

Informe ¿DÓNDE ESTÁN MIS DATOS?

2021:
una mirada
retrospectiva
a la pandemia



Un informe de:

Fundación
Karisma

Con el apoyo de:

E ELECTRONIC
FRONTIER
FOUNDATION **FF**

- 
1. Bienvenida
 2. Presentación general del informe a cargo de Carolina Botero
 3. Presentación de resultados a cargo de Lucía Camacho
 4. Conclusiones y recomendaciones a cargo de Carolina Botero
 5. Reflexiones a cargo de Veridiana Alimonti
 6. Preguntas

1. Presentación general del informe



Dónde están mis datos 2021

Lo hacemos desde 2015.

Evaluamos lo que las empresas dicen que hacen, no si lo hacen o no en la práctica.

DEMD permite que las personas comparen las empresas para elegir a su proveedor de internet considerando cuál protege mejor sus derechos -especialmente los de intimidad y libertad de expresión-. También analiza los compromisos en materia de género, accesibilidad, transparencia y seguridad digital.

Evaluamos a Claro, Movistar, ETB, EmCali, UNE-Tigo, Directv, Avantel y nuevos actores que facilitan la conectividad en la ruralidad: Hughesnet y Skynet.

Este es el primer informe de análisis de la pandemia, lo que motivó a la introducción de modificaciones en nuestra metodología de análisis.

Cambios ...

Este año decidimos introducir dos nuevos criterios de evaluación: neutralidad de la red y acceso directo.

¿La razón?

- **Neutralidad de la red:** Dada la elevada demanda del servicio de internet producto de la virtualidad obligada, el gobierno temió que fuese necesario suspender la neutralidad de la Red, por lo que preparó el terreno con medidas provisionales que desde Fundación Karisma observamos con preocupación.
- **Apetito de datos:** La pandemia también significó un aumento en el apetito del Estado por acceder a los datos de las personas suscriptoras de los servicios de telefonía móvil (ej. Circular 01 de 2020 de la SIC). No encontramos información sobre este tema en los informes de las empresas.

Cambios ...

- **Acceso directo:** La lectura sistemática de los informes producidos por Karisma en los últimos años indican ,por la información de varias empresas, que en Colombia hay “acceso directo” de las autoridades a las redes de los operadores de telefonía celular, usando como base el Decreto 1704 de 2012.
- El acceso directo como mecanismo de interceptación de comunicaciones es *ampliamente cuestionado porque su alcance es muy problemático para la garantía de derechos humanos, especialmente libertad de expresión, intimidad y debido proceso. Es una forma de vigilancia masiva* de las comunicaciones que es fácilmente abusada, que deteriora la confianza pública tanto en la responsabilidad del gobierno como en la fiabilidad y seguridad de las tecnologías de las comunicaciones.

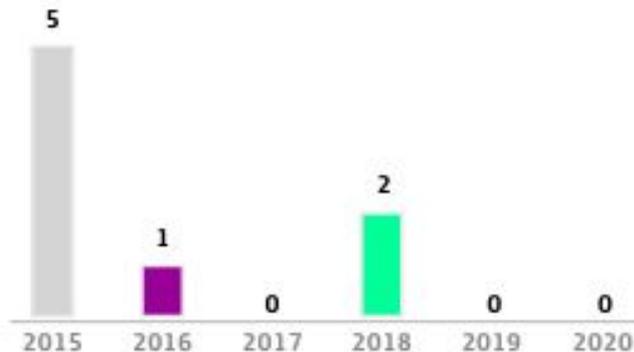
Cambios ...

- **Acceso directo:**

MOVISTAR fue la primera compañía en dar cuenta de esta situación en su informe sobre Colombia (2017).

Hay que considerar que a nivel global Telefónica identifica los “major events” como situaciones de fuerza mayor que los obligan, por ejemplo, a hacer “cambios operacionales significativos” y dentro de estos está el acceso abierto por parte de agencias de gobierno.

Solicitudes*



*Solicitudes sobre líneas fijas

Líneas móviles: No se reportan interceptaciones sobre líneas móviles: La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa sobre las líneas móviles.

Accesos afectados 0

Solicitudes rechazadas 0

Cambios ...

- **Acceso directo:**

Claro y Tigo. En sus informes dan cuenta de un marco legal que lo facilita. Podrían ser más claros.

Millicom (Matriz de Tigo) en su informe global hace un análisis del marco legal de la región y es clara al señalar que en Colombia existe acceso directo y que no establecer sus proporciones puede acarrear importantes sanciones a la empresa (este informe se encuentra en inglés y no está enlazado en la página de Tigo Colombia, por lo que no es considerado en la evaluación de 2021).

Informe de Millicom

Legal frameworks

In Bolivia and Paraguay, clear processes and requirements exist for judicial oversight over interception and customer metadata requests. In Colombia, due largely to the long-lasting internal conflicts and war on drugs, the processes are significantly more complex. However, judicial oversight does exist for initiation of interception. Information about the laws and procedures in Colombia is published in detail at <https://globalnetworkinitiative.org/policy-issues/legal-frameworks/>.

In Bolivia, the use of interception is restricted to exceptional circumstances, such as human and drug trafficking, in which we would receive court orders to activate lines. We have ongoing discussions with authorities regarding the implementation of interception techniques.

Procedures in Colombia require us to provide direct access for authorities to our mobile network. Regular audits ensure we do not obtain information about interception that is taking place. We are subject to strong sanctions, including fines,

if authorities find that we have gained such information. As a result, we do not possess information regarding how often and for what periods of time communications are intercepted in our mobile networks in Colombia. We also have a significant fixed-network business in Colombia; for these lines, we receive judicial orders, which we review and assess before opening the line for interception to take place. Length of interception is limited by law to a maximum of six months.

In Paraguay, as in Colombia, authorities mandate that we provide direct access to our mobile network. The procedures allow us to view the judicial order required for authorities to initiate the interception, and we are aware when interception occurs. We can file a complaint before the Supreme Court of Justice should we deem that the order or interception does not follow legal requirements.

For customer metadata requests, we receive written orders in all three countries. We assess the legality of these requests before providing authorities with the requested information.



¿Qué evaluamos en neutralidad de la Red y Acceso Directo?

- **[Eje de compromisos políticos]**
 - Neutralidad de la Red: evaluamos que las compañías publiquen sus prácticas de gestión del tráfico y que manifiesten un compromiso para respetar la neutralidad de la Red e informen sobre los eventos en que dicho principio podría llegar a ser limitado o restringido.
- **[Eje de intimidad]**
 - Acceso directo: evaluamos si las empresas informan públicamente sobre la posibilidad de acceso directo que tienen las autoridades públicas a su infraestructura y datos de las comunicaciones de sus suscriptores; si informan el marco legal en que este acceso se justifica; y si explicitan a sus suscriptores su rol o postura ante este tipo de eventos

2. Desempeño y hallazgos





Preliminar

- Este año nuestro informe incluye la sección “de contexto e interés”.
- Organizamos la información de manera que cada eje de evaluación pueda merecer un análisis individual.

En general

- Observamos que las empresas que tradicionalmente hemos evaluado demuestran en general un buen desempeño, los puntajes recibidos no se distancian de los de nuestro informe anterior. Las mejoras observadas se debieron a la atención al detalle que prestaron algunas empresas en la modificación de políticas ya existentes.
- La brecha que separa a las más recientes empresas que evaluamos en nuestro informe y las empresas tradicionales es significativo, esperamos que en ediciones futuras se vaya cerrando paulatinamente.

Principales hallazgos



 movistar	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		4	4
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		3	3
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		4	4
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Tuvo el mejor desempeño nuevamente en esta edición, en general el puntaje no varió significativamente en comparación con el desempeño del año anterior.
- En esta edición obtuvo el mejor puntaje en neutralidad de la Red y en acceso directo gracias a sus esfuerzos por reconocer dicha realidad y que datan desde el año 2017.
- Puede mejorar:
 - Integrando mecanismos de protección a la persona usuaria cuando el Estado solicita sus datos (procesos de notificación a la persona en procedimientos distintos a los de naturaleza penal, por ejemplo).

Principales hallazgos



tigo	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		1	3
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	3
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Este año recibió puntajes en criterios en los que en nuestra edición anterior no había habido cambios. Su posición mejoró y ahora es la empresa que mejor puntúa después de Movistar.
- Su desempeño en neutralidad de la Red fue bueno, y en materia de acceso directo fue una de las tres compañías que dio cuenta de esta realidad.
- Puede mejorar:
 - Informando sobre entrega de datos al sector público y tiempos de retención de datos.
 - Informando sobre procedimientos ante fuga de datos.
 - Integrando mecanismos de protección a la persona usuaria cuando el Estado solicita sus datos.

Principales hallazgos

Claro

claro	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		2	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		3	3
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Su puntaje no varió en comparación con el desempeño en nuestra evaluación anterior. Las principales novedades en torno a los nuevos criterios tienen que ver con haber recibido un buen puntaje en Neutralidad de la Red y el criterio de acceso directo.
- Puede mejorar:
 - Publicando datos comparativos sobre entrega de datos al sector público, bloques de URL, interceptaciones de las telecomunicaciones.
 - Contando con mayor desagregación de datos que recoge en su política de tratamiento.
 - Informando sobre procedimientos ante fuga de datos.
 - Integrando mecanismos de protección a la persona usuaria cuando el Estado solicita sus datos.

Principales hallazgos



eTb	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		1	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		1	1
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Este año su puntaje no cambió en comparación con los años anteriores. Recibió puntaje en el criterio de neutralidad de la Red pero no así en el de acceso directo.
- Puede mejorar:
 - Proveyendo una mayor desagregación en la información que está relacionada en su informe de transparencia de datos (interceptaciones).
 - Contando la manera como informa sobre proceso de entrega de datos al sector público.
 - Facilitando la accesibilidad de sus contenidos.
 - Contando cómo actúa en eventos de fuga de datos y la notificación a sus usuarios.
 - Integrando mecanismos de protección a la persona usuaria cuando el Estado solicita sus datos.

Principales hallazgos



Avantel INFORME	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		0	1
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad	2	2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión	3	3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital	4	4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Puntaje no varió significativamente en comparación con la edición del año anterior que fue la primera en que integró nuestro informe.
- Es la única que advierte que en su relacionamiento con aliados comerciales exigirá una política de tratamiento de datos acorde a sus propios estándares, que supervisará cómo esos aliados cumplen con sus políticas de tratamiento. Sin duda, una buena práctica que merece la pena ser imitada.
- Puede mejorar:
 - Publicando un informe de transparencia.
 - Contando con políticas de género y prácticas de accesibilidad.
 - Informando sobre la entrega de datos al sector público (procedimiento como estadísticas).
 - Informando sobre el acceso directo.

Principales hallazgos

DIRECTV

DIRECTV	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		0	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	1
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informe de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Es la única empresa que de manera expresa dice que notifica a las personas suscritas en sus servicios ante la gestión de solicitudes de entrega de datos de sus datos al sector público.
- Puede mejorar:
 - Informando sobre procedimiento de entrega de datos al sector público, bloqueos URL, interceptaciones.
 - Desagregando mejor datos que recoge de sus personas usuarias.
 - Contando cómo actúa ante eventos de fuga de datos.
 - Integrando mecanismos de protección a la persona usuaria cuando el Estado solicita sus datos.
- Nos parecen interesantes los cambios recientes que se ven reflejados en su sitio web, producto de la adquisición reciente por el grupo Wertheim, lo que influirá positivamente en futuras evaluaciones.

Principales hallazgos



EMCALI VALORAMOS LO ESENCIAL	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		2	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		0	0
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		0	1
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Sin mayor variación en su bajo desempeño en comparación con ediciones anteriores.
- Su página web permite la opción de configurarse el contraste y así facilitar el acceso a personas con discapacidad visual o baja visión.
- Puede mejorar:
 - Publicando informe de transparencia.
 - Publicando política de tratamiento de datos.
 - Informando procedimiento ante fuga de datos.
 - Publicando política de género.
 - Informando sobre acceso directo.

Principales hallazgos

HughesNet®

HughesNet.	Suma por criterio	Promedio por cje	
		2020*	2021
1. Compromisos políticos			0
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad			1
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión			2
3.1. Informa sobre la obligación legal de bloqueo			
3.2. Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital			2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Es su primera evaluación. Puede mejorar, en general, en todos los criterios de evaluación.
- Tuvo buen desempeño en neutralidad de la Red.
- Es importante que pueda informar a sus suscriptores sobre la manera en que se compromete con el respeto de sus derechos en el marco de sus operaciones (presentes en al menos 1000 municipios).

*La compañía se incluyó en este informe desde el año 2021, por tanto, no se reportan datos para el 2020.

Principales hallazgos



SkyNet Colombia	Suma por criterio	Promedio por eje	
		2020*	2021
1. Compromisos políticos			0
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad			0
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión			0
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital			3
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

- Es su primera evaluación y puede, en general, mejorar en todos los criterios.
- Es importante que pueda publicar sus políticas en su página web en aras de informar de manera suficiente a sus suscriptores (presentes en al menos 1100 municipios de Colombia).

*La compañía se incluyó en este informe desde el año 2021, por tanto, no se reportan datos para el 2020.

Vistazo a la calificación general

	claro	El Nueve	Movistar	tigo	etb	3	A	HughesNet	SkyNet
1. Compromisos políticos	2	2	4	3	2	2	1	0	0
2. Intimidación	2	0	3	3	1	2	2	1	0
3. Libertad de expresión	3	1	4	3	3	1	3	2	0
4. Seguridad digital	3	2	4	4	2	2	4	2	3

-  Cumple todos los parámetros
-  Bonificación por lenguaje incluyente en política de género
-  Cumple satisfactoriamente
-  Cumple parcialmente
-  Cumple de forma insuficiente
-  No cumple

3. Conclusiones



- La transparencia es un instrumento clave en la realización de otros derechos y es una importante forma de implementar el deber que las empresas tienen de respetarlos. La transparencia además facilita que las personas puedan exigir rendición de cuentas al Estado.
- Después de siete años de hacer el ejercicio encontramos que las empresas tienen más análisis de impacto en derechos de los que nos imaginamos, que hay conciencia sobre la conexión entre el desarrollo económico y social y el respeto por los derechos de las personas.
- Un ejemplo de esto fue cómo la pandemia nos obligó a imaginar escenarios extremos y la necesidad de articularlos en términos de derechos. Lograr esto requiere de diálogos “multi-stakeholder”, desde Karisma estamos muy dispuestas a ese proceso.

- Los incentivos para el desarrollo de compromisos en derechos son diversos. Inicialmente el liderazgo de ETB (empresa nacional pública) fue evidente, en los últimos años han sido más las empresas con matrices internacionales las que han liderado.
- El sector TIC es innovador y de rápidos cambios, se desarrolla en un entorno complejo de muchas tensiones, incentivos y tentaciones. A nivel internacional la discusión sobre su rol como intermediarios y la forma como pueden o deben abordar los desafíos de DDHH es un campo en evolución. Vale la pena que las empresas locales se pongan en sintonía con sus matrices.
- Sobre recomendaciones concretas favor ver el informe.

Queremos agradecer a las empresas por su participación en la retroalimentación de nuestro informe, abriendo espacios para discutir los resultados previos de su desempeño anual.

Gracias Lucía Camacho!

carobotero@karisma.org.co