia explica que “una razón importante para no hacerlo es que varios de los países donde se opera prohíben dicha divulgación” de modo que optaron por dividir las solicitudes por región, América Central y América del Sur. Sería interesante que la empresa evaluara la posibilidad de hacerlo por país, o publicar informes estadísticos específicos a través de sus subsidiarias locales, en los casos en que no hay esta prohibición. Se entiende que tal limitación no existe bajo la legislación panameña.

- **LOS INFORMES ESTÁN FÁCILMENTE ACCESIBLES A SUS USUARIOS.**

El informe no se encuentra en la página web de Tigo Panamá y aunque su búsqueda en la página web de Grupo Millicom debe realizarse en inglés, tampoco es fácil acceder a ellos. La forma más directa de obtener los informes en español es buscándolos directamente en Google bajo “Informe de transparencia Grupo Millicom”.

- **LOS INFORMES CONTIENEN DATOS RELACIONADOS AL NÚMERO DE SOLICITUDES RECIBIDAS, CUMPLIDAS Y EL TIPO DE SOLICITUD.**

El informe que publica Grupo Millicom no detalla si las solicitudes fueron cumplidas ni especifica el país. El reporte muestra el número de solicitudes recibidas por región, el tipo de solicitud (interceptación, datos relacionados con servicios de dinero móvil (MFS) y metadatos, como registro de llamadas, dirección IP, posicionamiento global GPS del usuario, tráfico de internet y documentos en la nube) y el número de solicitudes por tipo.

CALIFICACIÓN: TIGO RECIBE ½ DE ESTRELLA AL CUMPLIR CON DOS DE LOS TRES PARÁMETROS DE EVALUACIÓN.

3. NOTIFICACIÓN AL USUARIO

- **LA EMPRESA SE COMPROMETE A NOTIFICAR AL USUARIO SOBRE LA INFORMACIÓN SOLICITADA EN EL PRIMER MOMENTO PERMITIDO POR LEY.**

La información pública en el sitio web de la empresa no muestra que Tigo asuma este compromiso con el usuario.

CALIFICACIÓN: TIGO LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

4. AUTORIZACIÓN JUDICIAL

- **LA EMPRESA PROMETE EN SUS CONTRATOS, POLÍTICAS O TÉRMINOS DE SERVICIO A EXIGIR A LAS AUTORIDADES UNA AUTORIZACIÓN JUDICIAL ANTES DE SUMINISTRAR EL CONTENIDO DE LAS COMUNICACIONES DE SUS CLIENTES.**

Tigo menciona en la política de privacidad del sitio web que Tigo puede comunicar o transferir los datos de los usuarios en respuesta a una orden escrita de autoridad judicial competente o cuando así sea permitido o requerido en cumplimiento de la ley. No hace mención específica al contenido de las comunicaciones para detallar si, en estos casos, la autoridad competente para emitir la solicitud es solamente la autoridad judicial. De todos modos, la política de privacidad se refiere apenas al sitio web y la aplicación de Tigo. Por ejemplo, en su contrato de nuevos servicios, Tigo establece que entre las exclusiones de responsabilidad por pérdidas directas o indirectas a los usuarios, será cuando estas se den bajo instrucciones de autoridad competente, orden o mandato judicial.

Por otro lado, el informe de transparencia de Grupo Millicom sí especifica la rama judicial como la autoridad que puede emitir órdenes de interceptación en Panamá.

- **LA EMPRESA SE COMPROMETE A RECHAZAR REQUERIMIENTOS DE ENTREGA DE INFORMACIÓN EN CASOS QUE INCUMPLAN REQUISITOS LEGALES.**

Tigo no hace mención directa a este compromiso en su sitio web o contratos, sino que se limita a informar que solo comparten los datos cuando así sea permitido o requerido por la ley. Por otro lado, el Grupo Millicom sí realiza este compromiso en sus informes de transparencia. En ellos, Grupo Millicom explica que parte de su proceso interno es evaluar si la solicitud cumple con la ley correspondiente y de no estarlo buscan las vías legales para impugnar la solicitud o presentar una queja ante las autoridades competentes.

CALIFICACIÓN: TIGO RECIBE 1 DE ESTRELLA AL CUMPLIR CON LA MITAD DE LOS PARÁMETROS DE EVALUACIÓN.

5. DEFENSA DE DERECHOS HUMANOS

- **LA EMPRESA PROMUEVE A TRAVÉS DE CAMPAÑAS O ACTIVIDADES LA IMPORTANCIA DE LA PRIVACIDAD Y PROTECCIÓN DE DATOS DE SUS USUARIOS.**

Durante el año 2021, Tigo realizó una serie de publicaciones en varios meses a través de su blog promoviendo la importancia de la privacidad y protección de datos de sus usuarios. De los temas que pudimos encontrar, Tigo compartió artículos en los que expuso notable contenido sobre [“Datos del consumidor con Big Data”](#), [“Tiendas en línea ¿cómo cuidar los datos?”](#), [“¿Sacrificamos privacidad por comodidad?”](#) y [“¿Compartes datos personales en la red?”](#)

Si bien no se encontraron campañas a través de sus redes sociales, es un buen avance que la empresa escriba artículos tocando temas como derecho al olvido y oversharing.

- **LA EMPRESA PROMUEVE INICIATIVAS DE LEY, LITIGIO ESTRATÉGICO, O DE POLÍTICAS PÚBLICAS PARA LA PROTECCIÓN DE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS DE SUS USUARIOS.**

Las redes sociales (Twitter e Instagram) y el sitio web de la empresa no dan muestra de la promoción de iniciativas de ley, litigio estratégico, o de políticas públicas para la protección de la privacidad y la protección de datos de sus usuarios

- **LA EMPRESA PARTICIPA EN MECANISMOS O PROCESOS MULTISECTORIALES PARA LA PROMOCIÓN DE LOS DERECHOS HUMANOS EN EL MARCO DE SUS RESPONSABILIDADES EMPRESARIALES.**

Grupo Millicom no forma parte de la Iniciativa de Red Global (GNI) tras cuatro años siendo miembro. En reportes anteriores se reiteró que desde el año 2017, Millicom formaba parte de la GNI, la cual es una red multisectorial que tiene como objetivo principal el promover la privacidad, la libertad de expresión y la colaboración entre distintos actores del sector, quedando obligados a cumplir con una serie de principios encaminados a proteger los derechos de los usuarios de Internet. Se desconoce las razones y si Grupo Millicom formará parte de otro organismo multisectorial.

No obstante, en marzo del 2021 Tigo Panamá se convirtió en firmante de los Principios para el Empoderamiento de las Mujeres (WEPs, de su siglas en inglés). De esta forma renueva su compromiso con ONU Mujeres y el Pacto Global de las Naciones Unidas para el empoderamiento de la mujer tanto de dentro de la empresa como en la sociedad. Dando seguimiento al acuerdo Plan Educativo Solidario y Plan de Telecomunicaciones suscrito en el 2020, Tigo informó en marzo del 2021 que el proyecto ya beneficiaba a 300,000 personas en 130 comunidades del país.²³

En esa misma línea, Tigo firmó el acuerdo de cooperación con el Movimiento **#TODOPANAMÁ** para brindar una donación económica y apoyo de sus voluntarios para responder las afectaciones y necesidades por el COVID 19.²⁴ Igualmente, la empresa participó del Programa Escuela Virtual con el objetivo de disminuir la brecha digital a través de brindarle datos y minutos a estudiantes.

CALIFICACIÓN: TIGO RECIBE ½ DE ESTRELLA AL CUMPLIR CON DOS DE LOS PARÁMETROS DE EVALUACIÓN.

6. SEGURIDAD DIGITAL

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS PARA NAVEGAR EN SU PÁGINA WEB.**

La empresa, en efecto, utiliza el protocolo HTTPS al momento de navegar el usuario en su página web.

- **LA EMPRESA UTILIZA EL PROTOCOLO HTTPS INCLUSIVE A LA HORA DE HACER PAGOS EN LÍNEA.**

La empresa hace uso del protocolo HTTPS al momento de realizar pagos en línea.

- **LA EMPRESA PUBLICA O PONE A DISPOSICIÓN DE SUS CLIENTES INFORMACIÓN O CONTENIDOS SOBRE SEGURIDAD DIGITAL.SOBRE SEGURIDAD DIGITAL.**

A través de su política de privacidad de su sitio web y aplicación, Tigo informa que las comunicaciones a través del internet pueden no ser seguras si no están encriptadas y además ha publicado contenidos como [“Ciberseguridad en Panamá ¿se practica?”](#), [“Errores humanos y ciberataques ¿qué hacer?”](#), [“Ciberdelitos en Panamá”](#), [“Ciberseguridad, la otra cara de la pandemia”](#) y [“¿Cómo evitar ser víctima de un ciberataque?”](#) Todos disponibles en el blog de su sitio web y de fácil acceso a través de palabras claves como “ciberseguridad en Panamá”.

El blog de Tigo contiene información sobre estos temas además de los ya que ya mencionamos, sobre [“Datos del consumidor con Big Data”](#), [“Tiendas en línea ¿cómo cuidar los datos?”](#), [“¿Sacrificamos privacidad por comodidad?”](#), y [“¿Compartes datos personales en la red?”](#).

23. Twitter, Tigo Panamá, 17 de marzo de 2021. Disponible en: <https://twitter.com/tigopanama/status/1372274344878034953>

24. Tigo Panamá, Tigo y movimiento #TodoPanamá: Compromiso por la recuperación socioeconómica del país, 2021. Disponible en: <https://www.tigo.com.pa/sala-de-prensa/tigo-y-movimiento-todopanama-compromiso-por-la-recuperacion-socioeconomica>

- **LA EMPRESA MANTIENE UN PROTOCOLO PARA INFORMAR A SUS USUARIOS SOBRE FILTRACIONES DE DATOS.**

Tigo no mantiene información respecto a protocolos en ciberseguridad en su sitio web. No obstante, Grupo Millicom sí cuenta con una sección en su página web sobre ciberseguridad en inglés. De ahí se puede saber que Tigo utiliza una combinación de estándares como NIST Cybersecurity Framework (CSF) y del ISO/IEC 27001:2013 en ciberseguridad. Parte integral de estos protocolos es el manejo de incidentes, por ejemplo, la filtración de datos, y el uso de las mejores prácticas para mitigar y responder los incidentes.

Entre esas mejores prácticas se menciona la comunicación del incidente a nivel interno y público acorde a ciertos lineamientos. Por tal razón, se puede inferir que Tigo bajo Cable Onda, S.A., empresa afiliada a Grupo Millicom seguirá estos protocolos en caso de una filtración de datos.

CALIFICACIÓN: TIGO RECIBE 1 DE ESTRELLA AL CUMPLIR CON TODOS LOS PARÁMETROS DE EVALUACIÓN.

7. GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD

- **LA EMPRESA CUENTA CON UNA GUÍA PARA EL REQUERIMIENTO DE LA INFORMACIÓN PERSONAL DE SUS CLIENTES POR PARTE DE LA AUTORIDAD QUE SEA PÚBLICAMENTE ACCESIBLE Y TENGA EN CUENTA EL MARCO LEGAL LOCAL.**

La empresa no publica en su sitio web este tipo de guía. Sin embargo, al momento de hacer nuestro análisis, se nota que Grupo Millicom sí mantiene una guía aunque en inglés sobre la asistencia que brinda a las autoridades judiciales.²⁵

En el reporte anterior se otorgó una calificación parcial por la guía en inglés; sin embargo, no se otorgará puntaje en esta ocasión al no ver un avance concreto que haga la guía públicamente accesible y que contenga el marco legal local.

CALIFICACIÓN: TIGO LA EMPRESA NO OBTIENE ESTRELLA AL NO CUMPLIR CON NINGUNO DE LOS PARÁMETROS DE EVALUACIÓN.

¿QUIÉN DEFIENDE TUS DATOS?

PANAMÁ 2021

COMPAÑÍA TELEFÓNICA

CLARO

DIGICEL

+MÓVIL

TIGO

POLÍTICA DE PROTECCIÓN DE DATOS



INFORMES DE TRANSPARENCIA



NOTIFICACIÓN AL USUARIO



AUTORIZACIÓN JUDICIAL



DEFENSA DE DERECHOS HUMANOS



SEGURIDAD DIGITAL



GUÍAS PARA REQUERIMIENTO DE INFORMACIÓN PERSONAL ORIENTADAS A LA AUTORIDAD



RESULTADO

2 - 3/4



1 - 1/2



2



3



CONCLUSIÓN

El rol que tienen las empresas de telefonía móvil en la sociedad va más allá de conectar a sus usuarios y facilitar el intercambio de información. Este tiene también un componente humano, de derechos humanos, entre el cual se destaca en nuestro estudio el de la privacidad y la protección de la información personal frente a las solicitudes de información del Estado.

En esta tercera edición del reporte se puede ver un avance positivo en todas las empresas estudiadas e investigadas. Para empezar, casi todas han cumplido con la publicación de su política de privacidad aplicada a sus servicios en el sitio web a diferencia de años anteriores. Inclusive dos empresas se destacaron yendo más allá de la usual publicación de política de privacidad que requiere ser escudriñada en el sitio web para ser vista.

Más Móvil optó por hacer los tópicos de su política de privacidad de forma interrogativa mientras que Claro Panamá optó por agregar dos notables secciones específicas para privacidad en su página principal.

Por otro lado, se nota poco avance en los informes de transparencia. Aunque se nota que los informes de transparencia están siendo considerados por la mitad de las empresas dueñas de marcas panameñas, estos no son publicados o mencionados en el sitio web local. Es positivo que **Claro Panamá** y **Tigo**, a través de **América Móvil** y **Grupo Millicom** respectivamente, contribuyan con datos de Panamá a nivel global, pero falta el paso de hacer accesible esa información a los panameños.

Falta también que se pueda conocer el número específico de solicitudes hechas en Panamá en vez de la región centroamericana. Estos informes educan y permiten al usuario conocer que más allá de interceptación telefónica, las empresas también manejan información como geolocalización en tiempo real, registro de llamadas y de tráfico en el internet. Todas estas pueden ser solicitadas por la autoridad competente.

Se nota un bajo avance con las guías de requerimiento de información personal. Los usuarios panameños desconocen el protocolo interno que emplea la empresa apenas recibe una solicitud de requerimiento. Sin embargo, se puede inferir que el protocolo existe por los compromisos legales internacionales que tienen las cuatro empresas evaluadas como subsidiarias o afiliadas de empresas multinacionales. Un protocolo guía al personal interno de la empresa a responder conforme a la ley los requerimientos de información y disminuye errores. No obstante, el protocolo debe ser publicado y accesible tal como detectamos con **Claro Panamá**. **América Móvil**, la empresa dueña de Claro, posee un interesante documento en el que se ve fácilmente el fundamento legal panameño y algunos de los procedimientos que utilizan ante una solicitud de información.

Se destaca que, durante este año, solo Claro estuvo interesada en mantener una estrecha cooperación en la realización del reporte y en mejorar en sus buenas prácticas. A pesar de múltiples intentos de comunicación por varias vías, fue imposible entablar comunicación con los ejecutivos de **Digicel**, **Tigo** y **Más Móvil**.

Esta poca participación y los resultados obtenidos en esta versión del estudio no reflejan que exista una correlación entre la participación y una mejor puntuación. Sin embargo, la estrecha comunicación ha permitido conocer las preocupaciones de la empresa, del sector y los obstáculos o vacíos legales que enfrentan. Es decir, contextualiza la puntuación y además permite entender que la empresa responde de determinada manera, ya sea porque deba seguir lineamientos marcados por sus empresas dueñas o grupos a los que pertenecen o interpretaciones legales que tienen las autoridades competentes.

Fue producto de esta cooperación que se pudo entender que las empresas no asumen el compromiso de notificación al usuario de solicitudes de información del gobierno por el artículo 10 de la ley 51 de 2009 que requiere que la información suministrada a la autoridad competente es confidencial. Se entiende que las empresas hacen esta interpretación estricta y conservadora porque disminuye considerablemente el riesgo de que sea sancionada.

No obstante, no se comparte esta interpretación porque no es transparente con el usuario y conlleva a que las empresas en ningún momento comuniquen al titular que ocurrió una transferencia de sus datos a la autoridad competente. Por tal razón es que nuestro criterio de notificación al usuario evalúa que la empresa se compromete a comunicar en el primer momento permitido por ley. La empresa que asume este compromiso impulsa un entendimiento menos estricto y más alineado a estándares de derechos humanos en la ley 51 de 2009. Además, la empresa demostraría su disposición de gestionar junto a las autoridades la posibilidad de llevar a cabo la medida clave a la garantía del debido proceso y a un remedio efectivo en caso de solicitudes de datos que incumplan los parámetros de legalidad, necesidad y proporcionalidad.

Con este criterio, se destaca la redacción que utiliza **Más Móvil** en la que le advierte al usuario que la información podrá ser suministrada con o sin aviso. Esto abre la posibilidad de que, a la primera oportunidad legal, el usuario sea notificado.

No obstante, sí se considera un avance esta posibilidad de aviso plasmada en la política de **Más Móvil**, la redacción genérica “**con o sin aviso**”, desprovista de más explicaciones sobre cuándo sí se lo hace con aviso, deja abierto el entendimiento de que la empresa pueda siempre suministrar la información sin aviso.

En otros avances del reporte se identifica que el compromiso de requerimiento de autorización judicial ha sido al menos parcialmente asumido por todas las empresas estudiadas. Por año consecutivo, Tigo por medio de Grupo Millicom, es la única que se ha comprometido a no solo transferir el contenido de informaciones bajo autorización

judicial, sino que está dispuesta a interponer los recursos pertinentes si una solicitud de información no cumple los requisitos legales.

Seguidamente, se observa que la participación en la defensa de derechos humanos es positiva, resaltando que Más Móvil ha continuado publicando su avance con el Pacto Mundial de las Naciones Unidas y Digicel ha sido premiada por sus campañas de interconexión e inclusión social. No obstante, se nota que hay casi nula participación de las empresas en la promoción de privacidad y protección de datos personales a través de campañas, iniciativas legislativas o defensa de los usuarios en los tribunales. De haberlas, las empresas no las promocionan o difunden.

El mismo comportamiento pasivo o inactivo se observa en la promoción de seguridad digital. En casi todas las empresas estudiadas no se educa del tema a los usuarios o público en general cuando la ciberhigiene es esencial para la prevención de incidentes de ciberseguridad. Por tal razón, se destaca que Tigo continuamente publicó del tema en su blog durante el 2021 y posee un protocolo para responder ante filtraciones de datos aunque este no lo publica en su sitio web en Panamá, pero sí a través de Grupo Millicom.

En conclusión, se felicita el avance de las empresas en comparación con otros reportes. Las áreas por mejorar se han concentrado en asumir el compromiso de autorización judicial, de notificar al usuario sobre las solicitudes del gobierno a sus datos y en la difusión y publicación de las políticas que a nivel global implementan las empresas, pero que no terminan acercándose al usuario en Panamá.

IPANDETEC 
CENTROAMÉRICA