# ¿Dónde Están Mis Datos?

NOVIEMBRE 2016

POR: LAURA MORA
CAROLINA BOTERO

Fundación Karisma
www.karisma.org.co

“En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesible, es decir, tienen un formato electrónico diseñado para que su contenido pueda ser leído por el mayor número de personas posible, incluidas las que tienen algun tipo de discapacidad o de dificultada para la lectura y comprensión. Más información sobre el tema: http://www.documentoaccesible.com/#que-es

**Autoras:**
Laura Mora
Carolina Botero

**Coordinación editorial:**
Pilar Sáenz
Nathaly Espitia Díaz

**Portada:**
Mauricio Isaza

**Diagramación:**
Rubén Urriago

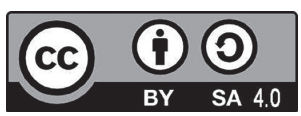
**Consulta esta investigación en línea en**
**dondeestanmisdatos.info**

**¿Dónde están mis datos?**

Es un proyecto de
Fundación Karisma


con el apoyo
de la EFF

Noviembre 2016



# Tabla de Contenido

# INTRODUCCIÓN

La red hace parte de nuestra cotidianidad, además de que moviliza una enorme cantidad de información, tanto la que es de conocimiento público, aspectos de nuestra vida personal que hacemos públicas —fotos o videos—, hasta datos muy privados —movimientos financieros o cuándo y con quién hablamos—. Todo esto hace parte de lo que allí se registra. Internet es una enorme base de datos y quizá todos debamos preguntarnos ¿Dónde están mis datos?

Cuando usamos el celular o el computador para acceder a internet para chatear, buscar noticias, leer correos electrónicos, entre otras posibilidades infinitas, no solo estamos interactuando con lo que buscamos o con quien conversamos. En este tejido que es la red, nuestros datos van pasando por las manos de muchos intermediarios que hacen parte del proceso. Los proveedores de servicios de internet (en adelante, ISP, por sus siglas en inglés) son intermediarios en este proceso y tienen una gran responsabilidad sobre los datos que transitan por sus redes. ¿Te has preguntado cuál es su papel en la garantía de nuestros derechos?

Cada día somos más quienes estamos en la red y establecemos diferentes relaciones con los ISP. En Colombia, de acuerdo con el *Boletín trimestral de las TIC - Cifras primer trimestre de 2016*, el número de personas con suscripción a internet está en aumento.

Al cierre del primer trimestre del año 2016, el número total de suscriptores [sic] a internet en el país alcanzó los 13.707.151, cifra compuesta por suscriptores a Internet fijo y móvil, lo que representa un índice de penetración del 28,1%, y un aumento de 1,5 puntos porcentuales con relación al índice de penetración del cuarto trimestre de 2015.[1]

Esta cifra se queda corta, pues, además de quienes tienen una suscripción a internet, en el país las personas también acceden a la red en espacios como universidades, lugares de trabajo, bibliotecas y otros como los café internet. Incluso es importante decir que en la cifra de personas con suscripción a internet no se encuentran quienes acceden a través de planes temporales para móviles (planes prepago). De acuerdo al Boletín, los principales ISP en Colombia, tanto para el acceso a internet residencial como para la internet móvil, son Claro (Telmex Colombia - COMCEL S.A.) Tigo-UNE

(Colombia Móvil S.A. E.S.P.), Telefónica-Movistar (Colombia Telecomunicaciones S.A. E.S.P) y ETB. Es por esta razón que estas empresas han sido incluidas en esta evaluación, además de Directv.

Siguiendo con la línea del primer informe ¿Dónde están mis datos?, publicado en 2015, Fundación Karisma analizó por segundo año consecutivo y desde una aproximación de derechos humanos las políticas de estos cinco ISP. El análisis buscó evaluar qué tanto estas empresas defienden nuestros derechos y cómo protegen nuestros datos. Con este propósito, Karisma buscó y analizó la información que los ISP comparten públicamente para establecer su compromiso con la transparencia, el debido proceso, la protección de datos, la intimidad y la libertad de expresión.

En 2016, Karisma ajustó los criterios de la evaluación teniendo en cuenta lo que aprendimos en el desarrollo y divulgación del primer informe. La revisión se alimentó también de las experiencias de otros proyectos similares que surgieron en este período, a saber, ¿Quién defiende tus datos? por la Red en Defensa de los Derechos Digitales (R3D)[2] en México, Hiperderecho[3] en Perú e InternetLab[4] en Brasil, además del informe que sirvió de base en 2015: *Who has your back?* [5] de la Electronic Frontier Foundation (EFF).

El objetivo de este ejercicio es visibilizar la importancia de las buenas prácticas en la gestión de los datos para la protección de nuestros derechos más allá de las obligaciones legales. La EFF ha podido monitorear la transformación positiva que se ha dado a través de los años entre las empresas que ha evaluado. En Karisma, con tan solo dos informes podemos decir que el efecto positivo también se va dando en Colombia. En 2016, los resultados muestran que hay interés de los ISP evaluados por mejorar sus prácticas. Sin embargo, queda mucho camino por recorrer.

Los informes anuales de ¿Dónde están mis datos? se presentan en una forma gráfica. En nuestro caso, los resultados se materializan en *baterías*. Una batería llena significa que el ISP cumplió con el criterio; mientras que una a media carga significa que la información encontrada era parcial o que no respondía completamente a los postulados del criterio. En algunos casos, se otorgó *un cuarto de carga* como reconocimiento al desarrollo de buenas prácticas en sus políticas. Cuando la batería está completamente descargada significa que no había información o la que estaba disponible no respondía a lo que se estaba planteando.

Los resultados de la evaluación de 2016 se pueden detallar de la siguiente manera:

## Sobre transparencia

Los ISP en Colombia no producen informes de transparencia que permitan conocer la forma cómo comparten con terceros, incluido el Gobierno Nacional, los datos de las personas ni su rol en el bloqueo de contenidos o cancelaciones de cuentas que pueden afectar la libertad de expresión de quienes usan sus servicios. Establecimos que los ISP en el país relacionan la transparencia fundamentalmente con aspectos económicos y financieros con el fin de evitar actos de corrupción. Es en estos temas que las empresas hacen informes de transparencia.

En el país no se asocia la transparencia corporativa con temas como la protección a la intimidad, al habeas data o a la libertad de expresión de quienes contratan sus servicios. Sin embargo, mientras en 2015 ninguna de las empresas obtuvo reconocimiento, en 2016 la ETB recibió *un cuarto de carga* en reconocimiento a su compromiso para trabajar en el tema. ETB creó un espacio en su sitio web donde publican información centralizada sobre temas como el proceso legal de bloqueo de contenidos de internet y de interceptación de comunicaciones y de solicitud de información de las personas usuarias por parte de las autoridades, aunque no indican lo que ha sucedido con esto durante un período determinado. Por ejemplo, pese a que dicen cómo debe ser legalmente una solicitud de información de datos personales, no informan cuántas solicitudes de información sobre quienes contratan sus servicios han recibido durante el último año. En todo caso, el sitio facilita el acceso a información de la empresa para consulta de cualquier persona. Eso es una buena práctica a resaltar.

## Sobre protección de datos

Las políticas de protección de datos de los ISP evaluados están públicas en sus sitios web y, en general, siguen buenas prácticas ya desarrolladas en internet. Por ejemplo, sus documentos de políticas se encuentran en el pie de página o footer del sitio y están claramente identificadas con el nombre de "Políticas de privacidad" o equivalentes, lo que facilita que las personas las localicen (algo que en 2015 era mucho menos frecuente). Sin embargo, de las políticas analizadas todavía los documentos que las contienen son fundamentalmente imágenes que no facilitan la navegación, por tanto, siguen siendo de difícil consulta y uso.

Directv cumple formalmente con los criterios al publicar políticas claras y de fácil acceso, mientras que el resto solo ganan reconocimiento por publicarlas. En general, los documentos de las empresas simplemente repiten la ley o son tan cortos que no desarrollan el tema apropiadamente, no entregan información clara y transparente para que se entiendan los procedimientos que se desarrollan alrededor de los datos personales y cómo pueden afectar los derechos a la intimidad y a la libertad de expresión, entre otros. Si todavía existen estas dificultades, resulta lógico encontrar que ninguno de los ISP evaluados, incluído Directv,  ha ido más allá para cumplir con un tema "deseable": que la información sea accesible a todas las personas, incluidas aquellas con alguna discapacidad que precisan de programas especiales de lectura. Ninguno de los documentos evaluados es accesible.

## Sobre la protección a la intimidad

Los ISP aún no comprenden el papel que tienen en cuanto a la protección de la intimidad de las personas. Ninguno de los ISP asume públicamente el compromiso de notificar a las personas cuando hayan solicitudes de información sobre sus datos. Como en 2015, este año solo Directv hace una mención al indicar

> [Q]ue en la mayoría de los casos en que la información se provee en respuesta a un requerimiento legal le proveerán notificación previa de dicho requerimiento

> u orden al suscriptor [sic] de modo que éste [sic] pueda impugnar en un procedimiento en corte.

Sin embargo, como lo mencionamos el año pasado, esta afirmación, aunque es una buena práctica, necesita precisiones. Con ello nos referimos a que continúa siendo una declaración discrecional y además de vaga que no va acompañada de los procedimientos que el ISP adelanta, por tanto, no puede decirse que haya un verdadero compromiso.

La existencia de procedimientos y controles para el suministro de información sobre las comunicaciones de las personas, garantiza su derecho a la intimidad y por eso nos interesa que los ISP tengan manuales y protocolos claros que implementen la ley, esto es un elemento deseable y aún no se da en ninguna de las empresas evaluadas.

El otro criterio que se evalúa para analizar la protección que los ISP hacen de la intimidad de quienes contratan sus servicios es si son claros en informar sobre sus obligaciones y prácticas de retención de datos, particularmente, al momento de entregar información de quienes contratan sus servicios solo cuando hay órdenes de fiscales. Al evaluar este criterio, nuevamente, vemos que es Telefónica-Movistar el único ISP que menciona la retención de datos. Además, en 2016, a raíz de una política global de esta empresa con detalles que dan mejor marco a las normas nacionales, han publicado una política global que busca proteger la privacidad. Su foco, sin embargo, está en los ataques informáticos, sin que desarrolle preceptos para evitar abusos en las facultades de los gobiernos para vigilar a la población. De otra parte, en cuanto al reconocimiento de que la información de comunicaciones que retienen es confidencial y solo se entregan con orden de un fiscal, este año reconocemos el micrositio creado por ETB en donde dan información sobre el marco legal que se aplica en Colombia cuando hay solicitudes de información de datos por las autoridades competentes. Esto también constituye una buena práctica.

Por otro lado, mientras en la Fundación Karisma investigábamos el sistema de registro de IMEI de celulares en Colombia, establecimos que cuando se discuten algunas políticas los ISP que operan en el país exponen importantes argumentos de privacidad en defensa de quienes contratan sus servicios. Durante el mencionado proceso de discusión ante la Comisión Reguladora de Comunicaciones (CRC), encontramos que Tigo-UNE hizo observaciones sobre la afectación que el sistema que exige a los operadores extraer metadatos de las comunicaciones tendría para los derechos de las personas. Entre otros argumentos, Tigo-UNE resaltó:

> La información que pide la CRC puede afectar la intimidad de las personas, porque a partir del cruce de datos que se pide por parte de la regulación, se puede establecer “patrones de comportamiento y localización”.

La información que pide la CRC puede violar las garantías que trae la ley de protección de datos, especialmente los principios de libertad, finalidad y necesidad[6]

Es importante resaltar que es posible que existan otros documentos similares de otros ISP, pero que, debido al gran número de archivos relacionados con este sistema de registro, hayamos pasado por alto documentación semejante.

## Sobre la protección a la libertad de expresión

Cuando nos referimos a filtrado, retiro o bloqueo de contenidos y cancelación de cuentas encontramos que la fusión de Tigo-UNE provocó que en este criterio, como en el relacionado con la protección a la intimidad, el ISP perdiera la calificación ganada en 2015. Este año, sin embargo, reconocemos como buena práctica que Telefónica-Movistar advierta en su política global que existen disposiciones contractuales que obligan a quien se suscribe al servicio a adoptar determinadas conductas.

La ETB logra *una carga completa* porque sus políticas son las más detalladas, ofreciendo información sobre los motivos que pueden llevar a la compañía a filtrar, bloquear e incluso cancelar cuentas. Además, entre los documentos publicados en su sitio web, se encuentra un manual de usos aceptables, cuyo fin es orientar a las personas sobre los comportamientos adecuados en el uso de los servicios que ofrece. También incluye un documento en el que informan que el bloqueo en Colombia se da únicamente por "pornografía infantil".

Desde Fundación Karisma asumimos también como un reto de la sociedad civil trabajar para que este tipo de esfuerzos no solo se visibilicen, sino que sean parte de la cultura empresarial. Proteger los derechos humanos de quienes contratan sus servicios debe ser un elemento central de las actividades de los ISP y debe reflejarse en las políticas que los guían.

## RESUMEN DE LA EVALUACIÓN

# METODOLOGÍA

Como lo expusimos en la introducción, la evaluación que se hace en el informe **¿Dónde están mis datos?** se estructura a partir de cuatro ejes: (1) transparencia sobre requerimientos de autoridades; (4) protección de datos; (3) intimidad; y (4) libertad de expresión.

¿**Dónde están mis datos?** analiza la información que se encuentra publicada en los sitios web de los ISP para evaluar cómo cumplen con los siguientes criterios:

1. El ISP publica informes de transparencia.
2. La política de protección de datos del ISP es clara y de fácil acceso.
3. El ISP informa a quienes contratan sus servicios que notificará cuando las autoridades han hecho solicitud de información de sus datos.
4. El ISP es claro sobre la forma cómo cumple con las obligaciones legales que pueden afectar la intimidad de quienes contratan sus servicios.
5. El ISP es claro sobre la forma como filtra, retira o bloquea contenidos y cómo cancela o suspende servicios.

En 2016, la evaluación se ocupó de analizar el caso de 5 empresas, 4 de estas habían sido incluidas en 2015: ETB, Telefónica-Movistar, Directv y Claro, y sustituimos a UNE por TigoUne, dada la fusión que hicieron las dos empresas en 2015.

Como parte de nuestra metodología, intentamos establecer contacto con todas las compañías evaluadas. Con quienes logramos hablar, hicimos un proceso de socialización de los resultados preliminares de la evaluación, realizada en el primer semestre del año. En estas reuniones se presentó la metodología de evaluación a implementar para el año 2016, además de que los ISP tuvieron la oportunidad de retroalimentarla.

En 2016 cambiamos la representación de la calificación usada en 2015:

- **Carga completa:** El ISP cumple con todos los parámetros.
- **Media carga:** El ISP cumple con uno de los parámetros.
- **Cuarto de carga:** Se reconocen buenas prácticas del ISP.
- **Sin carga:** El ISP no cumple con ninguno de los parámetros.

## Criterios de evaluación

En este segundo informe de ¿Dónde están mis datos?, incluimos cambios que tuvieron como objetivo hacer más comprensibles los criterios que usamos para hacer la evaluación, buscando así que en el corto plazo se generen cambios en las políticas de las compañías colombianas en beneficio de los derechos de las personas. Esto responde también a la experiencia adquirida en el proceso del primer informe, así como a los comentarios y sugerencias de los ISP. En este sentido, el informe presenta sus cinco criterios de evaluación estructurados en cuatro aspectos: (1) transparencia; (2) protección de datos; (3) intimidad; y (4) libertad de expresión.

Siguiendo esta nueva estructura, algunos aspectos se retiraron de los resultados de la evaluación, aunque se mantienen como criterios deseables que podrían ser incluidos tanto dentro de un informe de transparencia como en las políticas de protección de datos de los ISP. De esto modo, se presentan como sugerencias de la sociedad civil.

# I. Transparencia

## 1. El ISP publica informes de transparencia

En esta categoría se evalúa si el ISP ha publicado informes de transparencia que evidencien el tratamiento de los datos personales de quienes contratan sus servicios, además de los procedimientos y frecuencia para dar respuesta a las solicitudes de información por parte del Gobierno Nacional y otras entidades.

***Parámetro de respuesta***

(1) El ISP ha publicado un informe de transparencia en el último año.

- **Carga completa:** El ISP ha publicado un informe de transparencia en el último año.
- **Media carga:** El ISP publica informes de transparencia con algunos datos sobre el manejo de datos de las personas usuarias.
- **Cuarto de carga:** El ISP tiene buenas prácticas respecto de las políticas de protección de datos.
- **Sin carga:** El ISP no ha publicado un informe de transparencia en el último año.

***RECOMENDACIÓN. Los ISP deben trabajar en la publicación periódica de informes de transparencia que aborden la forma como responden a solicitudes de datos personales, que ofrezcan claridades sobre la forma cómo gestionan esos procesos y que expliquen su rol en los bloqueos y/o retiros de contenidos y cancelaciones o suspensión de servicios.***

***Informes de este tipo ya se empiezan a publicar por intermediarios como Facebook, que publica en su página web el* Informe de solicitudes de gobiernos*; Google, que tiene un informe de transparencia que incluye solicitudes gubernamentales de retirada de contenido, solicitudes de información sobre personas usuarias y solicitudes de propietarios de derechos de autor para el retiro de resultados de búsqueda;* Twitter, que al igual que en el caso de Google incluye informes sobre requerimientos legales de información sobre cuentas, requerimientos legales de retiro de contenidos, notificaciones relacionadas con derechos de autor; o incluso empresas que dan acceso a internet como Vodafone. Los ejemplos se van multiplicando alrededor del mundo, mostrando que existe una verdadera tendencia en este sentido. De hecho, países como México han incluido estos informes como una obligación legal.**

***Para la Fundación Karisma esta es una buena práctica que debería ser incentivada por los gobiernos y desarrollada por los ISP. Ahora bien, para que el informe sea útil consideramos que los informes periódicos deberían incluir datos del ISP sobre:***

- *Las solicitudes que ha hecho el Gobierno, a través de diferentes entidades del Estado, de información de las personas usuarias.*
- *La frecuencia con que el ISP entrega esta información al Gobierno*
- *El número de veces en que ha dado respuesta a las solicitudes hechas por el Gobierno, además de explicar el procedimiento que han tenido las mismas.*
- *El número de personas que han sido notificadas sobre estas solicitudes.*
- *Explicación del manejo de los datos que el ISP hace, si han sido administrados por terceros y, en tales casos, cuáles son las acciones llevadas a cabo para proteger esos datos (disposiciones contractuales, auditorías, etcétera), además de hacer seguimiento a las solicitudes que el Gobierno haga de información a esos terceros.*
- *Si ha actuado en defensa de las personas protestando solicitudes de información.*
- *El origen de las solicitudes de bloqueo y/o retiro de contenidos de internet, incluyendo "pornografía infantil", infracción al derecho de autor, cumplimiento de sus propias políticas, etc.*
- *El número de veces que el ISP ha procedido a bloquear y/o retirar contenidos de internet por cuenta propia o a solicitud de terceros, incluido el Gobierno.*
- *Si ha actuado en defensa de personas cuyo contenido ha sido objeto de una solicitud de bloqueo y/o retirado, y los motivos para ello, al menos en forma general.*

# II. Protección de datos

## 2. La política de protección de datos del ISP es clara y de fácil acceso

***Parámetro de respuesta***

**(1)** El ISP tiene una política de protección de datos que está publicada en su página web.

**(2)** La política de protección de datos del ISP es clara. Por clara, entendemos:

- Está escrita en un lenguaje sencillo que describe las diferentes situaciones y las explica —a través de ejemplos—, además de que incluye las referencias necesarias a la ley.
- La política de protección de datos especifica cómo, con quién y para qué el ISP comparte los datos de quienes contratan sus servicios.

**(3)** La política de protección de datos es de fácil acceso. Por fácil acceso, entendemos:

- Se encuentra fácilmente en el sitio web del ISP. Valoramos que se sigan las buenas prácticas ya desarrolladas en internet como que estos documentos se encuentran en el pie de página o *footer* del sitio y bajo el nombre de "Políticas de privacidad" o equivalente).
- Es un documento de fácil navegación, es decir, permite búsqueda, copia, etcétera. Valoramos especialmente que el documento respete estándares de accesibilidad y sean formatos que puedan usarse sin importar el software que tenga la persona que lo consulta.

- **Carga completa:** El ISP tiene su política de protección de datos publicada en su sitio web. Este documento es claro sobre cómo, con quién y para qué el ISP comparte los datos de quienes contratan sus servicios. Finalmente, es un documento de fácil acceso y de fácil navegación.
- **Media carga:** El ISP tiene su política de protección de datos publicada en su sitio web pero este no es un documento claro que especifica cómo, con quién y para qué el ISP comparte los datos de las personas suscriptoras. Tampoco es un documento de fácil acceso y de fácil navegación.
- **Cuarto de carga:** El ISP tiene buenas prácticas respecto de las políticas de protección de datos.
- **Sin carga:** El ISP no tiene su política de protección de datos publicada en su sitio web.

## 3. El ISP informa a quienes contratan sus servicio que notificará cuando las autoridades han hecho solicitud de información de sus datos

*Parámetro de respuesta*

**(1)** El ISP informa a quienes contratan sus servicios que está obligado por ley a entregar información personal de ellas y publica los procedimientos que emplea para responder a esos requerimientos de información, que incluyen notificar a la persona que es objeto del requerimiento para facilitarle la defensa si así lo desea.

- **Carga completa:** El ISP informa a quienes contratan sus servicios que por ley puede recibir requerimientos de información personal, además les indica cómo los tramita y se compromete a notificar a la persona afectada por una de estas solicitudes de información.
- **Media carga:** El ISP informa a quienes contratan sus servicios que por ley puede recibir requerimientos de información personal, además les indica cómo los tramita pero no se compromete a notificar a la persona afectada por una de estas solicitudes de información.
- **Cuarto de carga:** El ISP ha adoptado buenas prácticas de transparencia en la gestión de los datos de las personas que se los confían.
- **Sin carga:** El ISP no informa a quienes contratan sus servicios sobre su obligación legal, no tiene un procedimiento público para responder a los requerimientos de información ni el compromiso de que notificará sobre solicitudes de información de los datos de esas personas.

***RECOMENDACIÓN. Los ISP deben trabajar en mejorar la transparencia sobre la forma como entregan a terceros, incluidas a las autoridades competentes, los datos de quienes contratan sus servicios. Por tanto, sería deseable que los ISP:***

*Incluyeran en sus políticas información sobre la obligación legal de atender requerimientos de las autoridades competentes para entregar datos personales de quienes han contratado servicios con esta empresa. En desarrollo de esta obligación, el ISP publicara los procedimientos que usa para atender estos requerimientos, indicando, al menos, cuál es el departamento responsable de dar respuesta a las solicitudes de información, que, a su vez, está obligado a verificar la legalidad de la solicitud y a dejar registros tanto de las solicitudes como de las respuestas; informara que el responsable conoce y cumple con los acuerdos que el país tiene para cooperar en la entrega de información a autoridades extranjeras; y, finalmente, incluyera en el procedimiento los parámetros del compromiso del ISP (cuándo, cómo y dónde) mediante el cual el responsable de este procedimiento notifica a la persona afectada por una de estas solicitudes.*

# III. Intimidad

## 4. El ISP es claro sobre la forma cómo cumple con las obligaciones legales que pueden afectar la intimidad de las personas.

*Parámetro de respuesta*

**(1)** El ISP informa a quienes contratan sus servicios que está obligado por ley a hacer retención de datos. En Colombia, la provisión de servicios de telecomunicaciones es uno de los ámbitos donde se producen más datos y, como sucede en otros países, se obliga a los ISP a retener y a entregar esos datos para diversos propósitos. Las personas tienen una relación de dependencia con los ISP en dos niveles: (1) la provisión del servicio en sí mismo, y (2) la salvaguarda de los datos que fluyen a través de la conexión. Las obligaciones de retención buscan la conservación de los datos que generan la conexión de telefonía fija, celulares o de internet estableciendo el tipo de datos a conservar por los ISP, el tiempo de retención, y las condiciones para el acceso a esos datos, además de quienes están facultado para acceder. Las normas en Colombia que obligan a los ISP a esta retención son el Decreto 1704 de 2012 sobre investigaciones criminales y la Ley de inteligencia (Ley No. 1621 de 2013). Al ser una restricción al derecho a la intimidad es necesario que los ISP sean garantistas y transparentes para evitar abusos.

**(2)** El ISP informa que está obligado a cumplir con las órdenes legítimas que haga la Fiscalía General de la Nación en el marco de una investigación penal para acceder a los datos de geolocalización, metadatos e información de quienes contratan sus servicios y/o contenido que viajen por sus redes.

- **Carga completa:** El ISP informa que está obligado por ley a hacer retención de datos y a cumplir con las órdenes legítimas que haga la Fiscalía General de la Nación en el marco de una investigación penal para acceder a determinados datos de quienes contratan sus servicios.
- **Media carga:** El ISP informa de manera general sobre algunas de las obligaciones que tiene por ley frente a la retención de datos y las órdenes legítimas de la Fiscalía General de la Nación.
- **Cuarto de carga:** El ISP tiene buenas prácticas respecto de la información sobre retención de datos y la obligación de cumplir con las órdenes legítimas de la Fiscalía General de la Nación.
- **Sin carga:** El ISP no informa que está obligado por ley a hacer retención de datos y a cumplir con las órdenes legítimas que haga la Fiscalía General de la Nación en el marco de una investigación penal para acceder a determinados datos de quienes contratan sus servicios.

***RECOMENDACIÓN. Los ISP deben trabajar para mejorar la transparencia sobre la retención que hacen de los datos de quienes contratan sus servicios. Por tanto, sería deseable que los ISP:***

*Desarrollen y publiquen guías o protocolos en los que se describa que retiene datos de quienes contratan sus servicios en dos niveles: (1) para efectos del servicio que ofrece, y (2) por obligación legal. Estos documentos deben dar detalles sobre esta retención indicando de donde proviene la obligación legal, cuáles son los datos que retiene (derivados de la obligación legal y de los requerimientos para la provisión del servicio); indicar claramente el plazo durante el cual retiene los datos; y, dado que también hay una retención derivada de la relación contractual, establecer los fines para los que hace la retención de los datos cuando se derivan de la provisión del servicio.*

# IV. Libertad de expresión

## 5. El ISP es claro sobre la forma cómo filtra, retira o bloquea contenidos y cómo cancela o suspende servicios

***Parámetro de respuesta***

**(1)** El ISP tiene un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones.

**(2)** El ISP publica los procedimientos que emplea para filtrar, retirar, bloquear contenidos indicando los soportes legales y/o contractuales que lo justifican. Es decir, el ISP tiene en cuenta el debido proceso en sus procedimiento de filtrado, retiro o bloqueo de contenidos. Para ello, como mínimo, notifica a la persona de manera que tenga oportunidad de defenderse y cuenta con criterios de proporcionalidad y necesidad.

**(3)** El ISP publica los procedimiento que emplea para suspender y/o cancelar servicios. Es decir, el ISP tiene en cuenta el debido proceso en sus procedimiento para suspender y / o cancelar servicios. Para ello, como mínimo, notifica a la persona de manera que tenga oportunidad de defenderse y cuenta con criterios de proporcionalidad y necesidad.

- **Carga completa:** El ISP tiene un código de conducta para guiar a las personas en comportamientos no permitidos. Además, publica los procedimientos que emplea para filtrar, retirar o

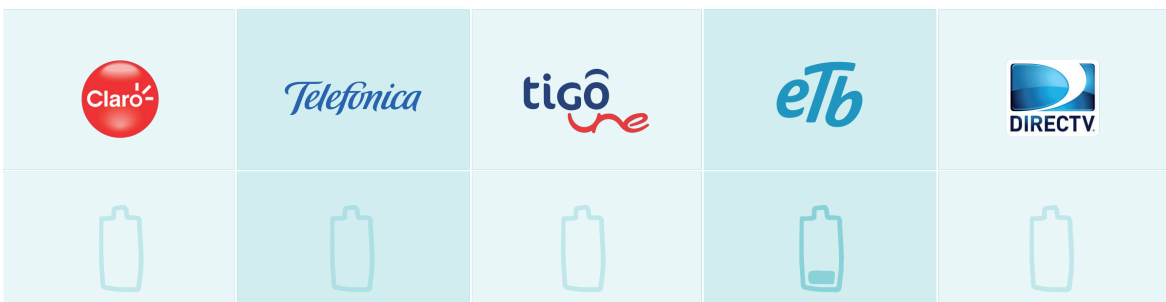
bloquear contenidos, y para suspender y/o cancelar servicios, indicando los soportes legales y/o contractuales que pueden justificar estas acciones.

- **Media carga:** El ISP tiene un código de conducta para guiar a las personas en caso de comportamientos no permitidos y/o publica los procedimientos que emplea para filtrar, retirar o bloquear contenidos, y para suspender y/o cancelar servicios.
- **Cuarto de carga:** El ISP tiene buenas prácticas respecto de la información sobre filtro, retiro o bloqueo de contenidos, además de cancelación o suspensión de servicios.
- **Sin carga:** El ISP no tiene un código de conducta para guiar a las personas en comportamientos no permitidos. Tampoco publica los procedimientos que emplea para filtrar, retirar o bloquear contenidos, ni para suspender y/ o cancelar servicios.

# RESULTADOS DE LA EVALUACIÓN

## I. Transparencia

### 1. El ISP publica informes de transparencia




En 2016, se modificó este criterio de evaluación teniendo en cuenta que tanto los resultados del año anterior como los obtenidos en la evaluación preliminar evidenciaban que las empresas no publican informes de transparencia. Se estableció que para los ISP el informe de transparencia es el que hacen ya desde hace muchos años informando sobre su gestión financiera. Este tipo de informe está más vinculado a temas de corrupción, por lo que la gestión de datos personales, además del compromiso empresariales con la defensa de la intimidad y la libertad de expresión de quienes contratan sus servicios aún no forma parte del mismo. Comprendiendo que hay un tema de cultura empresarial que debemos ayudar a cambiar, se simplificó el criterio de evaluación. En su lugar, elaboramos unas

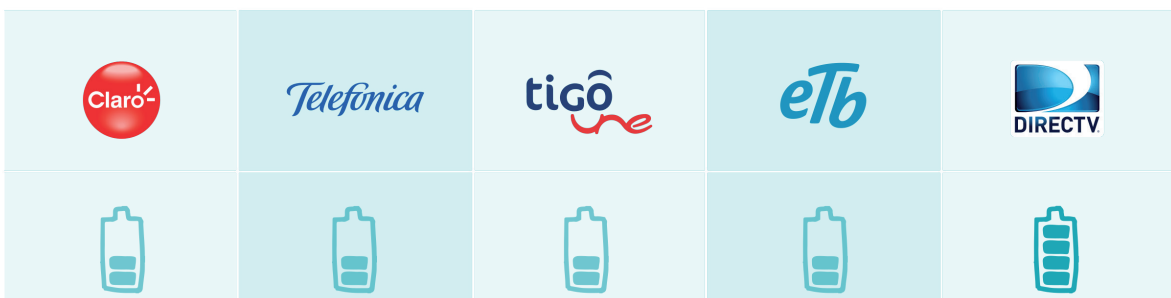
recomendaciones sobre lo que es un informe y el contenido deseable a partir de lo que planteamos en 2015.

No obstante el cambio, al igual que el año pasado, en esta categoría encontramos que ninguna de las empresas evaluadas publica informes de transparencia relacionados con la protección de la intimidad y la libertad de expresión. Sin embargo, ETB obtiene un cuarto de carga en reconocimiento a su compromiso por trabajar este tema. El ISP modificó su sitio web y ahora se puede acceder desde su portal principal a un espacio donde publican información centralizada sobre el proceso legal de bloqueo de contenidos de internet, de interceptación de comunicaciones y de solicitud de información de las personas usuarias por parte de las autoridades. En el mismo sitio, incluyeron el informe de gestión y sostenibilidad, la política de protección de datos y la de usos aceptables. De esta forma, ETB facilita el acceso a información de la empresa para consulta de cualquier persona. Sin embargo se trata esencialmente de información sobre la ley y sus políticas pero, como ya dijimos, el ISP no ofrece un informe de transparencia que muestre lo que sucede en la práctica al aplicar esas obligaciones y políticas durante un plazo de tiempo determinado. Es decir, no se concreta en un informe de transparencia sobre estos temas.

En Colombia tenemos un reto importante para ampliar la cultura empresarial. Es necesario explicar y promover que la transparencia va más allá de la gestión financiera de las empresas. Hasta ahora, la transparencia se asocia con información orientada a clientes empresariales, accionistas e incluso trabajadores de las compañías. Tan solo reconocer que con las nuevas tecnologías los datos son la moneda con que las personas pagamos en internet, que nuestra actividad en la red revela nuestra intimidad y que internet es un espacio privilegiado para que las personas ejerzan su derecho a la libertad de expresión obliga a los ISP a replantear su rol como intermediarios y a ampliar su compromiso con la transparencia, con el fin último de respetar los derechos humanos.

# II. Protección de datos

## 2. La política de protección de datos del ISP es clara y de fácil acceso.



Para este criterio de evaluación no solo valoramos que tuvieran publicadas sus políticas en sus sitios web, sino también consideramos otros aspectos que buscan reconocer las buenas prácticas que ya se están dando e impulsar nuevas. En este sentido, analizamos que los documentos estén escritos en un lenguaje claro, pero que, además, sean accesibles, por ejemplo, para personas con alguna discapacidad.

En este sentido, encontramos que todos los ISP cumplen con el primer parámetro de evaluación al tener publicada en su sitio web las políticas de protección de datos personales de las compañías. Para este año, además, destacamos que están publicadas en posiciones visibles dentro del sitio.

Sin embargo, las políticas no son claras al no estar escritas en un lenguaje sencillo y no describir diferentes situaciones a través de ejemplos. Tampoco especifican cómo, con quién ni para qué el ISP comparte los datos de las personas. Así, por ejemplo, la política de Claro es una copia de la Ley de protección de datos personales, mientras que las de Telefónica-Movistar, Tigo-UNE y ETB están escritas en un lenguaje dirigido a un público más técnico o especialista en aspectos jurídicos. Esto es una barrera que dificulta la compresión que podría tener una persona sobre lo que puede o no hacer el ISP o la forma en concreto en que estas empresas aplican las normas legales.

Solo Directv hace un mayor esfuerzo y presenta un documento más claro en donde hace un recuento de las definiciones, principios, derechos de los titulares u otros apartes de la Ley de protección de datos personales, explicadas en relación a las actividades que desarrolla la empresa. Además, respecto a los procedimientos sobre cómo y con quién se comparten los datos de las personas, la política del ISP señala que:

> El tipo de tratamiento que se realiza a los datos personales contempla lo siguiente: Compartir la información [para c]umplir con las disposiciones normativas sobre transferencia de datos a terceros países en caso que dicha transferencia sea necesaria; [p]roveer información a las autoridades que lo soliciten expresamente y en ejercicio de sus funciones o para responder requerimientos administrativos y/o judiciales.

Aunque comparado con el resto de ISP, Directv tiene una mejor política, es necesario afirmar que tampoco ofrece explicaciones sobre la forma cómo comparten los datos. Mucho menos indica con quienes los comparten, más allá de lo que la ley prevé.

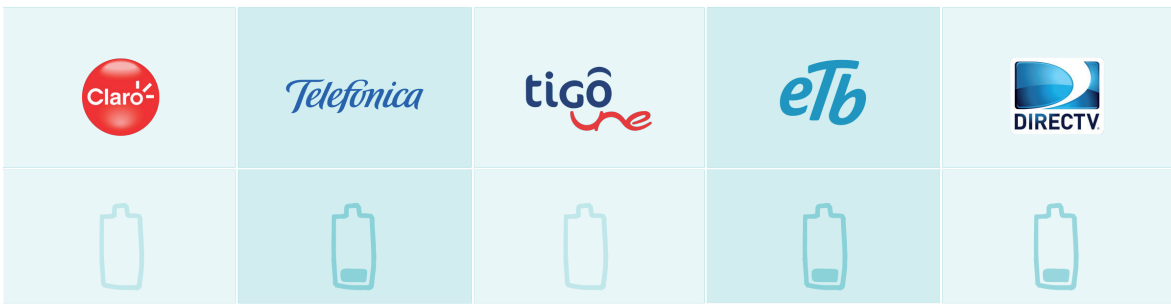
En cuanto a la facilidad de acceso a las políticas de los ISP, este año evidenciamos que se mantienen muchos de los aspectos que resaltamos en la evaluación de 2015. Claro tiene una política que aunque está publicada en su sitio web no es fácil de encontrar. Aunque hay un enlace al pie de la página del sitio con el título *Legal y Regulatorio*, que finalmente llevará a la política, se requiere revisar 17 páginas de documentos o usar el filtro sin saber bajo qué nombre buscar. El documento lleva por título *Políticas de Tratamiento de la Información* y, eventualmente, aparecerá en esa búsqueda en la página 13. El documento está en formato PDF que permite descarga, navegación y búsqueda desde cualquier dispositivo. Sin embargo, al ser un PDF sin etiquetado no es accesible para personas que requieran de programas especiales de lectura, como aquellas con alguna discapacidad visual, por lo cual se

recomienda ajustar el formato a estándares de accesibilidad y mejorar la ubicación del documento, hacerlo más fácil de encontrar.

En el caso de Telefónica-Movistar, UNE y ETB, las políticas de protección de datos aunque son fáciles de encontrar, no son fáciles de usar ni cumplen requisitos de accesibilidad. Aunque el formato en que están publicados es PDF, no se publican textos navegables sino un texto escaneado como imagen que no permite búsqueda interna, ni utilizar software lector de pantalla por parte de personas con alguna discapacidad visual o de acceso a textos escritos.

En este criterio, también Directv tiene mejores prácticas, pues su política de protección de datos es fácil de encontrar. En el *footer* de la página principal está el enlace *Protección de Datos Personales*, que remite a una página en donde se encuentra la política con el título *Manual interno de políticas y procedimientos sobre tratamiento de datos personales de Directv Colombia Ltda*. El documento está en formato PDF que permite descarga, navegación y búsqueda desde cualquier dispositivo. Por eso, Directv cumplió el criterio completo este año. Sin embargo, es necesario recordar que valoramos la accesibilidad de los archivos. Al ser un PDF sin etiquetado no es accesible para personas que requieran de programas especiales de lectura. Por lo que, aunque este año reciben el reconocimiento al cumplir el resto de los criterios, como en el caso de Claro, se recomienda ajustar el formato a estándares de accesibilidad.

## 3. El ISP informa a quienes contratan sus servicios que notificará cuando las autoridades competentes han hecho solicitud de información de sus datos.




En este criterio, encontramos que no hay un compromiso real de los ISP de informar a las personas cuando ha habido una solicitud de información de sus datos. Creemos que lo más probable es que los ISP no reconocen el rol tan central que juegan en la defensa de la intimidad de quienes contratan sus servicios.

Claro, en su política de protección de datos, solo menciona lo que ya dice la ley, es decir que uno de los derechos de las personas sobre sus datos es el de “ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos

personales". Esta es una obligación general que, de hecho, puede ser vista desde la óptica de las obligaciones comerciales, del uso que el ISP hace de los datos para efectos de la provisión del servicio. El ISP no informa en concreto su obligación legal de entregar información personal al Estado, mucho menos da detalles sobre el procedimiento que emplea cuando esto sucede. Lo mismo sucede con ETB. Sin embargo, a este ISP se le reconoce como buena práctica que en su política de protección de datos expone que se verifican las excepciones legales para la entrega de datos personales a las autoridades competentes y los casos pertinentes.

Directv, aunque no informa en concreto sobre su obligación legal de entregar información personal frente a un requerimiento del Estado, ni da detalles sobre el procedimiento que emplea cuando esto sucede, en su política de privacidad, afirma que notificará a quienes contratan sus servicios sobre la entrega de sus datos:

> Por ejemplo, pudiéramos ser requeridos que desglocemos cierta Información de los Clientes o IOPI en respuesta a un requerimiento u orden de la corte. En la mayoría de los casos en que la información se provee en respuesta a un requerimiento legal, nosotros le proveeremos notificación previa de dicho requerimiento u orden de modo que usted pueda impugnarla en un procedimiento en corte.

En este sentido, el ISP manifiesta su intención de notificar de las solicitudes que haga "la corte" en la "mayoría de los casos". Si bien es una buena práctica a destacar, es solo un compromiso discrecional y no incluye un procedimiento que apoye ese pronunciamiento.

Por su parte Tigo-UNE no informa nada sobre su obligación legal de entregar información personal al Estado, mucho menos da detalles sobre el procedimiento que emplea cuando esto sucede o se compromete con notificar cuando hay solicitudes de este tipo.

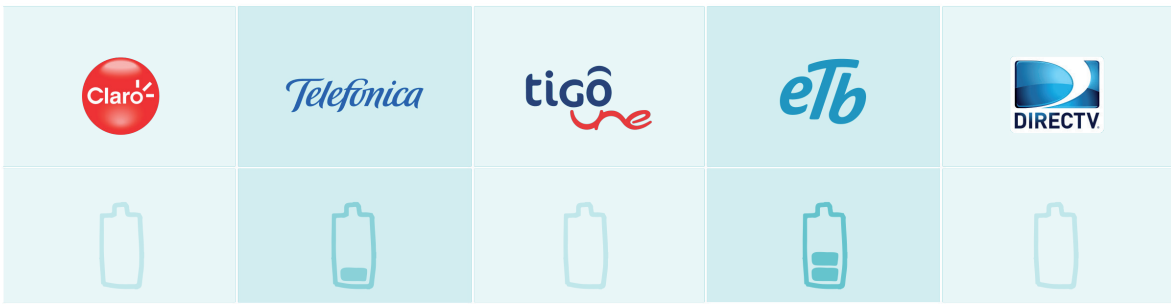
En cuanto a Telefónica-Movistar, si bien el ISP no informa en concreto su obligación legal de entregar información personal al Estado, si plantea en su política de privacidad, que hace parte de sus políticas globales, que

> Informaremos a nuestros clientes [sic] de aquellos casos relevantes en los que la pérdida, uso indebido o revelación de la información haya sido provocada por una violación en la seguridad de los sistemas y redes de la compañía o bien derivados de una decisión o acción técnica interna. En estos casos, informaremos a nuestros clientes [sic[] sobre las acciones correctivas realizadas y daremos las recomendaciones oportunas para ayudar a proteger sus intereses. En nuestra actuación con las fuerzas del orden respetamos la legislación local y los marcos reguladores.

Esto puede ser resaltado como una buena práctica en la medida en que la empresa busca proteger la privacidad de sus clientes. Sin embargo, esta disposición de la política global de la multinacional no se refiere a las solicitudes de información de los Estados, por tanto, no responde a este criterio. Adicionalmente, convendría localizarla y hacerla visible en el sitio web de la empresa para Colombia.

# III. Intimidad

## 4. El ISP es claro con quienes contratan sus servicios sobre la forma cómo cumple con las obligaciones legales que pueden afectar su intimidad.




Tal y como lo explicamos en la metodología, este punto se evaluaron dos aspectos. En primer lugar, sobre la obligación que tienen los prestadores de hacer retención de datos de conformidad con la reglamentación legal colombiana (Decreto 1704 de 2012 sobre investigaciones criminales y Ley de inteligencia), encontramos que, con excepción de Telefónica-Movistar, ninguno de los ISP informan a las personas que están obligados a hacer retención de datos.

Telefónica-Movistar, en sus políticas para Colombia, indica que

> Las bases de datos de Colombia Telecomunicaciones tienen vigencia indefinida. Los datos personales recolectados se conservarán por el tiempo que dure la relación existente entre la Empresa y el titular [sic] de los datos, y por el tiempo que sea necesario para el cumplimiento de los deberes legales o contractuales que Colombia Telecomunicaciones deba observar.

Sin embargo, parece que las políticas de la casa matriz está moviéndose en otro sentido. En la política de privacidad del grupo Telefónica manifiestan que:

> Sólo [sic] retenemos información de los interesados [sic] por el tiempo requerido por la ley o si es necesario para la consecución de un objetivo legítimo de nuestro negocio. Desde Telefónica nos comprometemos a atender todas las peticiones de oposición al tratamiento de datos en la medida en que no sean necesarias para la prestación del servicio.

Los dos documentos informan sobre la retención de datos que hace el ISP tanto para la provisión del servicio (contractual) como por orden legal. Ahora bien, comparando los dos documentos, se puede concluir que la política de la casa matriz es mucho más garantista y comprometida con los derechos de quienes contratan sus servicios que de su filial en Colombia. La política de la filial mantiene la

referencia a una vigencia "indefinida" de las bases de datos que ya habíamos apuntado en 2015 como preocupante.

El segundo aspecto de este criterio de evaluación está relacionado con la obligación del ISP de cumplir con las órdenes legítimas que haga la Fiscalía General de la Nación en el marco de una investigación penal con el fin de acceder a los datos de geolocalización, metadatos e información de quienes contratan sus servicios y/o el contenidos que cursen por sus redes. Respecto de este punto, encontramos que ETB es la única empresa que cumple con el parámetro, pues el ISP tiene publicado en su página de *Transparencia y Acceso a la Información* un documento en el que informan acerca del procedimiento de interceptación legal en Colombia, en donde, citando la Ley 1453 de 2011, señalan

> El fiscal podrá ordenar, con el objeto de buscar elementos probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados [sic], que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación.

Teniendo en cuenta el Decreto 1704 de 2012 sobre investigaciones legales, reiteran "[l]os proveedores deberán atender oportunamente los requerimientos de interceptación de comunicaciones que efectúe el Fiscal General de la Nación".

Los demás ISP evaluados realmente no parecen haber pensado el tema. Telefónica-Movistar y Tigo-UNE no hacen menciones sobre quién puede pedir información y cuál es la información que se puede pedir de acuerdo con las precisiones que hace la ley. Por su parte, Claro y Directv expresan de manera bastante amplia que pueden compartir información con autoridades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial. Esto es preocupante, pues las normas en Colombia son mucho más acotadas sobre quién puede pedir información y cuál es la información que se puede pedir.

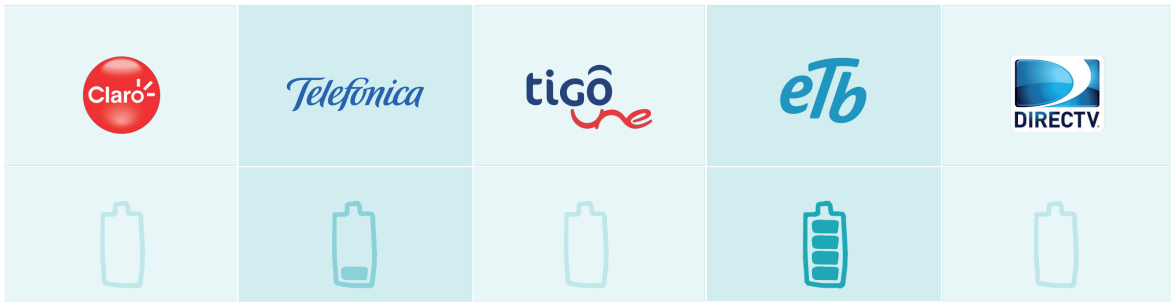
A pesar de lo anterior, es importante resaltar que este año, como parte de una investigación realizada desde la Fundación Karisma sobre el sistema de registro de IMEI de celulares en el país, establecimos que Tigo-UNE hizo observaciones durante el proceso ante la CRC sobre la afectación que tendría la obligación de los operadores de extraer metadatos de las comunicaciones los derechos de quienes contratan sus servicios. Entre otros argumentos, Tigo-UNE resaltó:

> "La información que pide la CRC puede afectar la intimidad de las personas, porque a partir del cruce de datos que se pide por parte de la regulación, se puede establecer "patrones de comportamiento y localización.
>
> La información que pide la CRC puede violar las garantías que trae la ley de protección de datos, especialmente los principios de libertad, finalidad y necesidad.[7]

Es importante resaltar que es posible que existan otros documentos similares de otros ISP, pero que, debido al gran número de archivos relación con este sistema de registro, hayamos pasado por alto documentación semejante.

# IV. Libertad de expresión

## 5. El ISP es claro con quienes contratan sus servicios sobre la forma como filtra, retira o bloquea contenidos, y cómo cancela o suspende servicios




En esta categoría, evidenciamos avances respecto de lo encontrado en 2015 en dos de los ISP evaluados: Telefónica-Movistar y ETB. Este año encontramos guías o códigos de conducta que dan parámetros a las personas en los comportamientos no permitidos por los ISP con el fin de evitar sanciones. La existencia de estos documentos supone que las empresas han hecho un análisis al interior sobre lo que justifica o no afectar el servicio de quienes contratan sus servicios. La evaluación que hace **¿Dónde están mis datos?** no tiene otro propósito diferente que analizar esa conciencia. No pretende calificar si las motivaciones son buenas o malas, tan solo da cuenta de su existencia.

Telefónica-Movistar, aunque no tiene un código de conducta para guiar sobre los comportamientos no permitidos en sus redes y servicios, tienen publicado en su sitio web un documento en el que hacen referencia a la seguridad de las personas, resaltando que [e]speramos que nuestros clientes utilicen los servicios contratados de conformidad con la ley y con lo estipulado por la 'política de uso aceptable' incluida en el contrato".

Por su parte, ETB cuenta con un documento denominado D*e políticas de uso aceptable ETB - PUA*, que

> [P]retende proteger a ETB y a sus usuarios [sic] de ataques de intrusos a sus sistemas, equipos y redes, así como coordinar y mantener los protocolos y lineamientos aceptados internacionalmente para el uso correcto y apropiado de los servicios.

Por otro lado, en relación con los procedimientos que emplean los ISP para filtrar, retirar o bloquear contenidos indicando los soportes legales y/o contractuales que lo justifican, o para cancelar o suspender servicios, encontramos que solo ETB hace menciones al respecto. Aunque el ISP no publica los procedimientos que usa para filtrar, retirar o bloquear contenidos, hace referencia a los soportes legales y/o contractuales que pueden justificar estas acciones. En el documento PUA ya mencionado, describen los usos que la empresa considera contrarios a los servicios que provee:

> (i) Interceptación de llamadas sin orden legal autorizada, así como el uso total o parcial de la información obtenida de esta forma. (x) Intentar acceder sin autorización a los sitios o servicios de ETB o de otro operador, mediante la utilización de herramientas intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades o cualquier otro medio no permitido o ilegítimo (xiii) Presentar, alojar o transmitir información, imágenes o textos que en forma directa o indirecta se relacionen con actividades sexuales con menores de edad. El CLIENTE declara que conoce lo dispuesto en la Ley 679 de 2001 y el Decreto 1524 de 2002, de acuerdo con lo cual se prohíbe expresamente el alojamiento de contenidos de pornografía infantil [...] entre otros.

ETB menciona que podrá dar por terminado el contrato, por tanto, suspender o cancelar servicios que presta, unilateralmente y sin que medie declaración judicial si se presenta alguno de los casos que allí describe. Adicionalmente, dentro de los documentos públicos del ISP se encuentra uno denominado *Libertad de expresión. ¿Cómo funciona el bloqueo de contenidos?*, en donde se informa claramente que "[l]os únicos contenidos que pueden ser bloqueados son los relativos a pornografía infantil y demás dispuestos en la ley".

El rol de los intermediarios de internet, entre los que están los ISP que ofrecen acceso a esta red, es clave para mantener internet como un espacio para el ejercicio de derechos humanos y para evitar indebidas intromisiones de terceros o del Estado a los derechos de las personas. ¿Dónde están mis datos? es un proyecto con alcances pedagógicos que busca impulsar buenas prácticas entre esas empresas para que, de una parte, protejan los derechos humanos y, de otra, ofrezcan información a las personas que usamos estos servicios sobre la forma cómo hacen uso de nuestros datos. El formato es el de una herramienta  que refleja esta importante realidad y que ayuda a informar a las personas para que consumimos estos servicios. Fundación Karisma tiene un compromiso con la protección y promoción de una internet libre, abierta, inclusiva y segura, y continuará haciendo esta evaluación periódica con ese fin.

# EVALUACIONES POR EMPRESA

Claro

| | | |
|---|---|---|
| 1 | Publica **informes** de **transparencia** | X |
| 2 | La política de **protección de datos** está **publicada** en su página web | ✓ |
| | La **política** de protección de datos del ISP es **clara** | X |
| | La política de protección de datos es de **fácil acceso** | +/- |
| 3 | **Informa** que está obligado por ley a entregar información personal y que notificará a las **personas usuarias** | X |
| 4 | **Informa** que está obligado por ley a hacer **retención de datos** | X |
| | **Informa** que está obligado a cumplir con las **órdenes** legítimas de la **Fiscalía** | X |
| 5 | Tiene una **guía** para las personas sobre **comportamientos no permitidos** con el fin de evitar sanciones | X |
| | **Publica** los **procedimientos** que emplea para filtrar, retirar, **bloquear contenidos** | X |
| | **Publica** los procedimientos que emplea para suspender y / o **cancelar servicios** | X |

X No cumple ✓ Cumple +/- Cumple parcialmente ● Buena práctica

DESCARGAR INFORME COMPLETO

DESCARGAR POR EMPRESA

Telefónica

| | | |
|---|---|---|
| 1 | Publica **informes** de **transparencia** | X |
| 2 | La política de **protección de datos** está **publicada** en su página web | ✓ |
| | La **política** de protección de datos del ISP es **clara** | X |
| | La política de protección de datos es de **fácil acceso** | +/- |
| 3 | **Informa** que está obligado por ley a entregar información personal y que notificará a las **personas usuarias** | ● |
| 4 | **Informa** que está obligado por ley a hacer **retención de datos** | ● |
| | **Informa** que está obligado a cumplir con las **órdenes** legítimas de la **Fiscalía** | X |
| 5 | Tiene una **guía** para las personas sobre **comportamientos no permitidos** con el fin de evitar sanciones | ● |
| | **Publica** los **procedimientos** que emplea para filtrar, retirar, **bloquear contenidos** | X |
| | **Publica** los procedimientos que emplea para suspender y / o **cancelar servicios** | X |

X No cumple ✓ Cumple +/- Cumple parcialmente ● Buena práctica

DESCARGAR INFORME COMPLETO

DESCARGAR POR EMPRESA

tigo une

| | | |
|---|---|---|
| 1 | Publica **informes** de **transparencia** | X |
| 2 | La política de **protección de datos** está **publicada** en su página web | ✓ |
| | La **política** de protección de datos del ISP es **clara** | X |
| | La política de protección de datos es de **fácil acceso** | +/- |
| 3 | **Informa** que está obligado por ley a entregar información personal y que notificará a las **personas usuarias** | X |
| 4 | **Informa** que está obligado por ley a hacer **retención de datos** | X |
| | **Informa** que está obligado a cumplir con las **órdenes** legítimas de la **Fiscalía** | X |
| 5 | Tiene una **guía** para las personas sobre **comportamientos no permitidos** con el fin de evitar sanciones | X |
| | **Publica** los **procedimientos** que emplea para filtrar, retirar, **bloquear contenidos** | X |
| | **Publica** los procedimientos que emplea para suspender y / o **cancelar servicios** | X |

X No cumple ✓ Cumple +/- Cumple parcialmente ● Buena práctica

DESCARGAR INFORME COMPLETO

DESCARGAR POR EMPRESA

eTb

| | | |
|---|---|---|
| 1 | Publica **informes** de **transparencia** | ● |
| 2 | La política de **protección de datos** está **publicada** en su página web | ✓ |
| | La **política** de protección de datos del ISP es **clara** | X |
| | La política de protección de datos es de **fácil acceso** | +/- |
| 3 | **Informa** que está obligado por ley a entregar información personal y que notificará a las **personas usuarias** | ● |
| 4 | **Informa** que está obligado por ley a hacer **retención de datos** | X |
| | **Informa** que está obligado a cumplir con las **órdenes** legítimas de la **Fiscalía** | ✓ |
| 5 | Tiene una **guía** para las personas sobre **comportamientos no permitidos** con el fin de evitar sanciones | ✓ |
| | **Publica** los **procedimientos** que emplea para filtrar, retirar, **bloquear contenidos** | +/- |
| | **Publica** los procedimientos que emplea para suspender y / o **cancelar servicios** | +/- |

X No cumple ✓ Cumple +/- Cumple parcialmente ● Buena práctica

DESCARGAR INFORME COMPLETO

DESCARGAR POR EMPRESA


# NOTAS


1. Ministerio de las Tecnologías de la Información y las Comunicaciones. (2016). *Boletín Trimestral de las TIC. Cifras primer trimestre de 2016*. Disponible en http://colombiatic.mintic.gov.co/602/articles-15639_archivo_pdf.pdf
2. Red en defensa de los derechos digitales. (2015). *Quien defiende tus datos*. Disponible en http://qdtd.org/qdtd/.
3. Hiperderecho (2015, 15 de noviembre). *Quien defiende tus datos*. Disponible en http://www.hiperderecho.org/qdtd/.
4. Interlab (2016). *Quem defende seus dados?* Disponible en http://quemdefendeseusdados.org.br/pt/.
5. Electronic Frontier Foundation (2015, 17 de junio). *Who has your back?*. Disponible en https://www.eff.org/who-has-your-back-government-data-requests-2015.
6. Jaime Andrés Plaza - Vicepresidente de Regulación TigoUne.(10 de marzo de 2016) [Carta enviada al Ministerio TIC y la CRC]. *Comentarios proyecto regulatorio "Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada"*. Disponible en: https://www.crcom.gov.co/recursos_user/2016/Actividades_regulatorias/mod_4813/TigoUne.pdf
7. Tigo-UNE. (2016, 10 de marzo). *Comentarios proyecto regulatorio "Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada"* [Carta enviada al Ministerio TIC y la CRC]. Disponible en https://www.crcom.gov.co/recursos_user/2016/Actividades_regulatorias/mod_4813/TigoUne.pdf.

# ¿Dónde Están Mis Datos?

Analizamos las políticas y documentos publicados en las páginas web de los intermediarios de Internet colombianos con una perspectiva de derechos humanos, buscando la transparencia.

www.dondeestanmisdatos.info

Un proyecto de

Fundación Karisma
www.karisma.org.co

Con el apoyo de

EFF