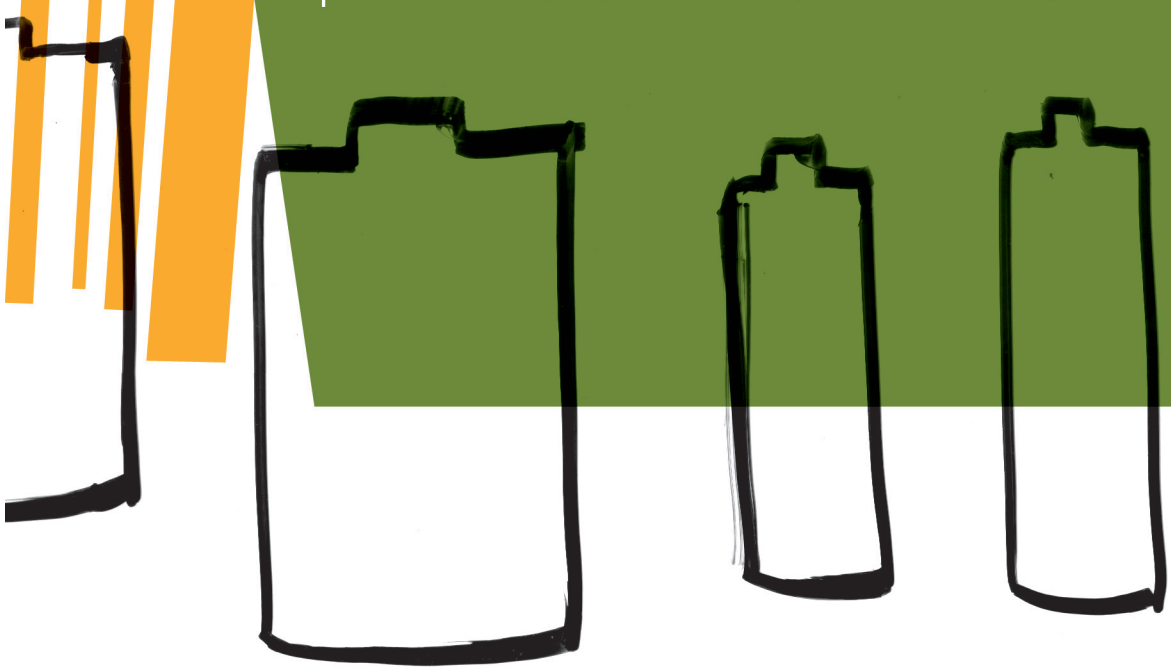
¿dónde están mis datos?

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

¿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

TABLA DE CONTENIDO

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.[1] 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

[1] 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.

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[2]; 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[3]; los documentos de la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH)[4]; los principios del GNI[5] y los *Principios necesarios y proporcionales*[6].

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[7], se incluyeron los criterios sobre políticas de género y accesibilidad.

---

[2] 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.

[3] 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/esresolucin-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

[4] 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; *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/IICIDH/RELE/INF.17/17. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf.

[5] *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.

[6] *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.

[7] 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[8] 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.

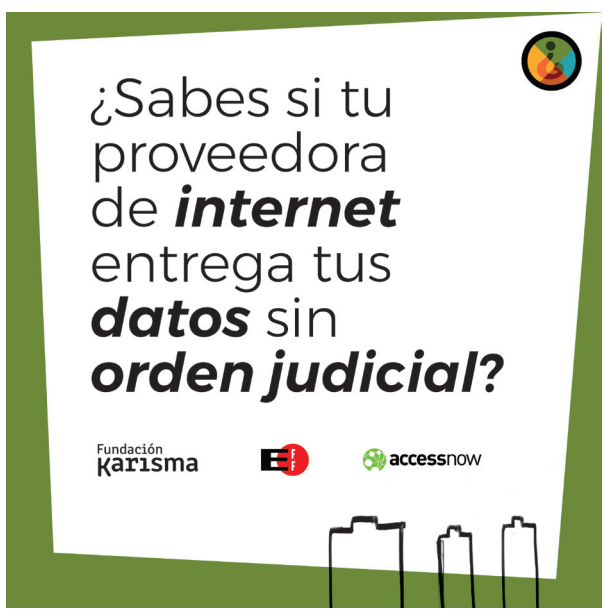
Otro cambio importante en ***¿Dónde están mis datos? 2017*** es que, además de las cinco empresas que se habían evaluado en años anteriores (Claro, Tigo-UNE, Telefónica-Movistar, ETB y Directv), se agregan dos empresas proveedoras de servicios de internet a nivel regional: Emcali y Telebucaramanga. Las 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.

[8] 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 Se debería notificar al cliente o particular cuando la violación de los datos afecte negativamente su intimidad o sus datos 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.

Nota metodológica

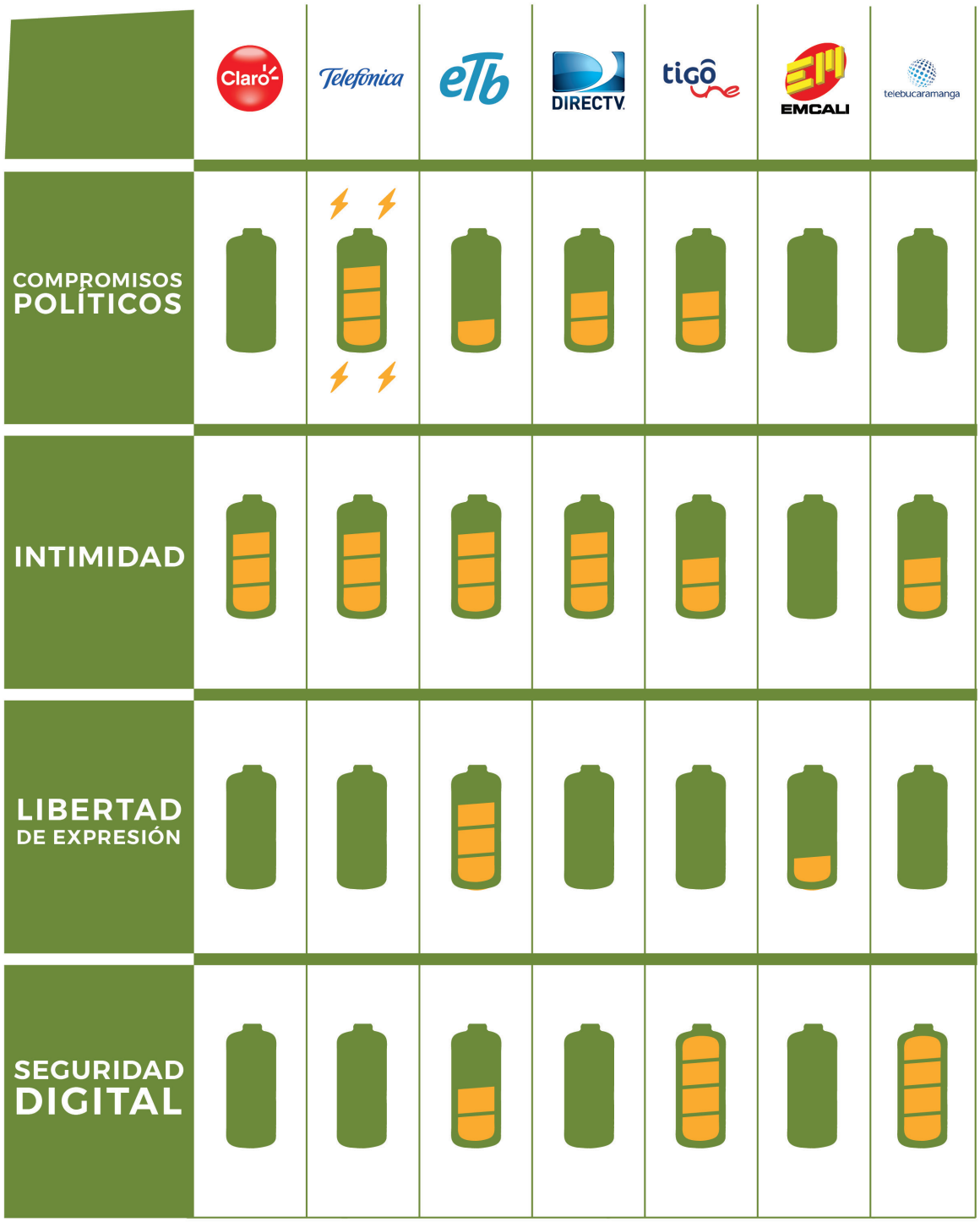
La evaluación[9] de ¿Dónde están mis datos? 2017 se hace a través de cuatro ejes temáticos (compromisos políticos, intimidad, libertad de expresión y seguridad digital). Cada eje temático se analiza a través de criterios determinados que se buscan en la información pública que las empresas evaluadas ofrecen en sus sitios web del país. Con excepción del criterio de implementación del protocolo HTTPS en los sitios web de las empresas (que se encuentra en el eje temático de seguridad digital), el valor que se asigna a cada criterio se mira a la luz de cuatro indicadores (publicidad, claridad, facilidad y accesibilidad) y otro adicional que sirve como bonificación (lenguaje inclusivo). Cuando analizamos la implementación del protocolo HTTPS, tan solo se revisa si existe o no la aplicación predeterminada del mismo para dar o no el puntaje correspondiente.

Los puntajes que obtiene cada empresa resultan de la suma de los valores recibidos en los indicadores para cada criterio. El promedio de los valores otorgados en los criterios –aproximados a la unidad– es el valor de cada eje temático. Las pilas representan esos valores. Tienen 4 niveles de carga que representan la evaluación obtenida por cada empresa, en el caso de existir alguna bonificación, se muestra con un símbolo.



[9] Es importante señalar que la evaluación final se realizó durante el mes de septiembre de 2017. Los cambios que las empresas introdujeron en sus sitios web después de este fecha no aparecen registrados en esta evaluación.

Principales hallazgos



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 y consideramos los datos adicionales que nos suministraron. 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.[10] 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.[11]

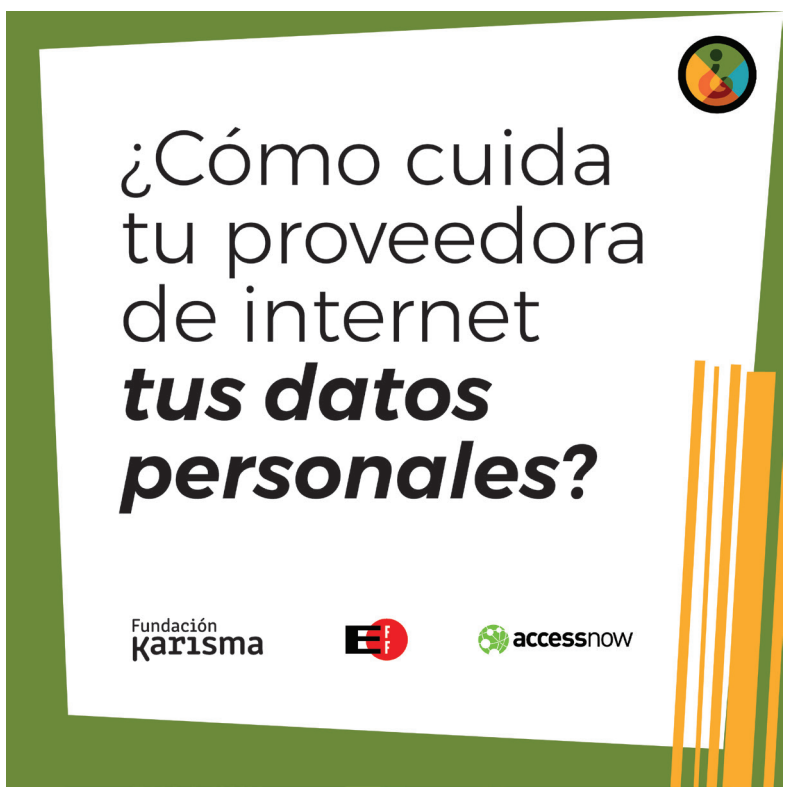
[10] Aunque en Colombia, las empresas proveedoras de internet no están obligadas a presentar informes de transparencia –en los que se comunica al público qué información privada han solicitado y/o han accedido entidades gubernamentales–, es una práctica cada vez más extendida en el mundo por empresas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

[11] *Principios necesarios y proporcionales*, *op. cit.* (nota 6).

- Solamente dos de las empresas evaluadas, Telefónica-Movistar y Directv, informan sobre su obligación de conservar datos de las personas e información sobre el uso que hacen de sus servicios.[12] La defensa de los derechos de las personas depende también de que haya información completa sobre la forma en la 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.

[12] 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).

- ETB, Tigo-UNE y Telebucaramanga aplican el protocolo HTTPS de manera predeterminada 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 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 con mostrar cómo actuarían para mitigar el impacto de esas brechas de seguridad, no si cumplen con esta obligación legal.



Claro

	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 solictudes 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		

Telefónica

	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 solictudes 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		

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 solictudes 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		

DIRECTV

	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 solictudes 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		

tigo une	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 solictudes 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		

EMCALI

	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 solictudes 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		

telebucaramanga

	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 solictudes 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		

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.[13] 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.

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.[14] 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 respecto 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.

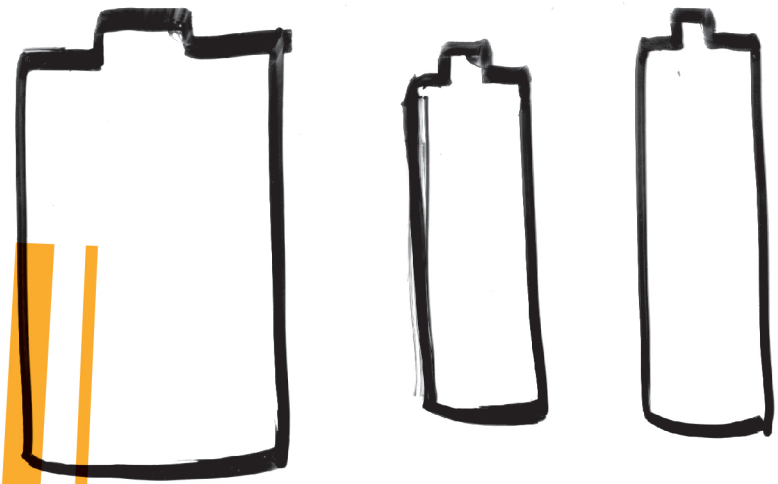
---

[13] 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, peligra 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.

[14] *Véase* la Ley 679 de 3 de agosto de 2001 y el Decreto 1524 de 23 de julio de 2002.

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.

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:

accessnow