

The background features a stylized circuit board pattern. The right side of the image is a solid green vertical band, while the rest of the background is white with light gray circuit traces and nodes. The main title is in large, bold, black capital letters.

# ¿QUIÉN DEFIENDE TUS DATOS?

Panamá 2019



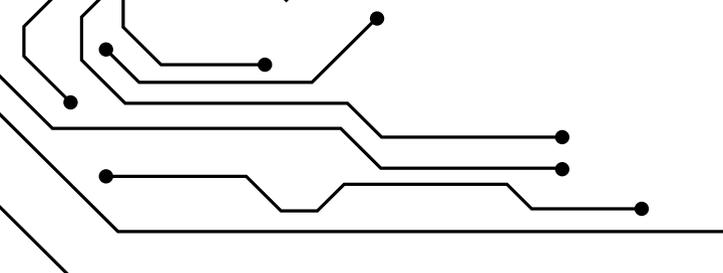
Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0):  
<https://creativecommons.org/licenses/by-sa/4.0/>

Diagramación: Isabel Valladares  
Edición: Raúl Altamar  
Coordinación: Veridiana Alimonti  
Autoría: Abdías Zambrano  
Revisión: Lía Hernández

Agosto 2019.



Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- 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.



# ¿Quién defiende tus datos?

---

## PANAMÁ

Desde 2011 la **Electronic Frontier Foundation (EFF)** publica una evaluación anual titulada Who has your back?, la cual evalúa las políticas de protección de datos de las principales compañías de telecomunicaciones e Internet en Estados Unidos. Su objetivo es el 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 latinoamericana para la realización de proyectos parecidos titulados “¿Quién defiende tus datos?” o ¿Dónde están mis datos? en Argentina, México, Colombia, Brasil, Perú, Paraguay, Chile 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 primer 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 primera edición fueron las cuatro actuales operadoras de telefonía móvil en el mercado de telecomunicaciones panameño: **Cable & Wireless Panamá (Más Móvil), Telefónica Panamá (Movistar), Digicel y Claro Panamá.**

**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 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.

**Movistar Panamá** es la filial panameña de la empresa multinacional española Telefónica

Móviles de España. La compañía opera en el mercado de las telecomunicaciones panameñas desde el 5 de abril de 2005, luego de que adquiriera los activos que mantenía BellSouth en Latinoamérica. Actualmente cuenta con líneas activas y ofrece servicios de línea móvil y servicios corporativos, además de encontrarse en proceso de venta a Millicom International Celular, transacción recientemente aprobada por el ente regulador.

**Digicel Panamá** es una marca perteneciente a Digicel Group, compañía que opera desde el año 2008 en la República de Panamá, ofreciendo servicios de telefonía móvil. En el año 2018 invirtió más de 100 millones de dólares en la incorporación de tecnología LTE Pro.

**Claro Panamá** es una marca de la subsidiaria Claro de la empresa América Móvil. La marca está en Panamá desde marzo de 2009, convirtiéndose en la cuarta operadora de telefonía móvil en el país. Actualmente cuenta con líneas fijas y ofrece los servicios de telefonía móvil, internet móvil y televisión satelital.



# Metodología de evaluación

## Criterios y parámetros

La investigación se desarrolló con el objeto de analizar y evaluar una serie de criterios con perspectiva de Derechos Humanos. Como consecuencia se ha utilizado como base un catálogo de instrumentos, resoluciones e informes elaborados por organismos regionales e internacionales. Los criterios utilizados son desarrollados a continuación:

### 1. Política de protección de datos

5

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. Sin embargo, ante la ausencia de una Ley de Protección de Datos Personales en vigor en Panamá, la Constitución Política<sup>1</sup>, la Ley de Acceso a la Información Pública<sup>2</sup> y la Ley No. 33 de 23 de abril 2013 que crea la Autoridad de Transparencia y Acceso a la Información Pública (ANTAI)<sup>3</sup> son los únicos textos legales que contienen algunos mecanismos de protección de la privacidad y datos personales de los ciudadanos. Sin embargo, existen legislaciones especiales para el tratamiento de datos crediticios, médicos y en el sector de las telecomunicaciones.

<sup>1</sup> Ver enlace de la Constitución Política de Panamá en la sección de referencias.

<sup>2</sup> Ver enlace de la Ley No. 6 de 22 de enero de 2002 en la sección de referencias.

<sup>3</sup> Ver enlace de la Ley No. 33 de 23 de abril de 2013 en la sección de referencias.

La Ley No. 51 de 18 de septiembre de 2009<sup>4</sup>, en su artículo 1, 2 y 6, estipula 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. 81 de 26 de marzo de 2019 “sobre Protección de Datos Personales”<sup>5</sup> fue sancionada y publicada en Gaceta Oficial después de varios años de discusiones en el Órgano Legislativo, con la participación de diferentes sectores de la sociedad. Esta ley finalmente viene a proteger 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. Esta ley es vacatio legis, por lo que entrará en vigencia y obligatorio cumplimiento en el año 2021.

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

<sup>4</sup> Ver enlace de la Ley No. 51 de 18 de septiembre de 2009 en la sección de referencias.

<sup>5</sup> Ver enlace de la Ley No. 81 de 26 de marzo de 2019 en la sección de referencias.

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 evaluamos si las empresas están comprometidas con la protección de los datos personales de sus usuarios, 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.

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.

## Parámetros

- La empresa cuenta con una política de protección de datos 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.

## 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.

### Parámetros

- La empresa publica 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.

### Parámetros

- La empresa se compromete a notificar al usuario sobre la información solicitada en el primer momento permitido por ley.
- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo.

## 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 sólo 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<sup>6</sup>. De igual forma la Ley No. 121 de 31 de diciembre de 2013<sup>7</sup>, 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.

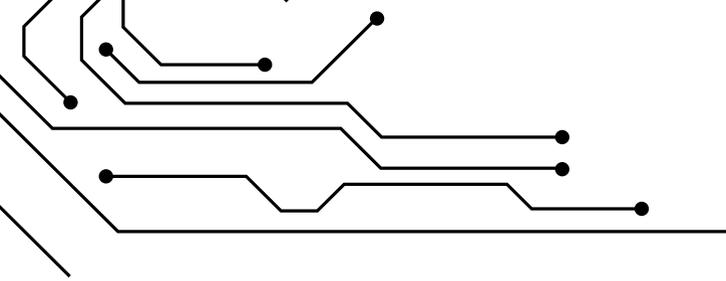
Con relación a las reglas para el acceso a los datos retenidos, la legislación panameña no cumple con los estándares de independencia e imparcialidad mediante el cual la autoridad que autoriza el acceso a los datos no es separada ni independiente de la autoridad que conduce la investigación.

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.

<sup>6</sup> Ver enlace de la Sentencia del Pleno de la Corte Suprema de Justicia de Panamá en la sección de referencias.

<sup>7</sup> Ver enlace de la Ley No. 121 de 31 de diciembre de 2013 en la sección de referencias.



## 5. Defensa de 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<sup>8</sup>. 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.

<sup>6</sup> 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 en la sección de referencia.

Sin embargo, la Ley 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,” 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.

Sin embargo, las brechas de seguridad digital generan que los datos personales de los usuarios sean susceptibles a ataques o incluso robos. Como consecuencia, es importante analizar el compromiso de las empresas con la seguridad de los datos que sus usuarios ingresan en sus sitios web.

### 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.

## 7. Guías para requerimiento de información personal orientadas a la autoridad

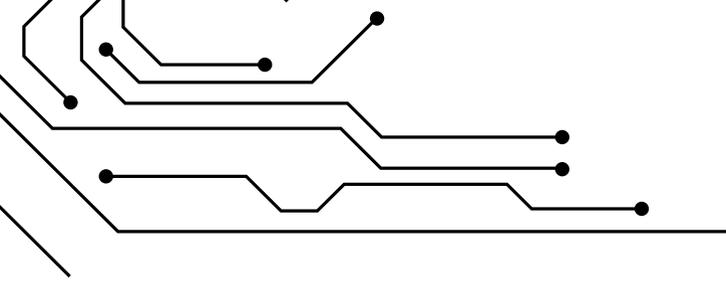
12

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.

Las guías ayudan a los usuarios a comprender qué información está disponible para la aplicación de la ley y sus protecciones, al tiempo que ayudan a las autoridades a mantener las solicitudes limitadas 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.



# 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 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.

### Evaluación

La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.

La empresa obtiene 1/2 estrella si cumple al menos con la mitad de los parámetros de evaluación.

La empresa obtiene 1/4 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 publica 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 1/2 estrella si cumple con dos de los parámetros de evaluación.

La empresa obtiene 1/4 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.
- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo.

### Evaluación

La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.

La empresa obtiene 1/2 estrella si cumple con mitad de 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 mitad de los parámetros de evaluación.

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

## 5. Defensa de 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.

### Evaluación

La empresa obtiene 1 estrella si cumple con todos los parámetros de evaluación.

La empresa obtiene 1/2 estrella si cumple con mitad de los parámetros de evaluación.

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

## 7. Guías para requerimiento de información personal orientadas a la autoridad

### Parámetros

Los parámetros evaluados para ese criterio son:

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

### Evaluación

La empresa obtiene 1 estrella si cumple con el parámetro de evaluación.

La empresa no obtiene estrella si no cumple con el parámetro de evaluación.

# Evaluación de las prácticas

---

## EMPRESA EVALUADA: + Móvil

### 1. Política de protección de datos

- La empresa cuenta con una política de protección de datos publicada en su sitio web.

+Móvil no mantiene una [política de protección de datos](#) en su sitio web y por eso no cumple con ese parámetro. Su empresa tenedora Cable & Wireless Communications sí mantiene una política en una sección denominada [Privacy statement](#) en la parte posterior de su sitio web.

Sin embargo, para calificar en los parámetros de ese criterio es necesario que la política esté disponible en el sitio de la empresa panameña, no solo porque es ese sitio que sus usuarios conocen, sino también porque tales políticas deben tener en cuenta el marco legal del país.

- La política es clara y de fácil acceso a los usuarios.

+Móvil no mantiene una [política de protección de datos en su sitio web](#) y por eso no cumple con ese parámetro.

- La política establece cuáles datos son recopilados.

+Móvil no mantiene una [política de protección de datos en su sitio web](#).

En los contratos de servicio de telefonía móvil celular Banda B no se hace mención a su política de protección de datos. Los contratos no están disponibles en la web.

- La política establece el plazo de retención de los datos de los usuarios.

+Móvil no mantiene una [política de protección de datos en su sitio web](#) y por eso no cumple con ese parámetro.

**CALIFICACIÓN: +Móvil no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**



## 2. Informes de transparencia

- La empresa publica informes de transparencia.  
+Móvil no publica informes de transparencia.
- Los informes están fácilmente accesibles a sus usuarios.  
Los usuarios de +Móvil se enfrentan a la desinformación acerca de las peticiones realizadas por las autoridades competentes, y cuales son aceptadas o rechazadas al no existir la buena práctica de la publicación de un informe con esta información en su sitio web.
- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.  
Los usuarios de +Móvil se enfrentan a la desinformación acerca de las peticiones realizadas por las autoridades competentes, y cuales son aceptadas o rechazadas al no existir la buena práctica de la publicación de un informe con esta información.

**CALIFICACIÓN: +Móvil no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**

## 3. Notificación al usuario

- La empresa se compromete a notificar al usuario sobre la información solicitada en el primer momento permitido por ley.  
La empresa no presenta ningún tipo de compromiso con los clientes para la notificación previa sobre información solicitada por las autoridades.
- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo.  
La empresa no incide en políticas públicas sobre la necesidad de una notificación a priori para que sus usuarios ejerzan el derecho a un remedio efectivo.

**CALIFICACIÓN: +Móvil no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**

## 4. Autorización judicial

- 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.

El sitio de + Móvil no contiene información en ese sentido. En el sitio de su tenedora, Cable & Wireless Communications, hay una sección de [anuncios legales](#) en que se informa en inglés:

“Cable & Wireless Communications permitirá el acceso a toda la información disponible y relevante proporcionada por los usuarios para cumplir con las leyes aplicables y para preservar los derechos y la propiedad de Cable & Wireless Communications. Además, Cable & Wireless Communications puede otorgar acceso a esta información en caso de emergencias”.

Aparte de estar disponible solo en el sitio de la tenedora y no queda claro si también se aplica a las subsidiarias de la empresa, la declaración anterior es genérica y no presenta un compromiso de exigir a las autoridades una autorización judicial antes de suministrar el contenido de las comunicaciones de sus clientes. Tampoco encontramos ese compromiso en su [Privacy statement](#).

- La empresa se compromete a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales.

+Móvil no proporciona datos de este parámetro en su página web. En cuanto a la sección de anuncios legales de su tenedora Cable & Wireless Communications, la declaración anterior no expresa el compromiso evaluado y tampoco está claro si sería aplicable a la empresa panameña. Finalmente, no se ha encontrado el compromiso valorado en el [Privacy statement](#) ya referido.

**CALIFICACIÓN: +Móvil no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**



## 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 ninguna iniciativa relacionada a este parámetro. En su página web y en sus redes sociales (Twitter e Instagram) notamos la ausencia de este tipo de campañas o actividades.

- 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 ninguna iniciativa relacionada a este parámetro. En su página web y en sus redes sociales (Twitter e Instagram) notamos la ausencia de este tipo de campañas o actividades.

- La empresa participa en mecanismos o procesos multisectoriales para la promoción de los Derechos Humanos en el marco de sus responsabilidades empresariales.

Cable and Wireless Panamá es miembro del Pacto Global de las Naciones Unidas desde el año 2006. El fin de este pacto es transformar el mercado global, potenciando un sector privado sostenible y responsable sobre la base de 10 principios en áreas relacionadas con los derechos humanos, el trabajo, el medio ambiente y la corrupción. Igualmente, este Pacto anexa los 17 Objetivos del Desarrollo Sostenible (ODS) de las Naciones Unidas de la Agenda 2030.

Al momento de analizar el informe de la Red del Pacto Global 2018, se informa de un error en la plataforma que imposibilita ver los avances obtenidos ese año. El [informe del año 2017](#) muestra su compromiso con la educación, la libertad de expresión, la salud, entre otros derechos como los laborales.

**CALIFICACIÓN: +Móvil recibe ¼ de estrella al cumplir con uno de los parámetros de este criterio.**

## 6. Seguridad digital

- La empresa utiliza el protocolo HTTPS para navegar [en su página web](#).

La empresa hace uso del protocolo HTTPS 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 en su página web a la hora de realizar [pagos en línea](#).

**CALIFICACIÓN: +Móvil recibe una estrella al cumplir con todos los parámetros de este criterio.**

## 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.

La empresa no mantiene este tipo de guía en su página web.

**CALIFICACIÓN: +Móvil no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**

# EMPRESA EVALUADA: Movistar

## 1. Política de protección de datos

- La empresa cuenta con una política de protección de datos publicada en su sitio web.

La empresa Movistar no mantiene una política de protección de datos en su sitio web al momento de realizar nuestra revisión.

Telefónica, dueña de Movistar Panamá, mantiene en [su sitio web global](#) un Centro de Privacidad y Seguridad. En la [sección de Privacidad](#) se encuentran mayores detalles de la política de protección de datos de la empresa.

Sin embargo, para calificar en los parámetros de ese criterio es necesario que la política esté disponible en el sitio de la empresa panameña, no solo porque es ese sitio que sus usuarios conocen, sino también porque tales políticas deben tener en cuenta el marco legal del país.

Cabe destacar que la empresa al momento de contestar esta pregunta mencionó que actualmente se encuentran en un proceso de actualización del texto de la política de protección de datos que mantenían anteriormente en su sitio web. Sin embargo, para este informe solo se puede considerar la información públicamente disponible en el momento de su finalización.

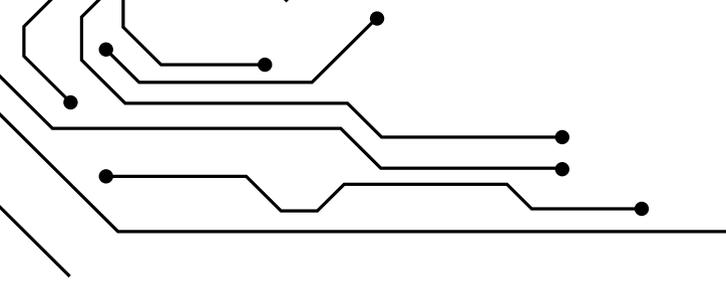
- La política es clara y de fácil acceso a los usuarios.  
Movistar no tiene una política de protección de datos en su sitio web.

- La política establece cuáles datos son recopilados.  
Movistar Panamá no mantiene una política de protección de datos en su sitio web y por eso no cumple con ese parámetro.

- La política establece el plazo de retención de los datos de los usuarios.

Movistar Panamá no mantiene una política de protección de datos en su sitio web y por eso no cumple con ese parámetro.

**CALIFICACIÓN: Movistar no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**



## 2. Informes de transparencia

- La empresa publica informes de transparencia.

La empresa Movistar, mediante su conglomerado Telefónica, publica informes de transparencia de forma anual. [El Informe de Transparencia de las Comunicaciones](#) por cada país registra los datos de interceptación legal, acceso a metadatos, bloqueo y filtrado de determinados contenidos y suspensiones geográficas o temporales del servicio.

Importante destacar que este informe declara que no ha recibido del año 2013 a la fecha requerimientos para el bloqueo y filtrado de determinados contenidos; y en cuanto a suspensiones geográficas o temporales de servicio solo una (1) petición en el año 2013.

- Los informes están fácilmente accesibles a sus usuarios.

El informe no es de fácil acceso para sus usuarios. El usuario debe dirigirse a la parte posterior extrema de la página web de Movistar, sección Sobre Telefónica y dirigirse a Telefónica Global. Posteriormente debe dirigirse a la sección de Negocio Responsable para finalmente elegir la sección de Informe de Transparencia. El informe debería estar disponible directamente en el sitio web de la empresa Movistar Panamá.

- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.

[El informe de transparencia](#) de la empresa Movistar separa las solicitudes de interceptación del contenido de la comunicaciones de las solicitudes de acceso a metadatos. Para cada una de las categorías la empresa brinda informaciones sobre el contexto legal, las autoridades competentes, el número de requerimientos recibidos y rechazados.

Se hace la salvedad que el sistema de registro no se efectúa por cliente afectado, sino por número de requerimientos.

En el año 2017 se atendieron 532 peticiones de interceptación legal y 10082 de acceso a metadatos. Es importante destacar que desde el año 2013 a la fecha, las solicitudes de interceptación legal han ido creciendo, mientras que las solicitudes de acceso a metadatos registraron un denotado descenso en el año 2016 con nuevo crecimiento en 2017.

La empresa Movistar no ha rechazado ningún requerimiento de entrega según el Informe de Transparencia de las Comunicaciones 2018. Sin embargo, en el [año 2016](#) fueron rechazadas 2997 peticiones de acceso a metadatos. Cabe destacar que no se aclaran los motivos de rechazo de las peticiones.

**CALIFICACIÓN: Movistar recibe ½ estrella al cumplir con dos de los parámetros de este criterio.**

### 3. Notificación al usuario

- La empresa se compromete a notificar al usuario sobre la información solicitada en el primer momento permitido por ley. La empresa no mantiene este tipo de compromiso en su Política de Privacidad o documento parecido en su sitio web o redes sociales.

- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo.

La empresa no cumple con este parámetro.

**CALIFICACIÓN: Movistar no recibe estrella al no cumplir con ninguno de los parámetros de este criterio.**

## 4. Autorización judicial

- 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.

No se logró encontrar ese compromiso público en los contratos, políticas o términos de servicio de Movistar Panamá. No obstante, el informe de transparencia de Telefónica señala la legislación aplicable y las autoridades competentes para la interceptación de las comunicaciones en Panamá.

De acuerdo con ellos, al menos en ese procedimiento, una autorización judicial previa es necesaria. Por esa razón, ese parámetro se considera parcialmente atendido.

- La empresa se compromete a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales.

En su [política global](#), aplicable a sus subsidiarias, Telefónica afirma que está sujeta a los entornos jurídicos en los países que opera, por lo que debe, en circunstancias excepcionales y siempre expresamente previstas en las leyes nacionales, dar respuesta a requerimientos de las autoridades competentes relativos a determinada información sobre las comunicaciones de sus clientes y/o usuarios. Afirma también que implementa un procedimiento global estricto, el cual garantiza tanto el cumplimiento de obligaciones en materia de colaboración con la administración de Justicia y autoridades competentes como la protección de los derechos de Privacidad y Libertad de Expresión de los afectados. Esa política se complementa con el [Procedimiento Global de requerimientos por parte de las autoridades competentes](#), que presenta principios y un resumen del procedimiento por el cual los requerimientos son aceptados o rechazados.

Aunque los documentos brinden informaciones y compromisos importantes, ellos se refieren a políticas globales de la empresa por lo que no dejan claro cómo se adaptan y aplican al marco legal del país. Por ende, ese parámetro se considera parcialmente atendido.

**CALIFICACIÓN: Movistar recibe 1/2 de estrella al cumplir parcialmente con los parámetros de este criterio.**



## 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 evidencia en redes sociales ([Twitter](#) e [Instagram](#)) o en su sitio web que promueva la importancia de la privacidad y protección de datos en sus usuarios a través de campañas y actividades.

- 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 evidencia en redes sociales ([Twitter](#) e [Instagram](#)) o en su sitio web que promueva iniciativas de ley, litigio estratégico, o de políticas públicas para la privacidad y protección de datos en sus usuarios.

- La empresa participa en mecanismos o procesos multisectoriales para la promoción de los Derechos Humanos en el marco de sus responsabilidades empresariales.

En el año 2016, Telefónica Movistar comenzó a formar parte de la [Iniciativa de Red Global](#) (GNI, por sus siglas en inglés), una red multisectorial que tiene como objetivo promover la privacidad, la libertad de expresión y la colaboración entre distintos actores del sector. La pertenencia a GNI obliga a Telefónica a suscribir una serie de principios que demuestran al menos una intención inicial por la protección de los derechos de los usuarios de internet.

**CALIFICACIÓN: Movistar recibe ¼ de estrella al cumplir con al menos uno de los parámetros de este criterio.**

## 6. Seguridad digital

- La empresa utiliza el protocolo HTTPS para navegar en su página web.

La empresa hace uso del protocolo HTTPS [en su página web](#).

- La empresa utiliza el protocolo HTTPS inclusive a la hora de hacer pagos en línea.

La empresa usa el protocolo HTTPS en su sección de [pagos en línea](#).

**CALIFICACIÓN: Movistar recibe una 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.

Movistar Panamá no publica una guía para el requerimiento de la información personal de sus clientes por parte de la autoridad. Sin embargo, su empresa madre, Telefónica, lo hace y publica en su página web el [Procedimiento Global de requerimientos por parte de las autoridades competentes](#), aprobado en 2016. Este procedimiento se aplica a todas las compañías de Telefónica en los países en los que opera.

Aunque sea importante por los principios que postula y por presentar el flujo observado por la empresa al entregar datos a las autoridades de investigación, no es posible saber cómo la empresa lo aplica en Panamá, teniendo en cuenta su contexto legal. Esa comprensión de manera detallada es lo más relevante para ese parámetro. Por ende, el parámetro recibe una calificación apenas parcial.

**CALIFICACIÓN: Movistar recibe 1/4 de estrella al cumplir parcialmente con los parámetros de evaluación.**

# EMPRESA EVALUADA: DIGICEL

## 1. Política de protección de datos

- La empresa cuenta con una política de protección de datos y está disponible en su sitio web.

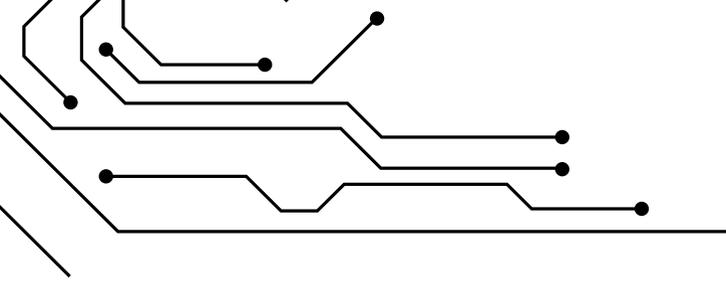
Digicel tiene su [Política de Privacidad](#) en su sitio web. Cabe mencionar que es la única operadora móvil de las analizadas que mantiene su política fácil de encontrar. Puedes ingresar por la sección de Términos y Condiciones o acudir a la parte inferior del sitio web sección Política de Privacidad.

- La política es clara y de fácil acceso a los usuarios. Digicel es la única operadora móvil de las analizadas que mantiene su política fácil de encontrar. Se puede ingresar por la sección de Términos y Condiciones o acudir a la parte inferior del sitio web sección Política de Privacidad. Igualmente es bastante clara para el usuario.

- La política establece cuáles datos son recopilados. La [política de protección de datos](#) de Digicel determina que los datos que la empresa puede recopilar incluyen a modo enunciativo, pero no se limitan a:

1. Información de contacto (como nombre, dirección, dirección de correo electrónico y número de teléfono).
  2. Información de identificación (como número de pasaporte, número de registro impositivo o número de seguro social, licencia de conducir, fecha de nacimiento).
  3. Información demográfica (como rango de edad, estado civil, género).
  4. Fotografías como las que puede enviar para concursos o competencias con premios.
  5. Información específica sobre productos (como preferencia, grupo cerrado de usuarios [CUG], familiares o amigos que eliges incluir en su plan de servicio, límite de crédito).
  6. Información bancaria (como transacciones bancarias de débito directas o de pago de facturas relacionadas).
  7. 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. La [política de protección de datos](#) de Digicel establece que retiene los datos de sus usuarios todo el tiempo necesario, mientras que otros datos serán retenidos por más tiempo por mandato de la Ley. Esta explicación por parte de la compañía deja al usuario confundido al no ser clara y específica.

**CALIFICACIÓN: Digicel recibe 1/2 estrella al cumplir con tres de los parámetros de evaluación.**



## 2. Informes de transparencia

- La empresa pública informes de transparencia  
Digicel no publica informes de transparencia en su página web.
- Los informes están fácilmente accesibles a sus usuarios.  
Los usuarios de Digicel se enfrentan a la desinformación acerca de las peticiones realizadas por las autoridades competentes, las cuales son aceptadas o rechazadas al no existir la buena práctica de la publicación de un informe de transparencia con esta información.
- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.  
Los usuarios de Digicel se enfrentan a la desinformación acerca de las peticiones realizadas por las autoridades competentes, las cuales son aceptadas o rechazadas al no existir la buena práctica de la publicación de un informe de transparencia con esta información.

**CALIFICACIÓN: Digicel no recibe estrella al no cumplir con los parámetros de evaluación.**

## 3. Notificación al usuario

- La empresa se compromete a notificar sobre la información solicitada en el primer momento permitido por ley.  
La empresa no mantiene este tipo de compromiso con sus clientes.
- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo.  
La empresa no cumple este parámetro.

**CALIFICACIÓN: Digicel no recibe estrella al no cumplir con 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 información de manera pública. La empresa se limita a afirmar que comparte la información personal de los usuarios “a requerimiento de autoridad competente, para fines investigativos y 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 no mantiene este tipo de información de manera pública. La empresa se limita a afirmar que comparte la información personal de los usuarios “a requerimiento de autoridad competente, para fines investigativos y expresamente configurados dentro del marco legal”.

**CALIFICACIÓN: Digicel no recibe estrella al no cumplir con 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 mantiene información sobre su participación en la promoción de la importancia de la privacidad y protección de datos de sus usuarios en su [página web](#). En la web de la empresa existe la sección de Noticias y comunidad, donde tampoco se visualiza esta información.

Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

- 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 mantiene información sobre su participación en la promoción de iniciativas de ley, litigio estratégico, o de políticas públicas para la privacidad y protección de datos de sus usuarios.

Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

- 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 mantiene información sobre su participación en mecanismos o procesos multisectoriales para la promoción de los Derechos Humanos en el marco de su responsabilidad empresarial en su página web.

Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

**CALIFICACIÓN: Digicel no recibe estrella al no cumplir con los parámetros de evaluación.**

## 6. Seguridad digital

- La empresa utiliza el protocolo HTTPS para navegar en su página web.

La empresa Digicel usa el protocolo HTTPS en [su sitio web](#).

- La empresa utiliza el protocolo HTTPS inclusive a la hora de hacer pagos en línea.

El [protocolo HTTPS](#) se mantiene a la hora de hacer recargas y pagos dentro del sitio web.

**CALIFICACIÓN: Digicel recibe una 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.

La empresa no mantiene este tipo de guía ni alguna que se le parezca en su página web.

**CALIFICACIÓN: Digicel no recibe estrella al no cumplir con los parámetros de evaluación.**



# EMPRESA EVALUADA: CLARO

## 1. Política de protección de datos

- La empresa cuenta con una política de protección de datos publicada en su sitio web.

La empresa de telefonía móvil Claro mantiene una [política de privacidad](#) en su página web. Pero su contenido parece enfocarse apenas en las informaciones personales recabadas de los usuarios en el sitio web de la empresa. Es una política de privacidad relacionada a la interacción del usuario con el sitio de Claro, no las reglas generales sobre ese tema aplicables por la empresa en el conjunto de su prestación de servicio. Por eso, ella no será considerada para calificar en ese parámetro.

A su vez, la empresa tenedora de Claro, América Móvil, publica en su página web [la política global de protección de datos](#) aplicable a todas sus subsidiarias. Sin embargo, para la calificación en los parámetros de ese criterio solo consideramos la política disponible en el sitio de la empresa panameña, porque es el sitio que sus usuarios panameños conocen y porque tales políticas deben tener en cuenta el marco legal del país.

- La política es clara y de fácil acceso a los usuarios.

La política disponible en el sitio de Claro no fue considerada adecuada para el análisis de ese parámetro, ya que no se refiere a la prestación de servicio por la empresa de manera general. Está enfocada apenas en las informaciones recabadas por las interacciones del usuario con el sitio de Claro Panamá.

- La política establece cuáles datos son recopilados.

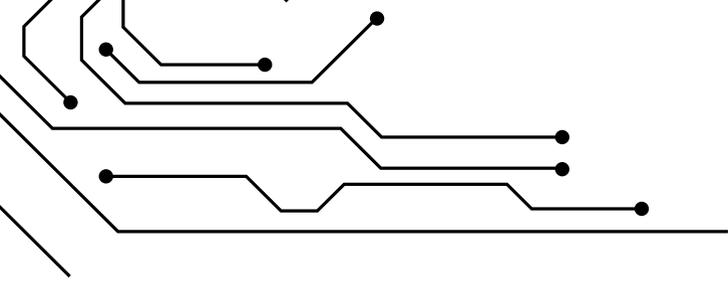
La política disponible en el sitio de Claro no fue considerada adecuada para el análisis de ese parámetro, ya que no se refiere a la prestación de servicio por la empresa de manera general. Está enfocada apenas en las informaciones recabadas por

las interacciones del usuario con el sitio de Claro Panamá.

- La política establece el plazo de retención de los datos de los usuarios.

La política disponible en el sitio de Claro no fue considerada adecuada para el análisis de ese parámetro, ya que no se refiere a la prestación de servicio por la empresa de manera general. Está enfocada apenas en las informaciones recabadas por las interacciones del usuario con el sitio de Claro Panamá.

**CALIFICACIÓN: Claro no recibe estrella al no cumplir con los parámetros de evaluación.**



## 2. Informes de transparencia

- La empresa publica informes de transparencia.

La empresa Claro afirma publicar informes de transparencia anualmente bajo su empresa matriz América Móvil. Estos informes se llaman [Informe de Sustentabilidad](#). Sin embargo, al momento de investigar el informe de sustentabilidad del año 2018 no se encontró información detallada sobre los distintos aspectos que un informe de transparencia debe contener.

- Los informes están fácilmente accesibles a sus usuarios.

Claro Panamá, mediante su empresa matriz América Móvil, publica anualmente un [Informe de Sustentabilidad](#), pero este documento no brinda informaciones sobre las solicitudes de acceso a datos de usuarios por autoridades de investigación y, por lo tanto, no atiende a los requisitos evaluados en este criterio.

- Los informes contienen datos relacionados al número de solicitudes recibidas, cumplidas y el tipo de solicitud.

Los usuarios de Claro se enfrentan a la desinformación acerca de las peticiones realizadas por las autoridades competentes, las cuales son aceptadas o rechazadas al no existir la buena práctica de detallar en el informe el número de solicitudes recibidas, cumplidas y el tipo de solicitud.

**CALIFICACIÓN: Claro no recibe estrella al no cumplir con los 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 sección de Privacidad y uso de la información personal en el sitio web de Claro no presenta un compromiso de la empresa con sus usuarios de proporcionar una notificación previa sobre una solicitud realizada por una autoridad competente para el pleno ejercicio del derecho de defensa.
- La empresa incide en políticas públicas sobre la necesidad de una notificación a priori para que el usuario pueda ejercer su derecho a un remedio efectivo. La empresa no cumple este requisito.

**CALIFICACIÓN: Claro no recibe estrella al no cumplir con los parámetros de evaluación.**

## 4. Autorización judicial

- 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 no hace mención en su página web o en su política de privacidad de la exigencia de una autorización judicial previa a las autoridades judiciales para proporcionarles el contenido de las comunicaciones de sus usuarios. Tampoco lo menciona en su contrato.

Sin embargo, la empresa América Móvil, dueña de Claro Panamá, hace mención en su [Política de Privacidad](#), de observancia obligatoria a sus subsidiarias, que nadie puede escuchar o monitorear ninguna conversación, transmisión de datos u otra forma de comunicación, ni revelar su existencia o contenido, salvo por orden escrita debidamente fundada y motivada de las autoridades competentes. Aunque sea un compromiso importante, ello se encuentra en una política global de la empresa por lo que no deja claro cómo se adapta y se aplica al marco legal del país. Por ende, ese parámetro se considera parcialmente atendido.

- La empresa se compromete a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales. La empresa no se compromete en su sitio web o en su política de privacidad a rechazar requerimientos de entrega de información en casos que incumplan requisitos legales.

Sin embargo, en su política global, América Móvil establece que “se podrá realizar la entrega de información de los particulares, realizar la geolocalización de una línea de comunicación móvil, bloquearla, restringirla o llevar un registro y control de las comunicaciones cuando dichas acciones sean requeridas en términos de la legislación que resulten aplicables, debiendo constar siempre por escrito, mediante oficio emitido y suscrito por una autoridad competente y cuyo requerimiento esté debidamente fundado y motivado en términos de ley”.

Aunque la disposición presente un compromiso importante, la consecuencia inmediata de rechazo no está tan evidente. Además, ello se encuentra en una política global de la empresa por lo que no deja claro cómo se adapta y se aplica al marco legal del país.

**CALIFICACIÓN: Claro recibe 1/2 estrella al cumplir parcialmente con 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 mantiene información sobre su participación en la promoción de la importancia de la privacidad y protección de datos de sus usuarios. En su [página web](#), no mantienen una sección de prensa; su sección de Responsabilidad Social no es actualizada desde el 2013.

Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

- 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 mantiene información sobre su participación en la promoción de iniciativas de ley, litigio estratégico, o de políticas públicas para la privacidad y protección de datos de sus usuarios. En su página web, no mantienen una sección de prensa; su sección de Responsabilidad Social no es actualizada desde el 2013.

Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

- 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 mantiene información sobre su participación en mecanismos o procesos multisectoriales para la promoción de los Derechos Humanos en el marco de su responsabilidad empresarial. En su página web, no mantienen una sección de prensa; su sección de Responsabilidad Social no es actualizada desde el 2013. Por otro lado, en redes sociales ([Twitter](#) e [Instagram](#)) tampoco se puede visualizar campañas o actividades referente a este tema.

Sin embargo, América Móvil, su empresa tenedora, es parte del [Pacto Mundial de las Naciones Unidas desde el año 2016](#).

**CALIFICACIÓN: Claro 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

El [sitio web de Claro](#) mantiene el protocolo HTTPS.

- La empresa utiliza el protocolo HTTPS inclusive a la hora de hacer pagos en línea.

El sitio de Claro Panamá permite crear un perfil para hacer pagos en línea y otras gestiones. Sin embargo cuando se utiliza [el perfil de usuario](#) y se ingresa al CAC Virtual o Centro Virtual de Atención al Cliente Claro no se utiliza el protocolo HTTPS, dejando en vulnerabilidad los datos de los clientes.

**CALIFICACIÓN: Claro recibe ½ estrella al cumplir con la mitad de los parámetros de evaluación.**

38

## 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.

La empresa no mantiene una guía para el requerimiento de la información personal de sus clientes por parte de la autoridad en su página web. Tampoco hace mención de su existencia en su contrato.

**CALIFICACIÓN: Claro no recibe estrella al no cumplir con los parámetros de evaluación.**



# ¿QUIÉN DEFIENDE TUS DATOS?

Panamá 2019

Compañía Telefónica	+MÓVIL	MOVISTAR	DIGICEL	CLARO
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				
<b>RESULTADO</b>	<b>1 1/4</b> 	<b>2 1/2</b> 	<b>1 1/2</b> 	<b>1 1/4</b> 

# Conclusiones

---

Después de analizar las políticas de privacidad de las distintas compañías de telefonía celular en Panamá y sus políticas de protección de los datos de sus clientes, llegamos a la conclusión que Panamá es uno de los países donde las compañías dejan en indefensión y sin protección a sus usuarios, sin mencionar la poca legislación de protección de datos personales en el país.

En el año 2021 se espera la entrada en vigencia de la primera ley que protege los datos personales de los ciudadanos en Panamá y su reglamentación.

La principal conclusión fue que a la industria de las telecomunicaciones le preocupaba poco o muy poco la protección de datos y la privacidad de los usuarios, a partir de informaciones disponibles en los sitios de las empresas de Panamá.

Nuestra segunda conclusión fue que las empresas mejor evaluadas en su mayoría son de capital extranjero y responden a estándares de privacidad y protección de datos personales de otras jurisdicciones con mayor preocupación en la privacidad de los usuarios.

Destacamos que las únicas empresas interesadas en cooperar con el estudio y con profundo interés de mejorar fueron Movistar y Claro. Al cierre de esta edición se mantenía en espera de respuesta +Móvil y Digicel.

Vemos de forma preocupante que ninguna de las empresas calificadas tiene a disposición de sus clientes y al público en general el contrato de servicios, ni una guía para el requerimiento de la información personal de sus clientes por parte de la autoridad panameña (la tenedora de Movistar mantiene una guía global general); tampoco se comprometen a avisarle a sus clientes si las autoridades les están investigando y solicitando acceso a datos de sus comunicaciones privadas.

Con eso les niegan la oportunidad de desafiar las solicitudes recibidas, así como comprometen el derecho del usuario de buscar reparación en caso de medidas excesivas. Solamente Movistar y +Móvil pertenecen a alguna coalición internacional garantista de los derechos humanos.

Solo Movistar publica anualmente un informe de transparencia y a pesar que todas tienen una política de protección de datos, muy pocas se refieren a la operación de la empresa en Panamá, incluso una se mantiene en otro idioma diferente al oficial en el país. De hecho, solo Digicel tiene una política de protección de datos para Panamá.

+Móvil y Movistar tienen las políticas globales de sus tenedoras, que no cuentan con enlace en la página web de la empresa panameña; Claro tiene la política global de América Móvil y una política local solo para los datos recabados en el sitio de la empresa.

De igual forma, tanto Movistar como Claro tienen compromisos importantes en las políticas de sus sedes globales sobre la autorización judicial y pedidos de información por parte de la autoridad, las cuales deberían ser incluidas en las políticas nacionales de acuerdo con las normas de Panamá.

Un punto en común que tuvieron todas las empresas fue su buena calificación en el uso de protocolo HTTPS, al todas hacer uso del mismo en sus sitios web. No obstante, Claro no utiliza el protocolo HTTPS en su Centro Virtual de Atención al Cliente, donde el usuario puede hacer pagos y otras gestiones.

Por lo tanto, instamos a las empresas panameñas de telefonía móvil a instaurar mejores medidas de protección de datos y hacerlas accesibles en sus sitios al público en general, iniciar la publicación de un informe de transparencia anual en el que se detalle la cantidad de requerimientos y clientes afectados por solicitudes de interceptación legal y acceso a metadatos recibidos por parte de la autoridad competente, y cuántos de ellos fueron rechazados y sus causas.

Este informe debería contener un apartado para establecer cuántas de las solicitudes aceptadas por la compañía resultaron en una notificación al usuario.

Las empresas deben también notificar a sus usuarios sobre los pedidos de acceso a datos de sus comunicaciones en el primer momento que la ley lo permita. Es un derecho de los usuarios a conocer que la información de sus comunicaciones fue entregada a la autoridad competente en el marco de una investigación penal, para que el usuario pueda ejercer su derecho de defensa en caso que la solicitud sea ilegal o desproporcionada.

Por último, instamos a las empresas que incidan en distintas iniciativas parlamentarias y políticas públicas que garanticen la defensa de los derechos humanos, específicamente en el derecho a la privacidad y la protección de datos personales.

Las empresas deben iniciar el proceso de creación de una guía para el requerimiento de información de carácter personal de sus usuarios por parte de las autoridades, a fin de brindar un mejor servicio, mostrando una genuina preocupación por los derechos de sus clientes.

Las recomendaciones y observaciones antes manifestadas a las empresas deben ser exigidas activamente por sus clientes. IPANDETEC seguirá trabajando al lado de los usuarios para que las empresas mejoren sus prácticas y defiendan nuestra privacidad. Hay mucho por avanzar.



## Referencias:

---

- 1. Constitución Política de la República de Panamá.**  
Disponible en: <https://www.constitucion.gob.pa/tmp/file/1/Texto-editado-por-la-Asamblea-Nacional.pdf>
- 2. 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>
- 3. 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>
- 4. 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>
- 5. 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](https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/72148.pdf)
- 6. 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](https://vlex.com.pa/vid/solicitud-pleno-suprema-sala-198250047?_ga=2.243494855.370176048.1551118645-1758111339.1550249042)
- 7. 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](https://www.gacetaoficial.gob.pa/pdfTemp/27446_B/44985.pdf)
- 8. Corte Interamericana de Derechos Humanos. Caso Escher y otros vs. Brasil.**  
Disponible en: [http://www.corteidh.or.cr/docs/casos/articulos/seriec\\_200\\_esp1.pdf](http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf)



**IPANDETEC**  
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS