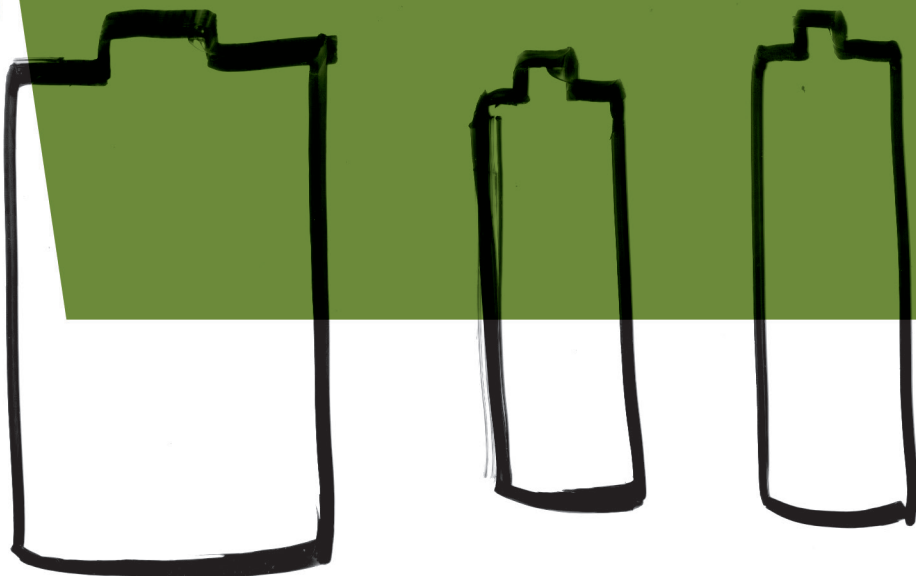


# ¿ dónde están mis datos?

Un informe de Fundación Karisma  
para saber qué tanto defienden  
nuestros derechos las empresas  
proveedoras de internet en Colombia.

INFORME 2017



Carolina Botero y Ann Spanger



# Fundación Karisma

Bogotá, Colombia  
2017

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: <http://www.documentoaccesible.com/#que-es>.

Fundación Karisma hace un especial reconocimiento a otros proyectos similares y, especialmente, a *Who has your back?* de la Electronic Frontier Foundation y a *Ranking Digital Rights* del Open Technology Institute, que han servido como inspiración para este proyecto. Agradecemos también a las personas de las empresas evaluadas que se reunieron con nosotros y que han estado trabajando en mejorar los resultados de su evaluación.

**Autoras:**

Carolina Botero  
Ann Spanger

**Revisión:**

Pilar Sáenz  
Amalia Toledo

**Coordinación editorial:**

Camila Barajas Salej

**Diseño gráfico:**

Mauricio Gatiyo

**Diagramación:**

Rubén Urriago



Este informe está disponible bajo Licencia Creative Commons Reconocimiento compartir igual 4.0.

Usted puede remezclar, retocar y crear a partir de esta obra, incluso con fines comerciales, siempre y cuando le de crédito al autor y licencien nuevas creaciones bajo las mismas condiciones. Para ver una copia de esta licencia visite:

[https://creativecommons.org/licenses/by-sa/4.0/deed.es\\_ES](https://creativecommons.org/licenses/by-sa/4.0/deed.es_ES).

# TABLA DE CONTENIDOS

<b>Introducción</b> .....	5
<b>Principales hallazgos</b> .....	8
<b>Conclusiones</b> .....	19
Transparencia .....	19
Intimidad .....	20
Libertad de expresión.....	21
Seguridad digital .....	21
<b>Metodología</b> .....	22
Ejes temáticos.....	22
Criterios de evaluación.....	23
Indicadores de evaluación .....	25
<b>Evaluación</b> .....	29
Claro .....	29
Telefónica-Movistar.....	31
ETB.....	33
Directv.....	35
Tigo-UNE.....	37
Emcali .....	39
Telebucaramanga .....	40



# Introducción

Nuestra vida en internet no puede distinguirse de nuestra vida en cualquier otro ámbito. A través de la red producimos y compartimos nuestra información, nuestras opiniones, buscamos lo que nos interesa y nos comunicamos con otras personas. En este proceso, fragmentos de nuestra vida, tanto pública como privada, quedan finalmente, flotando en el mundo virtual. Cómo esta información genera huellas y cómo esas huellas pueden ser rastreadas, registradas, acumuladas o compartidas por empresas privadas y gobiernos, es una preocupación actual que se conecta directamente con los derechos a la intimidad y a la libertad de expresión.

De acuerdo con el *Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC)*, el número de conexiones a internet en Colombia sigue en incremento.<sup>1</sup> Según las cifras del MinTIC en este mismo informe, el índice de penetración de las conexiones a internet de banda ancha en Colombia alcanzó el 57,6%. Esto plantea grandes retos para el respeto de los derechos humanos en el entorno digital.

La información que circula por internet y el poder de las empresas sobre nuestros datos interesa cada vez más a las autoridades, a los gobiernos y a diferentes agentes del mercado. Al acceder a esta información es posible crear perfiles, relativamente precisos, de cuáles son nuestros intereses y nuestras actividades. Así mismo, las redes las usamos para informarnos e informar. Si queremos que internet sea un verdadero vehículo de desarrollo social, es necesario que las empresas empiecen a considerar mecanismos para garantizar los derechos de las personas.

La protección de nuestros derechos tanto en línea como fuera de ella depende de la forma como usamos la tecnología (i.e. la configuración de nuestros celulares o de nuestros computadores), del marco legal que ofrece unas garantías y también de las políticas corporativas que implementan esas garantías. La evaluación que hace Fundación Karisma no tiene el alcance de revisar las prácticas de las personas en su relación con la tecnología. Sin embargo, su función sí es la de poner en evidencia las políticas corporativas de las empresas proveedoras de internet, la forma como las ajustan al marco legal (tanto en lo local como en relación con los estándares internacionales) y la forma como promueven, fortalecen o, por el contrario, debilitan el disfrute de los derechos de las personas en este entorno tecnológico. Este análisis también permite identificar las

---

<sup>1</sup> MinTIC (2017). *Boletín Trimestral de las TIC. Cifras primer trimestre de 2017*. Disponible en: [http://colombiatic.mintic.gov.co/602/articles-55212\\_archivo\\_pdf.pdf](http://colombiatic.mintic.gov.co/602/articles-55212_archivo_pdf.pdf).

buenas prácticas para el respeto de nuestros derechos en el entorno digital y resaltar a las empresas que las implementan, más allá de mirar si cumplen con las obligaciones legales.

En el informe *¿Dónde están mis datos? 2017*, Fundación Karisma analiza, desde una aproximación de derechos humanos, las políticas de siete empresas proveedoras de internet en Colombia. El análisis tiene el propósito de evaluar qué tanto estas empresas defienden nuestros derechos, especialmente la libertad de expresión y la intimidad; muestran un compromiso con la transparencia<sup>2</sup>; adoptan políticas de inclusión y asumen de forma responsable la protección de nuestros datos y su seguridad.

Para la evaluación tenemos en cuenta los estándares internacionales de derechos humanos descritos en documentos de organismos internacionales como las Naciones Unidas (NNUU) y la Organización de Estados Americanos (OEA), e incluso iniciativas más amplias como la *Global Network Initiative* (GNI). De esta forma, se consideraron para esta evaluación documentos como la [resolución de la Asamblea General de las NNUU sobre el derecho a la privacidad en la era digital](#)<sup>3</sup>; los documentos de la [Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos \(CIDH\)](#)<sup>4</sup>; los [principios del GNI](#)<sup>5</sup> y los [Principios necesarios y proporcionales](#)<sup>6</sup>.

Como novedad, este año incluimos dos nuevos ejes que abarcan cuatro nuevos criterios de evaluación. Se agregó el eje de compromisos políticos, en el que, además de informes de transparencia<sup>7</sup>, se incluyeron los criterios sobre políticas de género y accesibilidad.

---

<sup>2</sup> Tradicionalmente, en el mundo corporativo se asocia la transparencia con el compromiso y/o la obligación de las empresas de hacer pública su información financiera y evitar la corrupción. Sin embargo, en este documento hablamos del contexto concreto de las empresas proveedoras de internet y cómo su rol es central en el ejercicio de derechos humanos. Por lo tanto, la transparencia consiste en que publiquen los datos de su actuación frente a solicitudes de datos de las personas, solicitudes de bloqueos de contenidos o sitios web, notificaciones a las personas sobre estas actuaciones, etcétera.

<sup>3</sup> Asamblea General de NNUU. (2013, 20 de noviembre). *El derecho a la privacidad en la era digital*. A/C.3/68/L.45/Rev.1. Disponible en: [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/C.3/68/L.45/Rev.1&referer=http://protecciondatos.mx/2013/12/esresolucion-de-las-naciones-unidas-sobre-el-derecho-la-privacidad-en-la-era-digitalenunited-nations-resolution-privacy-digital-age/&Lang=S](http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&referer=http://protecciondatos.mx/2013/12/esresolucion-de-las-naciones-unidas-sobre-el-derecho-la-privacidad-en-la-era-digitalenunited-nations-resolution-privacy-digital-age/&Lang=S). [http://ap.ohchr.org/documents/S/HRC/d\\_res\\_dec/A\\_HRC\\_28\\_L27.pdf](http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf)

<sup>4</sup> CIDH & RELE. (2013, 31 de diciembre). *Libertad de expresión e internet*. OEA/Ser.L/V/II. CIDH/RELE/INF.11/13. Disponible en: [http://www.oas.org/es/cidh/expresion/docs/informes/2014\\_04\\_08\\_internet\\_web.pdf](http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf); *Declaración conjunta sobre libertad de expresión e internet de NNUU, OEA, OSCE y CADHP*. (2015). Disponible en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849>; CIDH & RELE. (2017, 15 de marzo). *Estándares para una Internet libre, abierta e incluyente*. OEA/Ser.L/V/II/CIDH/RELE/INF.17/17. Disponible en: [http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET\\_2016\\_ESP.pdf](http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf).

<sup>5</sup> *GNI Principles on Freedom of Expression and Privacy*. (s.f.). Disponible en [https://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy\\_0.pdf](https://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf).

<sup>6</sup> *Necesarios & proporcionados: principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones*. (2014, 10 de mayo). Disponible en: <https://necessaryandproportionate.org/es/necesarios-proporcionados>.

<sup>7</sup> Un informe de transparencia es la información que publica regularmente una empresa entregando una serie de estadísticas relacionadas con las solicitudes de datos personales, registros o contenidos. En estos informes se suele presentar el número de solicitudes que les hacen y el tipo de autoridades que las hacen en un período de tiempo determinado.

El otro eje es el de seguridad digital que, a su vez, se evalúa con dos pautas: el de informar sobre brechas de seguridad<sup>8</sup> y la adopción del protocolo HTTPS.

Sobre el criterio de políticas de género, vale la pena indicar que el propósito de su inclusión es el de educar e impulsar la discusión sobre las inquietudes relacionadas con diversidad sexual y de género en el sector de las tecnologías. Creemos que las preocupaciones que llevan a Fundación Karisma a hacer este informe las asume mejor una empresa con una cultura sensible a los temas de género. En el futuro esperamos ver reflejada, de manera transversal, la perspectiva de género en cada uno de los criterios evaluados.




































Somos conscientes de que hay otros temas importantes en la relación con el ejercicio de los derechos humanos. Es el caso de la sostenibilidad, la responsabilidad social empresarial, el compromiso con el medio ambiente, entre otros. Por eso es necesario aclarar que los ejes temáticos, y sus criterios, corresponden a los fines misionales de Fundación Karisma. Por este motivo, muchos otros, aunque importantes, quedarán por fuera.

Otro cambio importante en *¿Dónde están mis datos? 2017* es que, además de las cinco empresas que se habían evaluado en años anteriores (Claro, Tigo-UNE, Telefónica-Movistar, ETB y Directv), se agregan dos empresas proveedoras de servicios de internet a nivel regional: Emcali y Telebucaramanga. Las hemos escogido con el ánimo de aumentar el número de empresas que analizamos y también con el interés de evaluar el compromiso de empresas proveedoras más pequeñas por el respeto y la promoción de los derechos humanos en sus políticas. Emcali y Telebucaramanga, además, aparecen en las listas de empresas proveedoras de internet de Colombia que prestan un servicio de calidad, con mayor velocidad y cobertura.

---

<sup>8</sup> Una brecha de seguridad es un incidente que implica una fuga de información y, por tanto, la violación de datos. Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado. Estos incidentes deberán reportarse al Registro Nacional de Base de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderla. [http://www.sic.gov.co/sites/default/files/normatividad/CE\\_Implementacion\\_RNBD\\_fase\\_2.pdf](http://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf). Se debería notificar al cliente o particular cuando la violación de los datos afecte negativamente su intimidad o sus datos personales. Además se debería informar de las posibles consecuencias de la violación para el particular, especialmente, si puede facilitar la suplantación de su identidad, daños físicos, sufrimiento psicológico humillación o perjuicio de su reputación. También se debería informar de las circunstancias en que se haya producido la violación de datos personales con el fin de atenuar posibles efectos.

# Principales hallazgos

							
COMPROMISOS POLÍTICOS							
INTIMIDAD							
LIBERTAD DE EXPRESIÓN							
SEGURIDAD DIGITAL							

 Bonificación por uso del lenguaje inclusivo



Las evaluaciones de ¿Dónde están mis datos? 2017 se realizaron en dos períodos de tiempo. Entre abril y agosto de 2017, realizamos una evaluación preliminar que compartimos con las empresas proveedoras de internet que se interesaron en conocer sus resultados. Después de esta primera experiencia, llevamos a cabo una evaluación final en el mes de septiembre, que ajustamos tomando en cuenta sugerencias y cambios recientes que las empresas nos hicieron notar y los que identificamos en ese nuevo período. Además, tuvimos en cuenta la necesidad de hacer más explícito nuestro método de evaluación. El proceso de revisión significó el cambio de algunos resultados iniciales.

Los **principales hallazgos** que encontramos en el 2017 fueron:

- De las empresas evaluadas, ETB es la única que publicó en 2017 información equivalente a un primer informe de transparencia.<sup>9</sup> En el informe, ETB publica el tipo de peticiones de información privada que solicitaron diferentes entidades gubernamentales, indicado cuáles. Entre estas, se encuentran la Fiscalía General de la Nación, la Policía Nacional, el Ministerio de Defensa Nacional, la Dirección de Impuestos y Aduanas Nacionales y el Instituto Colombiano de Bienestar Familiar. ETB muestra el número de peticiones de información admitidas y rechazadas en relación con el tipo de datos solicitados (datos biográficos o geográficos).
- Es de resaltar el esfuerzo que han hecho las empresas en este tercer año de evaluación por facilitar a las personas interesadas la información sobre sus políticas de protección de datos. La mayoría de empresas tienen hoy mejores documentos.
- Se debe destacar que algunas empresas, como Telefónica-Movistar y ETB, han hecho un esfuerzo importante para comunicarle a las personas, de forma clara y más allá de la formalidad establecida en la ley colombiana, cuáles son sus políticas corporativas relacionadas con la protección de sus datos.
- De acuerdo con la información pública disponible en sus sitios web, varias empresas se comprometen a notificar a las personas cuando terceros solicitan su información; es el caso de Claro, Telefónica-Movistar, ETB y Directv. Este compromiso es interesante puesto que facilita el cumplimiento de estándares internacionales de derechos humanos. Aunque los derechos de defensa y debido proceso son una responsabilidad del Estado, el apoyo de las empresas, sin duda, se convierte en una garantía de respeto a los derechos humanos.<sup>10</sup>
- Solamente dos de las empresas evaluadas, Telefónica-Movistar y Directv, informan sobre su obligación de conservar datos de las personas e información sobre

---

<sup>9</sup> Aunque en Colombia, las empresas proveedoras de internet no están obligadas a presentar informes de transparencia –en los que se comunica al público qué información privada han solicitado y/o han accedido entidades gubernamentales–, es una práctica cada vez más extendida en el mundo por empresas similares.

<sup>10</sup> *Principios necesarios y proporcionales, op. cit.* (nota 6).

el uso que hacen de sus servicios.<sup>11</sup> La defensa de los derechos de las personas depende también de que haya información completa sobre la forma en que la empresa cumple este tipo de obligaciones legales.

- Algunas empresas tienen una política de género que está publicada en su sitio web; es el caso de Telefónica-Movistar y de Directv. Consideramos que esta es una buena práctica y que debe resaltarse en la medida en que promueve la diversidad y facilita la efectiva protección de los derechos de las personas de cara a las políticas y prácticas de las empresas en general.
- Telefónica-Movistar ha hecho un esfuerzo importante por difundir la política pública de accesibilidad del MinTIC. Esta política consiste en impulsar y dar a conocer la oferta que tiene el Estado de un software gratuito que le permite a las personas con discapacidad visual acceder a los contenidos que se encuentran en internet. Con esa práctica, la empresa está favoreciendo el uso de estas herramientas para que cada vez más personas puedan acceder a sus servicios y, a su vez, conocer sus derechos.
- Aunque todas las empresas evaluadas anuncian su compromiso con la defensa de los derechos de los niños, niñas y adolescentes, y se comprometen a tomar medidas contra la distribución de material de explotación sexual infantil, salvo ETB las empresas no explican el procedimiento que implementan para bloquear este tipo de contenidos y la forma como se protege la libertad de expresión de abusos en la aplicación de esta norma.
- Solamente una de las empresas evaluadas, ETB, en varios documentos desarrolla su compromiso con la libertad de expresión de las personas que utilizan sus servicios. Esta empresa ofrece guías sobre comportamientos no permitidos, y políticas sobre usos aceptables que le permiten saber a las personas los parámetros de los servicios y, en consecuencia, entender cuándo pueden ser cancelados o suspendidos.
- ETB, Tigo-UNE y Telebucaramanga aplican el protocolo HTTPS de manera pre-determinada en sus sitios web. Esta es la medida mínima de seguridad digital que se debe adoptar en internet para proteger los datos de las personas que interactúan con sitios web. Cabe resaltar que Emcali también tiene disponible el

---

<sup>11</sup> Esto se conoce como “retención y conservación de datos de personas”. Consiste en la obligación legal que tienen las empresas proveedoras de servicios de internet de almacenar diferentes datos personales de sus clientes. Esos datos involucran el uso que le dan a los servicios de telecomunicaciones, así como la ubicación geográfica de sus celulares. Esta información debe ser conservada por cinco años y debe ser entregada a las autoridades correspondientes para fines de investigación criminal y labores de inteligencia. Es importante considerar que estas empresas también guardan datos para propósitos propios de la prestación del servicio y comerciales. Para mayor información, revise las obligaciones del artículo 44 de la Ley 1621 de 2013 y del Decreto 1704 de 2011. Véase, además, Castañeda, J.D. (2015, 28 de febrero). La retención de datos en Colombia, una de las más largas del mundo. *Digital Rights Latin America and the Caribbean*. Disponible en <https://www.digitalrightslac.net/es/la-retencion-de-datos-en-colombia-una-de-las-mas-largas-del-mundo/> o los *Principios necesarios y proporcionales*, op. cit. (nota 6).


protocolo HTTPS, sin embargo, una persona que no tenga conocimiento sobre este tema entrará automáticamente a la versión insegura del sitio.

- Tigo-UNE y Telebucaramanga consideran las brechas de seguridad como una amenaza digital y muestran su compromiso de mitigarlas si llegaran a suceder. La *Ley de protección de datos* obliga a las empresas a informar sobre sus brechas de seguridad. Vale aclarar que en este criterio, solo evaluamos el compromiso de las empresas por informar al respecto y mostrar cómo actuarían para mitigar el impacto de esas brechas de seguridad, no si cumplen con esta obligación legal.

¿Cómo cuida  
tu proveedora  
de internet  
***tus datos  
personales?***

Fundación  
**Karisma**

**E**

 **accessnow**

The infographic features a green border and a circular icon in the top right corner containing a stylized human figure with colorful dots. On the right side, there are several vertical orange and yellow bars of varying heights.



	SUMA POR CRITERIO	PROMEDIO POR EJE
<b>COMPROMISOS POLÍTICOS</b>		
Política de género		
Política de accesibilidad		
Informes de transparencia		
<b>INTIMIDAD</b>		
Políticas de protección de datos		
Informa la obligación legal de retención de datos		
Informa las razones para responder a solicitudes de información de gobierno y personas privadas		
Procedimiento de entrega de datos		
Notificación a las personas de entrega de datos		
<b>LIBERTAD DE EXPRESIÓN</b>		
Procedimientos de bloqueo		
Procedimiento de cancelación		
Guía sobre comportamientos no permitidos		
<b>SEGURIDAD DIGITAL</b>		
Informa de fuga de datos personales y acciones de mitigación		
Uso de protocolo de seguridad (HTTPS) en su sitio web		

	SUMA POR CRITERIO	PROMEDIO POR EJE
<b>COMPROMISOS POLÍTICOS</b>		
Política de género		
Política de accesibilidad		
Informes de transparencia		
<b>INTIMIDAD</b>		
Políticas de protección de datos		
Informa la obligación legal de retención de datos		
Informa las razones para responder a solicitudes de información de gobierno y personas privadas		
Procedimiento de entrega de datos		
Notificación a las personas de entrega de datos		
<b>LIBERTAD DE EXPRESIÓN</b>		
Procedimientos de bloqueo		
Procedimiento de cancelación		
Guía sobre comportamientos no permitidos		
<b>SEGURIDAD DIGITAL</b>		
Informa de fuga de datos personales y acciones de mitigación		
Uso de protocolo de seguridad (HTTPS) en su sitio web		

 Bonificación por uso de lenguaje inclusivo



SUMA POR  
CRITERIO

PROMEDIO  
POR EJE

**COMPROMISOS  
POLÍTICOS**

Política de género



Política de accesibilidad



Informes de  
transparencia



**INTIMIDAD**

Políticas de  
protección de datos



Informa la  
obligación legal  
de retención de datos



Informa las razones para  
responder a solicitudes de  
información de gobierno y  
personas privadas



Procedimiento de  
entrega de datos



Notificación a  
las personas de  
entrega de datos



**LIBERTAD  
DE EXPRESIÓN**

Procedimientos  
de bloqueo



Procedimiento  
de cancelación



Guía sobre  
comportamientos  
no permitidos



**SEGURIDAD  
DIGITAL**

Informa de fuga de  
datos personales y  
acciones de mitigación



Uso de protocolo  
de seguridad (HTTPS)  
en su sitio web





**SUMA POR  
CRITERIO**

**PROMEDIO  
POR EJE**

**COMPROMISOS  
POLÍTICOS**

Política de género		
Política de accesibilidad		
Informes de transparencia		

**INTIMIDAD**

Políticas de protección de datos		
Informa la obligación legal de retención de datos		
Informa las razones para responder a solicitudes de información de gobierno y personas privadas		
Procedimiento de entrega de datos		
Notificación a las personas de entrega de datos		

**LIBERTAD  
DE EXPRESIÓN**

Procedimientos de bloqueo		
Procedimiento de cancelación		
Guía sobre comportamientos no permitidos		

**SEGURIDAD  
DIGITAL**

Informa de fuga de datos personales y acciones de mitigación		
Uso de protocolo de seguridad (HTTPS) en su sitio web		



SUMA POR  
CRITERIO

PROMEDIO  
POR EJE

**COMPROMISOS  
POLÍTICOS**

Política de género



Política de accesibilidad



Informes de  
transparencia



**INTIMIDAD**

Políticas de  
protección de datos



Informa la  
obligación legal  
de retención de datos



Informa las razones para  
responder a solicitudes de  
información de gobierno y  
personas privadas



Procedimiento de  
entrega de datos



Notificación a  
las personas de  
entrega de datos



**LIBERTAD  
DE EXPRESIÓN**

Procedimientos  
de bloqueo



Procedimiento  
de cancelación



Guía sobre  
comportamientos  
no permitidos



**SEGURIDAD  
DIGITAL**

Informa de fuga de  
datos personales y  
acciones de mitigación



Uso de protocolo  
de seguridad (HTTPS)  
en su sitio web







**SUMA POR  
CRITERIO**

**PROMEDIO  
POR EJE**

**COMPROMISOS  
POLÍTICOS**

Política de género		
Política de accesibilidad		
Informes de transparencia		

**INTIMIDAD**

Políticas de protección de datos		
Informa la obligación legal de retención de datos		
Informa las razones para responder a solicitudes de información de gobierno y personas privadas		
Procedimiento de entrega de datos		
Notificación a las personas de entrega de datos		

**LIBERTAD  
DE EXPRESIÓN**

Procedimientos de bloqueo		
Procedimiento de cancelación		
Guía sobre comportamientos no permitidos		

**SEGURIDAD  
DIGITAL**

Informa de fuga de datos personales y acciones de mitigación		
Uso de protocolo de seguridad (HTTPS) en su sitio web		



	SUMA POR CRITERIO	PROMEDIO POR EJE
<b>COMPROMISOS POLÍTICOS</b>		
Política de género		
Política de accesibilidad		
Informes de transparencia		
<b>INTIMIDAD</b>		
Políticas de protección de datos		
Informa la obligación legal de retención de datos		
Informa las razones para responder a solicitudes de información de gobierno y personas privadas		
Procedimiento de entrega de datos		
Notificación a las personas de entrega de datos		
<b>LIBERTAD DE EXPRESIÓN</b>		
Procedimientos de bloqueo		
Procedimiento de cancelación		
Guía sobre comportamientos no permitidos		
<b>SEGURIDAD DIGITAL</b>		
Informa de fuga de datos personales y acciones de mitigación		
Uso de protocolo de seguridad (HTTPS) en su sitio web		

# Conclusiones

▮ **A** partir del trabajo del tercer informe, podemos decir que en 2017 los resultados muestran cambios positivos, pero las empresas tienen resultados deficientes en la publicación de informes de transparencia y en la adopción de políticas en contra de la discriminación (de género o por discapacidad). No obstante, las empresas que han sido evaluadas durante los últimos 3 años nuevamente mostraron interés en mejorar sus prácticas y en mantener un diálogo más abierto con la sociedad civil.

Como en años anteriores, las empresas evaluadas aún tienen un importante camino por recorrer para mostrar un verdadero compromiso con proteger y respetar los derechos a la libertad de expresión, la intimidad y a ser más cuidadosas con la seguridad digital en los servicios digitales que proveen.

## I. Transparencia

Alrededor del mundo las empresas que ofrecen servicios de internet han estado implementando informes de transparencia con el fin de entregar a las personas información sobre la forma como cumplen con las normas legales sobre suministro de datos a requerimiento de las autoridades. Esta información es muy importante para que la sociedad civil pueda hacer un control independiente de las actuaciones del Estado y para evitar que entren en conflicto con estándares internacionales de derechos humanos.

De las siete empresas evaluadas, cuatro forman parte de multinacionales. Dos de las matrices de esas multinacionales, Millicom (Tigo-UNE) y Telefónica (Movistar), publican informes de transparencia adoptando esta buena práctica internacional. Las otras dos, AT&T (Directv) y América Móvil (Claro), aún no la adoptan. Sin embargo, América Móvil México está obligada legalmente a presentar informes anuales de transparencia. La buena práctica global, que se ha convertido en un ejemplo mundial, no ha llegado a Colombia. Las filiales locales de Millicom y Telefónica no han incorporado esta práctica, ni siquiera reseñan los informes ni la información sobre el país en sus sitios web locales y en todo caso, la información que ofrecen sobre el país es mínima.

Durante 2017, fue ETB, empresa nacional que no tiene vínculos con multinacionales, la primera en publicar este tipo de información y ponerse así a tono con la buena práctica internacional. El trabajo de Karisma buscará que más empresas se unan a esta práctica y nos permitan como sociedad civil analizar los datos que tales informes arrojen.

La información publicada por ETB muestra que muchas entidades públicas solicitan información en Colombia aunque no siempre la empresa suministra la información

solicitada. Las peticiones de las autoridades se refieren a datos biográficos, pero, según lo indica ETB, suelen ir acompañadas también de peticiones de geolocalización. La sociedad civil debe analizar estos datos y el nivel de intromisión a la intimidad de las personas que representan este tipo de solicitudes.

Finalmente, para ser la primera vez que analizamos políticas de las empresas en materia de género y accesibilidad nos sorprendimos gratamente de ver que es un tema que están considerando. En Karisma creemos que implementar políticas corporativas en estos temas incrementa las posibilidades de que la tecnología sea un factor de desarrollo y que sirva de herramienta para favorecer el ejercicio de derechos humanos en ambientes diversos.

## II. Intimidad

En las dos evaluaciones anteriores nos sorprendió ver cómo las políticas de protección de datos de las empresas eran documentos legales, descritos en forma compleja para la población común y usando formatos técnicos que no permiten su reutilización. Para 2017, la evolución de los documentos en las cinco empresas evaluadas desde el primer informe es importante.

Los esfuerzos que este año hicieron ETB y Telefónica-Movistar por mejorar la información hace que ahora sus políticas de tratamiento de datos personales se presenten en formatos más claros, accesibles y con más detalles sobre sus prácticas. Sin embargo, igual que las demás empresas, tanto ETB como Telefónica-Movistar, mantienen documentos que son de difícil lectura y no son documentos navegables. Parece que de esa manera es que las empresas entienden que cumplen formalmente con el requisito legal de publicar sus políticas de protección de datos. ¿Será que es eso lo que espera la Superintendencia de Industria y Comercio, que es la autoridad de protección de datos en Colombia?

Establecer que las empresas se comprometen a notificar a las personas cuando alguien solicita información sobre ellas es otro hallazgo muy importante en la defensa de la intimidad. Para garantizar el debido proceso y el derecho a la defensa en casos de vigilancia de las comunicaciones, la persona que está siendo sujeta a vigilancia debe ser notificada de la decisión. Esto le permite defenderse o buscar otra solución. Con base en los estándares internacionales de derechos humanos, la demora en realizar esta notificación debe ser excepcional y debe justificarse; en cualquier otro caso, se deberá notificar a la persona.<sup>12</sup> Aunque es una obligación del Estado, las empresas proveedoras pueden hacerlo por voluntad o a petición, precisamente, como un compromiso con la defensa del derecho a la intimidad de quienes confían en ellas sus datos.

---

<sup>12</sup> De acuerdo a los *Principios necesarios y proporcionales*, la demora en notificar se justifica cuando se pone en peligro la finalidad para la que se autoriza la vigilancia, peligrando una vida humana, o porque la propia autoridad judicial así lo define. Véase el Principio No. 8, disponible en <https://necessaryandproportionate.org/es/necesarios-proporcionados>.

### III. Libertad de expresión

Estamos viendo una preocupante tendencia en el mundo en la que los gobiernos presionan a las empresas proveedoras de internet para que bloqueen, corten contenidos, URL, servicios de internet o cuentas. Probablemente, estas acciones incrementarían de varias formas: desde cortes generales de internet a la población hasta bloqueos selectivos para evitar que las personas accedan a aplicativos o contenidos determinados.

En la actualidad, en Colombia la ley solo contempla el bloqueo de material relacionado con abuso sexual de niños, niñas y adolescentes.<sup>13</sup> Esto es lo que reconocen las empresas en sus políticas, y en consecuencia se comprometen a defender sus derechos cumpliendo con estas disposiciones. ETB es la única empresa que va más allá y explica el procedimiento que usan en estos casos. Ninguna de las empresas evaluadas lo hace respecto a esta ni a otra circunstancia.

A parte de este tema existen otro tipo de bloqueos. Como lo demuestra la información suministrada por ETB también se dan por órdenes judiciales y por *phishing*. Incluso, las empresas pueden adoptar condiciones y términos de uso, en donde definan otros comportamientos o acciones que pueden provocar que una persona pierda su condición de cliente. En este sentido, creemos que es importante impulsar la transparencia en el comportamiento de las empresas cuando se enfrentan a circunstancias que pueden significar que se vean interesadas u obligadas a bloquear o cortar sus servicios de internet, o, por razones muy similares, cancelar cuentas y servicios de sus clientes.

### IV. Seguridad digital

Las personas pueden tener comportamientos y adoptar herramientas más seguras, pero creemos que las empresas proveedoras de internet pueden también implementar medidas más seguras y ofrecer más información sobre la forma como mitigan las brechas de seguridad que se pueden presentar, se trata de trabajar en la construcción de confianza que es una buena medida para mejorar la seguridad digital.

En la primera evaluación que se hace en materia de seguridad digital es necesario resaltar los resultados de Tigo-UNE y de Telebucaramanga. Estas empresas no solo ofrecen información sobre la forma como actúan frente a brechas de seguridad, sino que, además, implementan el protocolo HTTPS de forma predeterminada, al igual que ETB. En todo caso, como ni Claro ni Telefónica-Movistar obtienen resultados positivos en esta medición debemos llamar la atención en nombre de la mayoría de usuarios del país, pues estas dos empresas tendrían juntas buena parte del mercado colombiano

---

<sup>13</sup> Véase la Ley 679 de 3 de agosto de 2001 y el Decreto 1524 de 23 de julio de 2002.

# Metodología

## I. Ejes temáticos

Para la realización de ¿Dónde están mis datos? 2017 empleamos un sistema de evaluación basado en la necesidad de examinar los compromisos públicos de las empresas proveedoras de internet tanto en el aspecto de políticas corporativas como en el respeto y la atención que ofrecen a la intimidad, la libertad de expresión y la seguridad digital de las personas que usan sus servicios.

En consecuencia, los ejes que evaluamos son:

**Compromisos políticos.** Entendemos que las políticas que las empresas adoptan en diferentes temas es la forma como materializan los compromisos políticos. Son la manera en la que las empresas dan importancia a problemáticas sociales. Nos interesa analizar y promover aquellas problemáticas con las que estas empresas pueden generar un compromiso hacia la inclusión e igualdad, y una responsabilidad frente a la transparencia de sus operaciones. Inicialmente, la manera en la que medimos esto es considerando que las empresas tengan políticas de género y de accesibilidad para personas con discapacidad, y que publiquen un informe de transparencia (o su equivalente) para Colombia, al menos anualmente.

**Intimidad.** Las empresas demuestran a través de formas concretas el respeto a la intimidad de las personas que contratan sus servicios. La intimidad es un derecho fundamental, reconocido en el Artículo 15 de la *Constitución Política de Colombia*. La evaluación busca ir más allá de las normas de protección de datos, por lo que se evalúa que las empresas adopten políticas de protección de datos. Además, se tiene en cuenta que informen sobre la obligación legal que tienen de retener datos, las bases legales por las que están obligadas a atender solicitudes de información de datos de las personas, los procedimientos que usan para entregar esos datos y si notifican a las personas sobre la entrega de datos a terceros.

**Libertad de expresión.** El rol de las empresas proveedoras de internet es clave para el respeto a la libertad de expresión de las personas que contratan sus servicios. Considerando que la libertad de expresión es un derecho fundamental reconocido en el Artículo 20 de la *Constitución Política de Colombia*, en nuestra evaluación tenemos en cuenta que las empresas realicen un esfuerzo por proteger ese derecho a través de la divulgación de sus procedimientos de bloqueo y de la cancelación de servicios. Además,

consideramos que la empresa tenga una guía de comportamientos no permitidos que le posibilite a las personas entender cuáles son sus derechos y sus deberes en ese sentido.

**Seguridad digital.** Las empresas demuestran a través de acciones concretas su compromiso de garantizar la seguridad de sus productos y servicios. Nuestro interés en que la seguridad digital haga parte de la agenda de las empresas, en aras de la protección de la información privada de las personas que acceden a sus servicios de internet, es prioritario. Por ello, en nuestra evaluación del 2017 tuvimos en cuenta dos acciones concretas de las empresas. Por un lado, analizamos si informan sobre los procedimientos que emplean en caso de sufrir brechas de seguridad y, por otro, evaluamos si utilizan el protocolo seguro de transmisión de datos (HTTPS) en todos sus sitios web y, particularmente, en aquellos en los que existe un intercambio de información (compras, ventas y/o consultas).

## II. Criterios de evaluación

Son los criterios que evaluamos en cada uno de los ejes.

DEFINICIÓN DE CRITERIOS		
1. Compromisos políticos		(Antes ítem 1)
1.1. Política de género	La empresa publica en su sitio web para Colombia una política comprometida con la promoción de la igualdad de género, que idealmente, incluye acciones concretas en las siguientes áreas: (1) selección y contratación de personal (diversidad sexual y de género); (2) desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos; (3) equilibrio familiar-laboral (e igualdad en beneficios); (4) prevención del acoso sexual; y (5) la promoción de imágenes públicas no sexistas.	Nuevo
1.2. Política de accesibilidad	La empresa publica en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos (ej. sitio web) y de información de sus servicios para personas con discapacidad.	Nuevo
1.3. Informes de transparencia	La empresa publica periódicamente en su sitio web para Colombia informes de transparencia que aborden la forma en que responden a solicitudes de datos personales por parte de terceros (ej. sector público), que ofrezcan claridades sobre la forma en que gestionan esos procesos, y si hacen o no notificaciones pertinentes y puntuales a las personas titulares de los datos. Además, este informe debe incluir una explicación de su rol y de los criterios que emplean en los bloqueos y/o retiros de contenidos, cancelaciones o suspensión de servicios.	

DEFINICIÓN DE CRITERIOS		
2. Intimidad		(Antes ítems 2, 3 y 4)
2.1. Políticas de protección de datos	La empresa publica en el sitio web para Colombia su política de protección de datos.	
2.2. Informa la obligación legal de retención de datos	La empresa informa públicamente que está obligada por ley a retener datos, el tipo de datos que retiene y el tiempo por el que los retiene.	
2.3. Informa las razones para responder a solicitudes de información del sector público y personas privadas	La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada o ha acordado cumplir con solicitudes de datos personales por parte del sector público y/o personas privadas. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa o a dar acceso a datos personales a terceros privados como parte de acuerdos comerciales (ej. publicidad).	
2.4. Procedimiento de entrega de datos al sector público y empresas privadas	La empresa da a conocer su procedimiento para responder a solicitudes de información del sector público y de personas privadas. Para ello, por ejemplo, ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes.	
2.5. Notificación a las personas sobre la entrega de datos a terceros	La empresa notifica a las personas titulares de datos que ha entregado su información en cumplimiento de un requerimiento de solicitud por parte de un tercero.	
3. Libertad de expresión		(Antes ítem 5)
3.1. Procedimientos de bloqueo	La empresa publica en el sitio web para Colombia los procedimientos que emplea para filtrar, retirar o bloquear contenidos indicando los soportes legales (ej. pornografía infantil) y/o contractuales que lo justifican. Aplica en estos procedimientos el debido proceso y, como mínimo, tiene un procedimiento para atender quejas de cualquier persona que crea haber sido indebidamente bloqueada. Estos procedimientos cuentan con criterios de proporcionalidad y necesidad.	
3.2. Procedimiento de cancelación	La empresa publica en el sitio web para Colombia los procedimientos que emplea para suspender y/o cancelar servicios. Aplica en estos procedimientos, el debido proceso y, como mínimo, notifica a la persona afectada para que tenga la oportunidad de defenderse. Estos procedimientos, además, cuentan con criterios de proporcionalidad y necesidad.	



DEFINICIÓN DE CRITERIOS		
3. Libertad de expresión		(Antes ítem 5)
3.3. Guía sobre comportamientos no permitidos	La empresa publica en el sitio web para Colombia 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.	
4. Seguridad digital		(Nuevo ítem)
4.1. Informa los procedimientos para cumplir la obligación legal de informar brechas de seguridad	La empresa informa públicamente su procedimiento para responder a las brechas de seguridad, incluyendo (1) notificación sin demora indebida a las autoridades pertinentes; (2) notificación a las personas afectadas, y (3) el tipo de medidas que la empresa puede tomar para mitigar los daños.	Nuevo
4.2. Uso de protocolo mejorado de transmisión de datos (HTTPS) en su sitio web	La empresa tiene activado de forma predeterminada el protocolo seguro de transmisión de datos (HTTPS) en el sitio web de Colombia.	Nuevo

### III. Indicadores de evaluación

#### A. Indicadores para la evaluación de criterios basados en documentos publicados en las páginas web de las empresas evaluadas

En este examen empleamos un sistema de indicadores que nos permite medir la forma como las empresas proveedoras actúan frente a cada uno de los criterios evaluados:

1. **Publicidad.** Que la información esté publicada. Entendemos que la información es pública cuando se encuentra en el sitio web de la empresa en Colombia y está disponible en español.

La valoración se hace de la siguiente manera:

- El documento es público en el sitio web de la empresa en Colombia y está disponible en español. (4 puntos)
- El documento es público pero no aparece en el sitio web de la empresa en Colombia y/o está en otro idioma. (2 puntos)
- El documento no se encuentra disponible en el sitio web de la empresa en Colombia ni está disponible en español. (0 puntos)

2. **Claridad.** Que la información sea presentada en un lenguaje no técnico, comprensible para cualquier persona. Esto quiere decir que la información es com-

prensible para un público amplio, no especializado, de diferentes edades y en contextos sociales y culturales diversos.

La valoración se hace computando los resultados de la evaluación realizada por Fundación Karisma y por dos personas externas. Las personas externas representan perfiles no especializados (ni en tecnología, ni en derecho) y divergen tanto en género como en edad. Cada una examina partes aleatorias de los textos publicados por las empresas en relación con los criterios de evaluación de **¿Dónde están mis datos?**

Para evaluar la claridad, Fundación Karisma y las personas externas deben leer los textos y escoger la afirmación que mejor represente cada texto de la siguiente manera:

- El texto está escrito en forma sencilla, es de fácil comprensión, no tiene lenguaje técnico o, teniendo lenguaje técnico, está suficientemente explicado y no genera confusiones. (4 puntos)
- El texto está escrito de forma moderadamente compleja, contiene lenguaje técnico que no es suficientemente claro o no está adecuadamente explicado, lo cual dificulta su comprensión. (2 puntos)
- El texto está escrito en forma muy compleja, contiene mucho lenguaje técnico que no está explicado y no se logra su comprensión. (0 puntos)

3. **Facilidad.** Que la información sea fácil de encontrar en el sitio web de la empresa en Colombia (número de clics). Entendemos que la información es fácil de encontrar cuando se encuentra en el sitio web principal de la empresa proveedora y/o tiene un enlace que lleva directamente a esta.

La valoración se hace de la siguiente manera:

- 1 a 2 clics = muy fácil (4 puntos)
- 3 a 4 clics = fácil (2 puntos)
- 5 o más clics = difícil (0 puntos)

4. **Accesibilidad.** Que el mayor número de personas, incluidas aquellas que tienen algún tipo de discapacidad o dificultad para la lectura, puedan utilizar y acceder a la información.

En la evaluación de este año solamente tuvimos en cuenta que la información esté presentada en un documento navegable, en el que puedan realizarse búsquedas, y del que se puedan copiar y pegar partes. Entendemos que esto último aumenta la posibilidad de que la información sea usada efectivamente por más personas para indagar sobre sus derechos y deberes. Además, mejora la probabilidad de que los lectores automáticos la reconozcan para beneficio de personas con dificultad para la lectura.

La valoración se hace de la siguiente manera:

- El documento es navegable, permite búsquedas y se pueden copiar partes del texto. (4 puntos)
  - El documento es navegable o permite búsquedas o se pueden copiar partes del texto. (2 puntos)
  - El documento no es navegable, no permite búsquedas ni copiar partes del texto. (0 puntos)
5. **Lenguaje inclusivo.** Aunque este año no dimos un puntaje al lenguaje inclusivo dentro de la evaluación, los esfuerzos que las empresas hagan por hacer más incluyentes sus documentos, fueron tenidos en cuenta y se bonificaron hasta con un (1) punto. Respecto al lenguaje inclusivo y su importancia en una política de género y contra la discriminación se puede consultar:
- *Guía para el lenguaje incluyente* de la Alcaldía Mayor de Bogotá, Colombia.<sup>14</sup>
  - *Manuales y textos para el lenguaje incluyente*, recopilados por la Universidad Nacional de Colombia.<sup>15</sup>
  - *Guía para el lenguaje inclusivo y no discriminatorio* de CETEO en España.<sup>16</sup>
  - *Guía para la revisión del lenguaje desde una perspectiva de género*, elaborado por la Dra. Mercedes Bengoechea de la Universidad de Alcalá de Henares, España.<sup>17</sup>

## **B. Indicador para el criterio técnico de seguridad digital: implementación del protocolo HTTPS**

Implementar el protocolo HTTPS es la mínima medida de seguridad digital que deben aplicar los responsables de sitios web. Es una práctica que cada vez más se exige a los administradores de sitios web con el fin de proteger la información de sus usuarios. Sin embargo, en algunos casos, aunque se tiene una versión segura del sitio, de forma pre-determinada se ofrece acceso a una versión insegura. Esta es una mala práctica.

Para que se otorguen cuatro puntos en la evaluación de este criterio, se requiere que la empresa tenga implementado de forma predeterminada el protocolo HTTPS en la totalidad de su sitio web. Es decir, que cuando una persona escribe en su navegador la dirección web de la empresa entra automáticamente a la versión segura del sitio.

---

<sup>14</sup> Alcaldía Mayor de Bogotá. (2015). *Guía para el lenguaje incluyente*. Bogotá, Colombia: Secretaria Distrital de Hacienda. Disponible en [http://www.shd.gov.co/shd/sites/default/files/documentos/todo\\_guia\\_lenguaje.pdf](http://www.shd.gov.co/shd/sites/default/files/documentos/todo_guia_lenguaje.pdf).

<sup>15</sup> Universidad Nacional de Colombia. (s.f.) *Manuales y textos sobre lenguaje incluyente*. Disponible en <http://www.humanas.unal.edu.co/nuevo/titulo-manuales-y-textos-sobre-lenguaje-incluyente/>

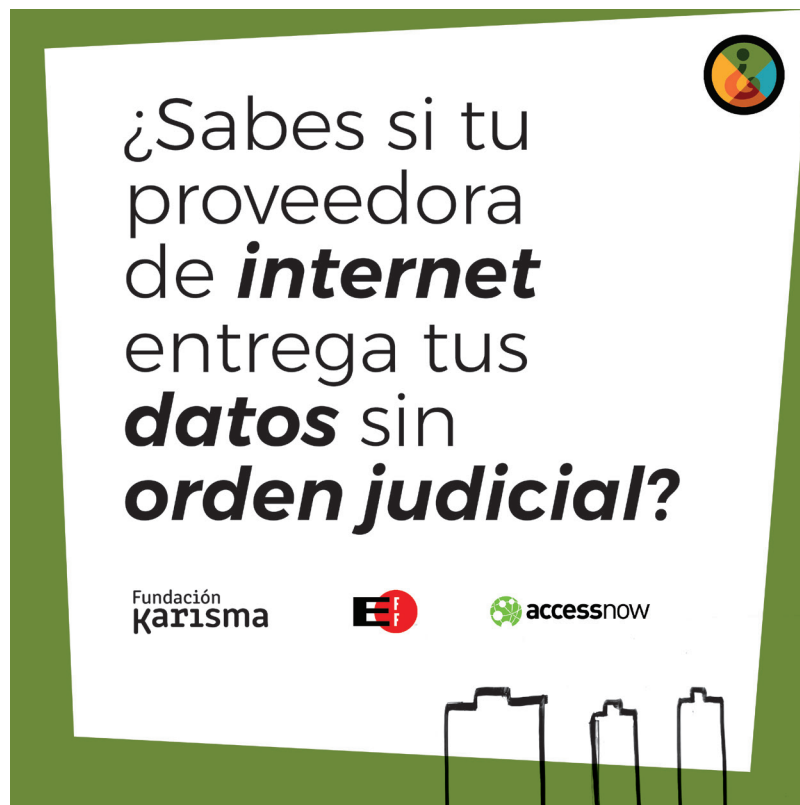
<sup>16</sup> CETEO. (s.f.) *Guía para el lenguaje inclusivo y no discriminatorio*. Disponible en [http://www.aspaymcyf.org/pdf/Memorias/GUIA%20LENGUAJE%20NO%20SEXISTA%20E%20INCLUISVO\\_CETEO.pdf](http://www.aspaymcyf.org/pdf/Memorias/GUIA%20LENGUAJE%20NO%20SEXISTA%20E%20INCLUISVO_CETEO.pdf).

<sup>17</sup> Bengoechea, M. (s.f.). *Guía para la revisión del lenguaje desde una perspectiva de género*. Disponible en <http://www.bizkaia.eus/home2/Archivos/DPTO1/Noticias/Pdf/Lenguaje%20Gu%C3%ADa%20lenguaje%20no%20sexista%20castellano.pdf>.

Es posible que en algunas circunstancias las personas entren a la versión segura del sitio web, a pesar de que la empresa no tienen activada de forma predeterminada la implementación del protocolo HTTPS:

- Ingresando al sitio web de la empresa a través de buscadores que redireccionan a la versión segura del mismo. En esos casos, el mérito es del buscador, no de la empresa.
- Instalando complementos a los navegadores (ej. HTTPS Everywhere) que despliegan de forma automática la versión segura de los sitios web, a pesar de que no sea la versión predeterminada. Nuevamente, en este caso el mérito no es de la empresa, sino de la persona.
- Implementación parcial del protocolo HTTPS para algunas páginas del sitio web (ej. páginas donde hay intercambio de información como compras o autenticaciones).

En ninguno de estos casos otorgamos puntaje, por no cumplir con los componentes del criterio: implementación del protocolo HTTPS y uso en forma predeterminada.



# Evaluación

Los detalles de la evaluación que efectuamos durante el mes de septiembre de 2017 a las páginas web de cada empresa y nuestra lectura de esos resultados se describen a continuación:

## Claro

CLARO	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (homificación)	Suma por criterio	Promedio por eje
<b>1. Compromisos políticos</b>							0
1.1. Política de género	0					0	
1.2. Política de accesibilidad	0					0	
1.3. Informes de transparencia	0					0	
<b>2. Intimidad</b>							3
2.1. Políticas de protección de datos	1	0,75	1	1	0	4	
2.2. Informa la obligación legal de retención de datos	0					0	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,5	0,75	1	0	3	
2.4. Procedimiento de entrega de datos	1	0,5	0,5	1	0	3	
2.5. Notificación a las personas de entrega de datos	1	1	1	1	0	4	
<b>3. Libertad de expresión</b>							0
3.1. Procedimientos de bloqueo	0					0	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0					0	
<b>4. Seguridad digital</b>							0
4.1. Informa de fuga de datos personales y acciones de mitigación	0					0	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	0					0	

### Comentarios:

- + Claro publica una política de protección de datos en la que informa cuáles son las razones que tiene en cuenta para responder a las solicitudes de información del Gobierno o de otras entidades. Por ejemplo, Claro indica que puede atender a una solicitud legal o que puede hacer uso de información que se encuentra en sus bases de datos, previo consentimiento de la persona titular, con fines comerciales.
- + Claro se compromete, en su política de protección de datos, a notificar a las personas en caso de que su información sea solicitada por terceros.
- Claro no hace pública una política de género, así como tampoco lo hace en relación con la accesibilidad para personas con discapacidad.
- Si bien América Móvil, propietaria de Claro, publica anualmente un *informe de sustentabilidad*, este no es un informe de transparencia. El informe trae algunos datos sobre Colombia, especialmente, en materia de seguridad digital, pero no ofrece datos sobre las solicitudes de información personal por parte del Gobierno o de otras entidades.
- Claro no informa a las personas sobre la retención de datos, no habla del tiempo de retención ni del tipo de obligaciones legales que tiene.
- Aunque Claro informa a las personas que contratan sus servicios que existe una ley para la protección de niños, niñas y adolescentes contra el abuso sexual, y contra el material de explotación y abuso sexual infantil, no existe en su sitio web ningún documento que informe los procedimientos de bloqueo o cancelación de contenidos en este tema o en cualquier otro.
- Claro no cuenta con una guía de comportamientos no permitidos que le posibilite a las personas saber claramente cuándo, por qué y cómo pueden perder su calidad de clientes.
- Aunque Claro habla sobre seguridad digital y le pide a quienes contratan sus servicios confiar en la celeridad y efectividad de sus acciones en caso de que exista una amenaza a la seguridad de la información, no hay ningún documento ni información disponible relacionada con la forma como desarrolla ese compromiso, especialmente, frente a una posible fuga de datos y las acciones que podrían llevarse a cabo para mitigarla.
- Claro no utiliza el protocolo HTTPS de forma predeterminada en su sitio web.

## Telefónica-Movistar

Telefónica Movistar	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (homificación)	Suma por criterio	Promedio por eje
<b>1. Compromisos políticos</b>							<b>3</b>
1.1. Política de género	1	1	0,25	1	1	4	
1.2. Política de accesibilidad	1	1	1	1	0	4	
1.3. Informes de transparencia	0,5					1	
<b>2. Intimidad</b>							<b>3</b>
2.1. Políticas de protección de datos	1	0,75	1	1	0	4	
2.2. Informa la obligación legal de retención de datos	1	1	1	1	0	4	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,5	0,5	1	0	3	
2.4. Procedimiento de entrega de datos	1	0,5	0,75	1	0	3	
2.5. Notificación a las personas de entrega de datos	1	0,75	0,5	1	0	3	
<b>3. Libertad de expresión</b>							<b>0</b>
3.1. Procedimientos de bloqueo	0					0	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0					0	
<b>4. Seguridad digital</b>							<b>0</b>
4.1. Informa de fuga de datos personales y acciones de mitigación	0					0	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	0					0	

### Comentarios:

- + Telefónica-Movistar publica en su sitio web una política de género exclusiva para nuestro país, en la que hace referencia a la necesidad de hacer más incluyentes sus espacios de trabajo, con el fin de evitar el acoso, de garantizar que el porcentaje de mujeres dentro de su planta laboral aumente y que puedan acceder

- a cargos de liderazgo. En esta política, además, hay un intento por emplear un lenguaje incluyente que muestra su compromiso con la diversidad.
- + Telefónica-Movistar es la única empresa de las evaluadas que impulsa la política estatal de facilitar que las personas con discapacidad visual puedan acceder al software que el MinTIC les ofrece gratuitamente. Aunque la publicación no es tan clara sobre esto y se requiere tener algo de contexto para comprender su alcance, es una iniciativa que consideramos muy positiva.
  - + Telefónica-Movistar informa a las personas sobre la retención de datos de una forma clara que permite saber la duración y los fines por los que se realiza.
  - + Telefónica-Movistar informa las razones por las que podría dar información a terceros y se compromete a notificar a las personas implicadas sobre estas solicitudes.
  - Aunque Telefónica, la matriz, tiene un informe de transparencia a nivel global, que incluye un apartado sobre Colombia, este informe no se encuentra publicado en el sitio web de Telefónica-Movistar Colombia. Además, este informe no es claro en relación con el tipo de solicitudes que recibe por parte de terceros, sean autoridades locales o terceros privados; y cuándo, cómo y porqué puede compartir información de las personas que utilizan sus servicios.
  - Aunque Telefónica-Movistar anuncia su obligación legal para prevenir el abuso sexual contra niños, niñas y adolescentes, no existe en su sitio web ningún documento que informe lo relacionado con procedimientos de bloqueo o cancelación de contenidos en este tema o en cualquier otro. La empresa tampoco publica una guía de comportamientos no permitidos que le permita a las personas que usan sus servicios tener más claridad sobre cómo pueden perder o conservar su calidad de clientes.
  - Aunque Telefónica-Movistar tiene una política sobre seguridad digital, no desarrolla su compromiso en relación con amenazas contra la seguridad de la información y no informa sobre las acciones posibles para mitigarlas.
  - Telefónica-Movistar no utiliza el protocolo de seguridad HTTPS de forma predefinida.



## ETB

ETB	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (bonificación)	Suma por criterio	Promedio por eje
<b>1. Compromisos políticos</b>							<b>1</b>
1.1. Política de género	0					0	
1.2. Política de accesibilidad	0					0	
1.3. Informes de transparencia	1	0,75	0,75	1		4	
<b>2. Intimidad</b>							<b>3</b>
2.1. Políticas de protección de datos	1	0,5	0,75	1		3	
2.2. Informa la obligación legal de retención de datos	1	0,5	0,75	1		3	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,75	0,75	1		4	
2.4. Procedimiento de entrega de datos	1	0,5	0,75	1		3	
2.5. Notificación a las personas de entrega de datos	1	0,75	0,75	1		4	
<b>3. Libertad de expresión</b>							<b>3</b>
3.1. Procedimientos de bloqueo	1	1	0,75	1		4	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	1	1	0,75	1		4	
<b>4. Seguridad digital</b>							<b>2</b>
4.1. Informa de fuga de datos personales y acciones de mitigación	0					0	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	1	1	1	1		4	

### Comentarios:

- + ETB es la única empresa evaluada que publica información periódicamente sobre solicitudes de información. Aunque ETB no lo nombra como tal, para Fundación Karisma, este tipo de documento equivale a un informe de transparencia. ETB indica el tipo de solicitudes que recibe y las entidades gubernamentales que las hacen.

- + ETB publica una política de protección de datos en la que informa sobre la retención de datos, las razones para responder a solicitudes del Gobierno, o de otros, y para dar información. Además, da cuenta de sus procedimientos para entregar datos y anuncia que notificará a las personas titulares de los datos.
- + ETB publica tres documentos relacionados con la libertad de expresión de las personas: (1) los procesos que usa para el bloqueo de contenidos relacionados con abuso sexual infantil, (2) las políticas de uso aceptable de sus servicios, y (3) unos códigos de conducta que equivalen a una guía sobre comportamientos no permitidos, puesto que orientan a las personas sobre la forma como ETB procede para mantener sus servicios.
- + ETB utiliza en su sitio web el protocolo HTTPS de forma predeterminada.
- ETB no tiene una política de género pública.
- ETB no tiene una política de accesibilidad pública.
- ETB no da cuenta de cuáles son los procedimientos que emplea para la cancelación de sus servicios.
- Aunque ETB menciona la necesidad de la seguridad digital y pide a las personas que tengan confianza en sus procedimientos, no da cuenta sobre su compromiso de informar ante brechas de seguridad ni comunica las acciones que desarrollaría para mitigarlas.

## Directv

DIRECTV	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (homificación)	Suma por criterio	Promedio por eje
<b>1. Compromisos políticos</b>							2
1.1. Política de género	1	1	0,75	1		4	
1.2. Política de accesibilidad	0					0	
1.3. Informes de transparencia	0,5	0	0	0		1	
<b>2. Intimidad</b>							3
2.1. Políticas de protección de datos	1	0,75	0,75	1	0	4	
2.2. Informa la obligación legal de retención de datos	1	0,5	0,75	1	0	3	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,75	0,75	1	0	4	
2.4. Procedimiento de entrega de datos	0					0	
2.5. Notificación a las personas de entrega de datos	1	1	0,75	1	0	4	
<b>3. Libertad de expresión</b>							0
3.1. Procedimientos de bloqueo	0					0	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0					0	
<b>4. Seguridad digital</b>							0
4.1. Informa de fuga de datos personales y acciones de mitigación	0					0	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	0					0	

### Comentarios:

- + Directv tiene un código de ética que contempla la necesidad de incluir la diversidad sexual y de género como parte de sus políticas de igualdad. Esta política está dirigida a generar igualdad de oportunidades y a evitar el acoso laboral.

- + Directv publica una política de protección de datos en la que informa sobre la retención de datos. Además, da cuenta de las razones para responder a solicitudes de terceros que pidan información de las personas, por ejemplo, por una orden legal o un contrato comercial (con previo consentimiento del titular).
- + Directv se compromete a notificar a las personas titulares de los datos sobre las solicitudes de información por parte de terceros y los usos que puedan hacer de sus bases de datos.
- Aunque AT&T, matriz de Directv, tiene un informe de transparencia global en el que menciona a Colombia, este informe no se encuentra publicado en el sitio web de Directv Colombia. En todo caso, la información es insuficiente porque tampoco es clara en relación con el tipo de solicitudes que recibe por parte de terceros (sean autoridades locales o privados) ni cómo, cuándo y por qué puede dar información de las personas que utilizan sus servicios.
- Aunque Directv, como las demás empresas, tiene la obligación legal de evitar la propagación de material relacionado con el abuso sexual de niños, niñas y adolescentes, no tiene publicados en su sitio web documentos relacionados con los procedimientos que emplea para hacer el bloqueo de contenidos de este tipo o de cualquier otro. Tampoco tiene una guía de comportamientos no permitidos que facilite a quienes contratan sus servicios conocer cómo pueden perder o conservar su calidad de clientes.
- Directv no emplea en su sitio web el protocolo de seguridad HTTPS.
- Directv tiene en cuenta la seguridad digital y le pide a quienes contratan sus servicios confiar en sus procedimientos para prevenir amenazas a la seguridad de la información. Sin embargo, no da cuenta sobre su compromiso de informar sobre brechas de seguridad ni de las acciones que llevará a cabo para mitigarlas.

## Tigo-UNE

TIGO UNE	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (bonificación 1 punto)	Suma por criterio	Promedio por eje
<b>1. Compromisos políticos</b>							2
1.1. Política de género	1	0,5	0,5	1		3	
1.2. Política de accesibilidad	1	0,5	0,5	1		3	
1.3. Informes de transparencia	0,5					1	
<b>2. Intimidad</b>							2
2.1. Políticas de protección de datos	1	0,75	1	1		4	
2.2. Informa la obligación legal de retención de datos	0					0	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,5	1	1		4	
2.4. Procedimiento de entrega de datos	0					0	
2.5. Notificación a las personas de entrega de datos	0					0	
<b>3. Libertad de expresión</b>							0
3.1. Procedimientos de bloqueo	0					0	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0					0	
<b>4. Seguridad digital</b>							4
4.1. Informa de fuga de datos personales y acciones de mitigación	0,5	0,25	0,75	1		3	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	1	1	1	1		4	

### Comentarios:

- + Tigo-UNE publica un código de ética en el que habla de la necesidad de tener políticas inclusivas de diversidad sexual y de género. No obstante, solo es una mención y no constituye, en sí misma, una política amplia y clara.

- + Tigo-UNE menciona en su código de ética la necesidad de hacer más accesibles sus servicios en consideración con las personas con discapacidad.
- + Tigo-UNE publica sus políticas de protección de datos en las que informa las razones por las que puede responder a solicitudes de información por parte del Gobierno o de otras entidades privadas.
- + Tigo-UNE se compromete a informar sobre brechas de seguridad que comprometan información de las personas que contratan sus servicios y las acciones que podrían llevar a cabo para evitarlas y/o contrarrestarlas.
- + Tigo-UNE utiliza en su sitio web el protocolo de seguridad HTTPS de forma pre-determinada.
- Tigo-UNE no informa sobre su obligación de hacer retención de datos ni cómo la aplica.
- Tigo-UNE no se compromete a notificar a las personas cuando terceros, sean autoridades locales o privados, soliciten su información. Tampoco hace mención a los procedimientos que podría llevar a cabo para hacer esta entrega.
- Tigo-UNE no publica en su sitio web ningún documento relacionado con la libertad de expresión de las personas que utilizan sus servicios. Al igual que las demás empresas, menciona su compromiso contra la difusión de material relacionado con el abuso sexual de niños, niñas y adolescentes. No obstante, no informa los procedimientos que aplica cuando esto supone bloqueos de contenidos ni en este caso ni en ningún otro. La empresa no tiene una guía de comportamientos no permitidos ni tampoco algún documento sobre usos aceptables de sus servicios, que le permita saber a las personas cuándo, cómo o porqué pueden perder su calidad de clientes.

## Emcali

EMCALI	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (bonificación 1 punto)	Suma por criterio	Promedio por eje (máx. 5 puntos)
<b>1. Compromisos políticos</b>							<b>0</b>
1.1. Política de género	0					0	
1.2. Política de accesibilidad	0					0	
1.3. Informes de transparencia	0					0	
<b>2. Intimidad</b>							<b>0</b>
2.1. Políticas de protección de datos	1	0,25	0,25	0,25		2	
2.2. Informa la obligación legal de retención de datos	0					0	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	0					0	
2.4. Procedimiento de entrega de datos	0					0	
2.5. Notificación a las personas de entrega de datos	0					0	
<b>3. Libertad de expresión</b>							<b>1</b>
3.1. Procedimientos de bloqueo	1	0,25	0,25	0,5		2	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0					0	
<b>4. Seguridad digital</b>							<b>0</b>
4.1. Informa de fuga de datos personales y acciones de mitigación	0					0	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	0					0	

### Comentarios:

- De todos los ejes y criterios que evaluamos, Emcali solo tiene en su sitio web un documento de política de protección de datos. Lamentablemente, esta situación es insuficiente para evaluar los puntos que tenemos en cuenta en ¿Dónde están mis datos? 2017. Esto nos pone alerta sobre la necesidad de sensibilizar a esta empresa respecto a los derechos de las personas que utilizan sus servicios.
- Emcali emplea el protocolo HTTPS pero no lo hace de forma predeterminada, por esta razón no pudimos otorgarle un punto en el eje de Seguridad Digital.

## Telebucaramanga

TELEBUCARAMANGA	Publicidad	Claridad	Facilidad	Accesibilidad	Lenguaje inclusivo (bonificación 1 punto)	Suma por criterio	Promedio por eje (máx. 5 puntos)
<b>1. Compromisos políticos</b>							0
1.1. Política de género	0					0	
1.2. Política de accesibilidad	0					0	
1.3. Informes de transparencia	0					0	
<b>2. Intimidad</b>							2
2.1. Políticas de protección de datos	1	0,5	1	0		3	
2.2. Informa la obligación legal de retención de datos	0					0	
2.3. Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	0,25	1	0		2	
2.4. Procedimiento de entrega de datos	1	0,25	1	0		2	
2.5. Notificación a las personas de entrega de datos	1	0,5	1	0		3	
<b>3. Libertad de expresión</b>							0
3.1. Procedimientos de bloqueo	0					0	
3.2. Procedimiento de cancelación	0					0	
3.3. Guía sobre comportamientos no permitidos	0	0	0	0		0	
<b>4. Seguridad digital</b>							4
4.1. Informa de fuga de datos personales y acciones de mitigación	1	1	1	1		4	
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web	1	1	1	1		4	

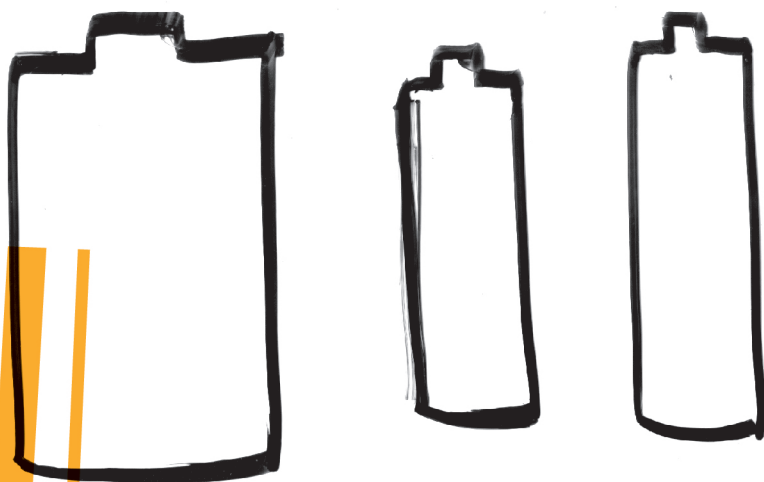
### Comentarios:

- + Telebucaramanga publica en su sitio web una política de protección de datos en la que informa las razones por las que podría dar información a terceros.
- + Telebucaramanga informa a quienes contratan sus servicios sobre los usos que puede dar a la información contenida en sus bases de datos.



- + Telebucaramanga utiliza el protocolo HTTPS de forma predeterminada.
- + Telebucaramanga informa a las personas que utilizan sus servicios sobre el tipo de acciones que emplea para proteger su infraestructura, sus datos y acciones preventivas ante posibles amenazas identificadas.
- + Telebucaramanga se compromete a notificar a las personas en caso de que entregue a terceros información contenida en sus bases de datos.
- Telebucaramanga no tiene públicas políticas de género ni de accesibilidad.
- Telebucaramanga no informa sobre la obligación legal de retención de datos.
- Telebucaramanga no tiene ningún documento publicado en su sitio web en el que refleje su compromiso con la libertad de expresión de quienes contratan sus servicios. Por ejemplo, no hay información acerca del bloqueo de contenidos ni el procedimiento que usan para ello. Tampoco hay una guía de comportamientos no permitidos ni una política de usos aceptables.

El informe ¿Dónde están mis datos? 2017 es la tercera publicación que realiza la Fundación Karisma en busca de impulsar prácticas de transparencia en los intermediarios de Internet. Para conocer y descargar el texto completo de este año visita <https://karisma.org.co/donde-estan-mis-datos-2017/>. Puedes conocer los informes anteriores en <https://karisma.org.co/DEMD/>



Un informe de: \_\_\_\_\_

Fundación  
**Karisma**

Con el apoyo de: \_\_\_\_\_

