



¿QUIÉN DEFIENDE TUS DATOS?



BUSCANDO LA TRANSPARENCIA DE LOS
INTERMEDIARIOS DE INTERNET EN PARAGUAY

Maricarmen Sequera

ABRIL 2017



Quien Defiende Tus Datos es un proyecto desarrollado por TEDIC y forma parte de una iniciativa regional en cinco países de América Latina coordinada por Electronic Frontier Foundation, una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

Consulta esta investigación en:

<https://qdttd.tedic.org>

Colaboradores: Katitza Rodriguez y Kurt Opsahl de EFF

Edición y diagramación: Luis Alonzo Fulchi

Comunicación: Jazmín Acuña

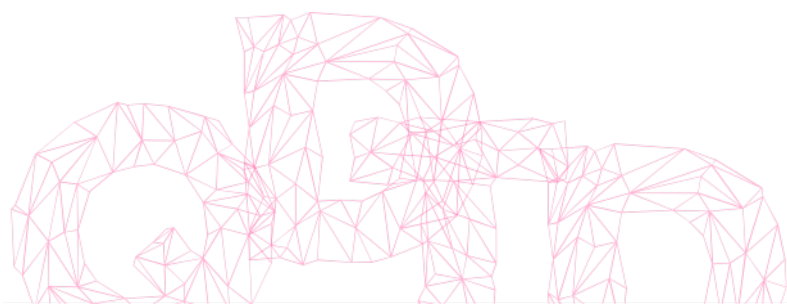
Diseño: Guada Lobo

Tabla de contenidos

Introducción.....	1
Contexto paraguayo.....	3
Tigo.....	6
Personal.....	7
Copaco.....	8
Claro.....	9
Vox.....	9
Chaco Comunicaciones.....	10
Criterios de Evaluación.....	11
1. Políticas de privacidad y protección de datos personales.....	11
2. Autorización judicial.....	13
3. Notificación al usuario.....	15
4. Posicionamiento público en contra de la vigilancia masiva o sin control.....	18
5. Transparencia.....	20
6. Bloqueo de contenidos en Internet.....	21
Metodología.....	23
Categoría 1: Política de privacidad y protección de datos personales.....	23
Categoría 2: Autorización judicial.....	25
Categoría 3: Notificación al usuario.....	26



Categoría 4: Posicionamiento público en contra de la vigilancia masiva o sin control.....	27
Categoría 5: Transparencia.....	29
Categoría 6: Bloqueo de contenidos en Internet.....	30
Reportes de evaluación.....	31
Reporte 0: Cuadro general comparativo 2017.....	31
Reporte 1: Política de privacidad y protección de datos.....	32
Reporte 2: Autorización judicial.....	34
Reporte 3: Notificación.....	36
Reporte 4: Posicionamiento público en contra de la vigilancia masiva o sin control.....	37
Reporte 5: Transparencia.....	39
Reporte 6: Bloqueo de contenidos en Internet.....	41
Evaluaciones por proveedora de Internet.....	43
Tigo.....	43
Personal.....	50
Claro.....	57
Vox.....	63
Copaco.....	70
Chaco Comunicaciones (ChacoNet).....	76





INTRODUCCIÓN

Cada vez más paraguayos y paraguayas se conectan a Internet a través de los teléfonos celulares y computadoras para comunicarnos y acceder a una mayor cantidad de información. Esta información pasa por cables subterráneos que se conectan por el océano al *Backbone*¹ internacional hasta los servidores de Internet a lo largo y ancho del mundo. La conexión entre los usuarios y esta infraestructura de Internet, la realizan las empresas proveedoras de Internet (ISP por su nombre en inglés). En Paraguay las ISP más conocidas son: Tigo, Claro, Personal, Copaco, etc..

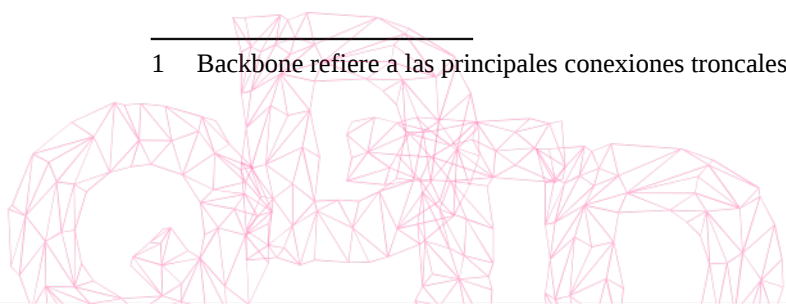
Para conectar a esta *infraestructura* se producen una innumerable cantidad de datos sobre las comunicaciones, que son los famosos *metadatos* y pueden exponer la vida privada de las personas. La forma en la cual las proveedoras de Internet prestan dicho servicio de conexión y manejan los metadatos asociados se vuelve esencial para la protección de la vida privada de la población.

En este contexto, resulta de una gran relevancia que los usuarios de servicios de Internet –y telecomunicaciones en general– conozcan en detalle cómo las proveedoras de Internet tratan su información personal y cuál es el mejor modelo de *economía digital* que mejor cumple los estándares de protección de los derechos humanos. Este es un factor clave para la competencia empresarial y la confianza de los usuarios.

Las empresas son las únicas que se encuentran entre la autoridad y los datos de las personas. ¿Quién es transparente sobre sus políticas? ¿Quién exige una autorización judicial antes de entregar tus datos? ¿Quién defiende a sus clientes? ¿Quién Defiende Tus Datos?

“¿Quién Defiende Tus Datos?” es un proyecto de TEDIC (Tecnología y Comunidad), la organización de derechos digitales más importante en Paraguay y EFF (Electronic Frontier Foundation), que evalúa las políticas y prácticas de privacidad de las 6 empresas proveedoras de acceso a servicios de telecomunicaciones más importantes de Paraguay. Estas comprenden la gran mayoría del mercado de telefonía fija, móvil y banda ancha. Las empresas evaluadas son: Tigo, Personal, Vox, Copaco, Claro y Chaco Comunicaciones.

1 Backbone refiere a las principales conexiones troncales de Internet

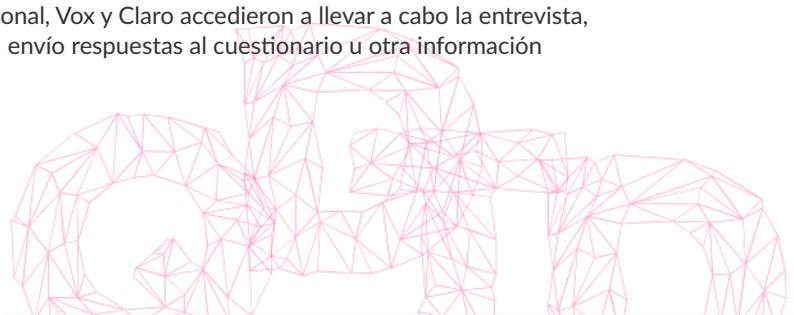




El reporte de TEDIC es parte de un proyecto regional que involucra a [R3D](#) de México, [Fundación Karisma](#) de Colombia, [Hiperderecho](#) de Perú, [InternetLab](#) de Brasil y es coordinado por [EFF](#) de los Estados Unidos.

Para llevar a cabo las evaluaciones, se examinó información públicamente disponible como los avisos de privacidad, códigos de prácticas comerciales y otra información disponible en los sitios de Internet de las empresas evaluadas. Adicionalmente, a cada compañía le fue enviado un cuestionario, la metodología de la investigación y un informe provisional de evaluación, así como una la invitación para realizar una entrevista para acceder a información adicional y de primera mano. Toda información enviada por parte de las proveedoras de Internet han sido consideradas para la evaluación final².

2 Al momento de publicar el reporte, únicamente Tigo Personal, Vox y Claro accedieron a llevar a cabo la entrevista, salvo Copaco y Chaco Comunicaciones, ninguna empresa envió respuestas al cuestionario u otra información adicional.





CONTEXTO PARAGUAYO

Internet llega a la mayoría de los hogares paraguayos por medio de línea de Abono Digital Asimétrica (ADSL, por sus siglas en inglés) y en mucho menor medida las tecnologías de microondas o fibra óptica.

En términos de uso de Internet, el porcentaje de penetración se aproxima 36%³. Por porcentaje de penetración, entendemos a la *cantidad de personas que pueden acceder dentro de un país*. Cabe recordar que Paraguay puede denominarse un país pequeño en tanto su población ronda los 7 millones de personas⁴ y su territorio unos 400.000 km².

El acceso a Internet en Paraguay es *sumamente desigual* entre los hogares más ricos y los más pobres: según un informe de CEPAL⁵ la diferencia es de 20 veces superior del quintil más rico con relación al quintil más pobre. La *brecha de conexión* entre zona urbana y rural es de 20 puntos porcentuales. De todos modos, se aprecia un descenso de la desigualdad en el acceso, medido por el coeficiente de Gini⁶ que disminuyó en el Paraguay y se encuentra en el 0,44 % en el año 2013.

En lo que refiere a la *velocidad de acceso*, ocupa penúltimo lugar en América Latina con la Internet más lenta⁷. Las velocidades de carga y descarga en banda ancha móvil son menores a 2,65 mbits/s por lo que también es la más lenta en versión móvil⁸.

3 Indicadores del Desarrollo Mundial (IDM) arrojan 36%, mientras que CONATEL calcula un 30% sobre la base de datos de la Unión Internacional de Telecomunicaciones (UIT) World Telecommunications Indicators Database. Ver <http://wdi.worldbank.org/table/5.1> y <http://www.conatel.gov.py/files/MANUAL%20PLAN%20NACIONAL.pdf>

4 Población paraguaya <http://countrymeters.info/es/Paraguay>

5 CEPAL informe 2015 http://repositorio.cepal.org/bitstream/handle/11362/38605/S1500568_es.pdf

6 El coeficiente de Gini es un número entre 0 y 1, en donde 0 corresponde a la perfecta igualdad y el valor 1 a la perfecta desigualdad.

7 Paraguay tiene el segundo internet más lento de Latinoamérica <http://www.lanacion.com.py/2016/02/17/paraguay-tiene-el-segundo-internet-mas-lento-de-latinoamerica>

8 Según el Observatorio Regional de Banda Ancha (ORBA), 2014: <http://www.cepal.org/es/observatorio-regional-de-banda-ancha>



Según datos de la Comisión Nacional de Telecomunicaciones (CONATEL)⁹ –ente regulador de las telecomunicaciones en Paraguay–, a junio de 2016 Paraguay cuenta con 7.445.061¹⁰ suscriptores de Internet móvil (5.855.382 prepago y 1.589.679 con planes) y 185.125 suscriptores de Internet fijo, con un total de 437.243 suscripciones.

Dentro de los planes de banda ancha, los que cuentan con mayor suscriptores son los que van de 1 a 2 megas, contabilizando un total de 174.231 suscripciones. Según fuentes oficiales se tienen 382.446 de cuentas activas de Internet¹¹ que equivalen al 5,4%¹² con relación a la población total del país. Vale aclarar que los abonos al servicio de Internet varían de acuerdo a los meses del año y que diferentes planes de servicio pueden corresponder a un mismo usuario.

Por su parte, si observamos el acceso a banda ancha con relación al PIB per cápita¹³, vemos que en el año 2010 era necesario destinar el 22% del ingreso para acceder a un servicio de Internet, mientras que en el 2014 disminuyó a un 15% aproximadamente¹⁴. Por otra parte la la tarifa mínima de bolsas de datos prepago de banda ancha móvil es de 0,2 U\$D¹⁵.

	julio/2014	agosto/2014	septiembre/2014	octubre/2014	noviembre/2014	diciembre/2014	
Menores a 512 Kbps	0	0	0	0	0	0	0 suscripciones
Entre 0,512 y 2 Mbps	56.703	55.073	54.330	53.628	52.767	52.234	52.234 suscripciones
Entre 2 y 10 Mbps	225.372	220.738	217.215	211.568	205.946	199.884	199.884 suscripciones
Más de 10 Mbps	0	0	0	0	0	0	0 suscripciones
Total suscripciones	282.075	275.811	271.545	265.196	258.713	252.118	252.118 suscripciones
Ingresos mensuales	15.915.359.723	14.909.100.195	15.258.886.950	14.734.890.951	13.939.366.928	13.791.429.730	13.791.429.730 Guaraníes
Acceso por medio de teléfonos inteligentes y tablets	1.439.507	1.560.325	1.560.766	1.715.165	1.741.400	1.890.745	1.890.745 suscripciones
3G/4G GPRS	379.605	445.119	686.440	743.827	509.483	477.742	477.742 suscripciones

Obs: se considera banda ancha a velocidades no inferiores a 512 kbps

Internet Móvil de Julio a Diciembre de 2014 - Informe CONATEL

9 Suscriptores de Internet móvil y fijo (2010-2014) Fuente CONATEL <http://www.conatel.gov.py/images/2015-2/PNT/DESARROLLO/midt%202014.pdf>

10 Telefonía móvil e Internet móvil por medio de teléfonos inteligentes, tabletas y otros dispositivos. Planilla 20 de setiembre. Informe de Solicitud de acceso a la Información pública. 2016.

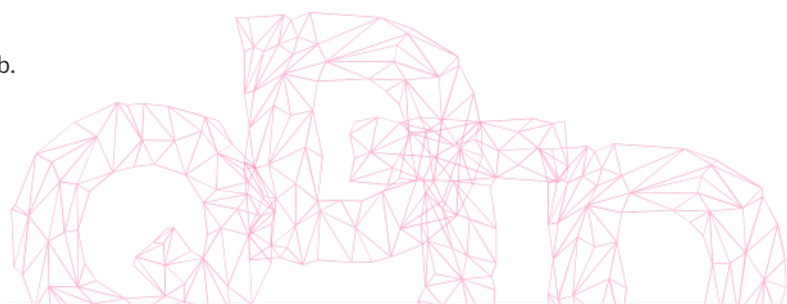
11 Infografía del periódico nacional Última Hora sobre las suscripciones en las Proveedoras de Servicio de Internet (ISP). <http://www.ultimahora.com/imagenes-01610005250496100000000/jpg> 8 de febrero de 2016.

12 Abonados a Internet por banda ancha fija (por cada 100 personas) Banco Mundial. 2013 <http://datos.bancomundial.org/indicador/IT.NET.BBND.P2/countries/PY?display=graph> Ver informe del Observatorio Regional de Banda Ancha (ORBA) de la CEPAL, con datos de UIT, World Telecommunications Indicators Database, 2014. Paraguay contaba con 4,9% en móviles y 1,7% en fijos de suscripciones en comparación con la población total.

13 Este indicador es una aproximación a la proporción del ingreso que debe destinarse para acceder al servicio de banda ancha; a menor proporción, mayor asequibilidad.

14 Informe de CEPAL

15 Con capacidad de transferencia de datos menor a 100 Mb.



(Internet fijo)	julio/2014	agosto/2014	septiembre/2014	octubre/2014	noviembre/2014	diciembre/2014	
Menores a 512 Kbps	7.537	7.537	7.552	7.320	7.230	7.183	suscripciones
Entre 0,512 y 2 Mbps	115.867	115.488	116.138	115.229	114.462	114.245	suscripciones
Entre 2 y 10 Mbps	51.663	54.263	55.607	59.012	62.666	62.748	suscripciones
Más de 10 Mbps	744	784	826	859	909	949	suscripciones
Total suscripciones	175.811	178.072	180.123	182.420	185.267	185.125	suscripciones
Ingreso mensuales	29.234.775.591	29.611.414.069	30.088.296.620	30.757.601.904	31.204.690.964	32.052.312.467	Guaraníes

Obs: se considera banda ancha a velocidades no inferiores a 512 kbps

Internet Fija de Julio a Diciembre de 2014 - Informe CONATEL

Por otro lado Internet móvil tiene una amplia cobertura para redes de 2G/3G/4G siendo la 3G la más utilizada. La red 4G es aún muy limitada, siendo las empresas Copaco-Vox y Personal las que cuentan con servicio de 4G accesible para usuarios. Por su parte, las empresas Tigo y Claro fueron adjudicadas recientemente para la prestación de banda ancha de Internet 4G¹⁶.

En cuanto a las *líneas telefónicas móviles*, el país cuenta con 7.412.303 líneas activas, lo que se evidencia que existen más dispositivos móviles que habitantes¹⁷.

Con relación a la *Regulación de portabilidad numérica*¹⁸ que significa la posibilidad de cambiar de empresa proveedora sin perder el número telefónico y que está vigente hace 3 años, Claro fue la firma que más clientes obtuvo (34.012), seguida por Personal (7.185). En cambio, Tigo perdió 23.590 usuarios y Vox 17.607¹⁹. De acuerdo con las explicaciones de técnicos del sector de telecomunicaciones, solo el 1% de todos los usuarios de un país realiza la portabilidad numérica²⁰.

Con relación a hechos punibles, todas las proveedoras de Internet colaboran con el Ministerio Público entregando información pertinente para persecución de delitos y crímenes. Las solicitudes se deben realizar a través de una orden judicial que argumente y tenga la información mínima del caso investigado. Sin embargo en los hallazgos de la presente investigación, se constató que el Ministerio Público accede a los metadatos de

16 Adjudicación de 4G a Tigoy Claro <http://www.conatel.gov.py/index.php/articulo-destacado/9-banners-home/4-banner-1>

17 Ídem Nota de Pie 7

18 Ver marco regulatorio en la portada de CONATEL <http://conatel.gov.py>

19 Tigo Paraguay lidera el mercado móvil <http://www.mediatelecom.com.mx/index.php/agencia-informativa/noticias/item/75329-tigo-paraguay-lidera-54-7-del-mercado-m%C3%B3vil>

20 Ídem anterior

llamadas a través simples solicitudes dirigidas a las ISPs. También se constató que no se publican las estadísticas sobre las solicitudes realizadas a las proveedoras por parte del Estado..

Cabe resaltar que hay una fuerte concentración del sector en lo que refiere a servicios de Internet y de telefonía móvil en Paraguay.

Para el estudio del proyecto han seleccionado a los principales Proveedores de Servicios de Internet de Paraguay²¹ con base en la información encontrada en el Plan Nacional de Telecomunicaciones 2011-2015:

TIGO²²

Tigo pertenece a la empresa Millicom International Cellular S.A., administrado por TELECEL S.A.. Este es un grupo global de telecomunicaciones y medios con sede en Luxemburgo que ofrece servicios móviles, de voz, datos, televisión por cable, banda ancha y finanzas. Es el actual líder del mercado en telecomunicaciones con el 52% de participación en el país, con 3.861.126 usuarios de telefonía móvil.

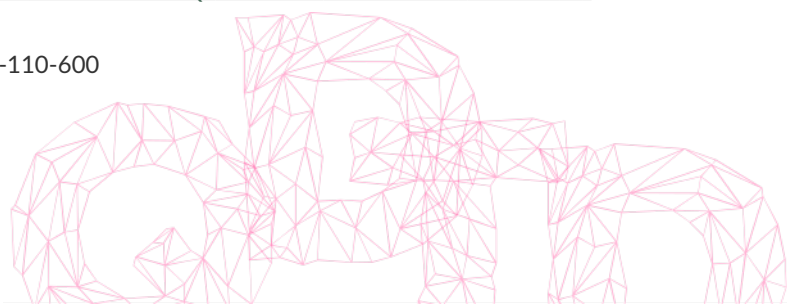
Los planes son flexibles para contratar Internet y telefonía móvil, y tienen dos modalidades: prepago sin contrato o contratos libres con posibilidad de rescisión a fin de mes sin cargos – excluyendo los planes que implican la compra de teléfonos móviles. Es decir no tienen vigencias mínimas para ninguno de sus servicios que incluyen Internet. Dependiendo de la zona pueden variar los planes: desde 2 Mbps por 28 U\$D a 30 Mbps por 108 U\$D²³ Con respecto a la fibra óptica, en la web no aparecen detalles de suscripción, pero su costo es poco accesible: su instalación cuesta 330 U\$D y el plan más bajo de 1 Mbps cuesta 42 U\$D al mes. Para contar con una IP Pública fija, hay que abonar un cargo extra de 3,9 U\$D mensuales²⁴.

21 Lista de Proveedoras de Internet en Paraguay
https://en.wikipedia.org/wiki/List_of_internet_service_providers_in_Paraguay

22 Web oficial de Tigo <http://tigo.com.py>

23 Planes de Internet: <https://ayuda.tigo.com.py/hc/es/articles/215723528--Qu%C3%A9-velocidad-de-internet-es-ideal-para-mi->

24 Consultas de la investigadora a atención al cliente: 0800-110-600





La empresa también ofrece suscripción a TV con modalidades cable y UHF: actualmente posee 236.262 abonados.

Finalmente también provee transferencias de dinero a través de su plataforma *Tigo Money* que procesó operaciones por 240.000 millones de guaraníes en el año 2015²⁵. Su informe global anual agrega que la empresa de telecomunicaciones tiene actualmente 1.623 sitios móviles en todo el territorio paraguayo²⁶.

PERSONAL²⁷

Empresa de origen argentino, administrada por NÚCLEO S.A., que ocupa el segundo lugar de participación en el mercado. Tiene el 32% de suscripciones, que son unos 2.410.531 usuarios de telefonía móvil y 119.889 usuarios de Internet con frecuencia 1900 MHz.

Sus servicios de planes de Internet para móvil y hogares son flexibles para la rescisión del contrato, lo que significa la posibilidad de cancelación del servicio en cualquier momento sin cargos –sin tomar en cuenta los contratos de compra de teléfonos móviles. Los planes varían entre la modalidad: prepago y pospago. La velocidad del servicio de banda ancha pospago para hogares es de 256 Mbps y los planes que se ofrecen están entre 1,5 Mbps con un costo de 12,6 U\$D a 10 Mbps por 34 U\$D²⁸. Los planes prepago varían entre 200 Mbps con el costo de 0,27 U\$D a 8 GB por 27 U\$D²⁹. No se cuenta con datos para conocer los detalles del número de suscripciones en planes prepago y pospago, banda ancha ni fibra óptica. Sin embargo se cuenta con un “mapa de la cobertura” 3G y 2G (sin microdatos)³⁰.

Su servicio de televisión prepaga con modalidad TV satelital cuenta con 22.296 suscripciones donde ocupa el tercer lugar en el mercado nacional.

25 Según datos preliminares de la Superintendencia de Bancos (SIB) 12 de febrero 2015.

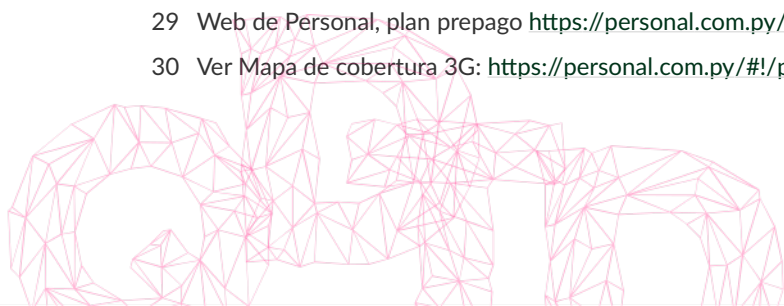
26 Informe anual Millicom 2014. 4,3 millones de dólares
<http://www.millicom.com/media/2940878/CRreport2014HighlightsSpanish.pdf>

27 Web oficial de Personal: <https://personal.com.py>

28 Web de Personal, plan pospago https://personal.com.py/#!/public/internet/plan_pospago

29 Web de Personal, plan prepago https://personal.com.py/#!/public/internet/plan_prepago/

30 Ver Mapa de cobertura 3G: <https://personal.com.py/#!/public/institucional/cobertura/>





También cuenta con un sistema transferencia de dinero llamado “*Billetera Personal*” que ha procesado operaciones de alrededor de 36.000 millones de guaraníes³¹.

COPACO³²

Empresa estatal con acciones de capital público-privado desde el año 2001³³ que brinda servicio de Internet a hogares por cable, ocupando el tercer lugar en este sector con el 17% del mercado, cuenta con 67.116 usuarios suscritos³⁴. Esta empresa está dirigida por sus Accionistas, Síndicos y Presidente, este último nombrado por Decreto del Presidente de la República. El funcionamiento administrativo se rige por las leyes de administración Financiera del Estado y sus reglamentos, y cuenta con presupuesto anual del Estado.

La empresa ofrece un servicio ADSL con anchos de banda que oscilan entre 768 Kbps y 1 Mbps por 16,4 U\$D a 8 Mbps por 82,1 U\$D. La cancelación del servicio se puede realizar en cualquier momento sin cargos según su modelo de contrato³⁵. La tecnología LTE 4G con la modalidad fija inalámbrica cuenta con contratos de 12 a 24 meses y con planes que pueden variar entre 18 Gb y 2,3 Tb de tope de descargas, con velocidades de hasta 40 Mbps. Para obtener IP pública es necesario abonar adicionalmente 5 U\$D.

Los costos para acceder al servicio de fibra óptica dependen de una Disposición Tarifaria vigente para la instalación como acceso de última milla. Las tarifas mensuales dependen de su ancho de banda que oscilan de 1 Mbps por 34,7 U\$D a 10 Mbps por 283,6 U\$D³⁶. El contrato de este servicio es indeterminado, cualquiera de las partes pueden cancelarlo en cualquier momento³⁷. Actualmente la empresa no ofrece los detalles de cantidad de suscripciones a los diferentes planes. Por otro lado ofrece servicio de televisión paga con la modalidad IPTV con un total de 2.901 abonados según el informe oficial de CONATEL.

31 Según datos preliminares de la Superintendencia de Bancos (SIB) 12 de febrero 2015.

32 Web oficial de Copaco <https://www.copaco.com.py>

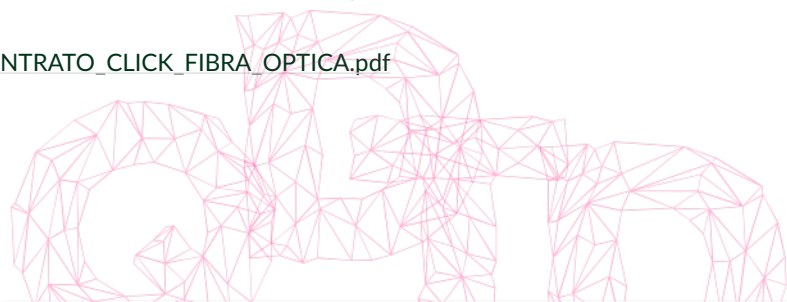
33 Ver detalles de la estructura orgánica <https://www.copaco.com.py/portal/index.php/sobre-copaco.html>

34 Periódico Última Hora <http://www.ultimahora.com/con-3-anos-portabilidad-tigo-mantiene-diferencia-y-vox-se-hunde-n965468.html>

35 Modelo de contrato https://www.copaco.com.py/portal/images/empresa/Contrato_ADSL.pdf

36 <https://www.copaco.com.py/portal/index.php/parawaynet/servicios-internet/click-fibra-optica.html>

37 Ver cláusula de la copia del contrato de Copaco
https://www.copaco.com.py/portal/images/empresa/CONTRATO_CLICK_FIBRA_OPTICA.pdf





CLARO³⁸

Es una marca de servicios de comunicaciones que pertenece a la empresa mexicana América Móvil. Actualmente ocupa el tercer lugar en el mercado de telefonía móvil con 780.555 usuarios que corresponde al 11% del mercado nacional y ocupa el cuarto lugar en proveedor de Internet con 48.000 abonados.

Los contratos de los servicios cuentan con flexibilidad a la hora de cancelarlo —sin tomar en cuenta la compra un teléfono celular. Los planes de banda ancha móvil varían entre 2 Gb por 10,6 U\$D a un plan full de 10 Gb por 25 U\$D³⁹ con velocidad de 5Mbps. No ofrecen servicio de IP Pública ni fibra óptica. No se encuentra información acerca de los detalles de la cantidad de usuarios con contratos de servicio prepago y pospago de banda ancha móvil ni de domicilio.

VOX⁴⁰

Empresa estatal de capital público-privado que depende de la telefónica estatal Compañía Paraguaya de Comunicaciones (Copaco). Esta última desembolsó 3 millones de dólares por la compra del 100% de las acciones de la empresa privada de telefonía móvil Vox⁴¹ en el año 2010.

Ofrece los servicios de telefonía móvil, operando con la tecnología GSM, en la frecuencia “1700/2100 AWS”. Ocupa el último lugar en el mercado nacional con el 5% que equivale a 359.957 abonados en el servicio de telefonía móvil y el quinto lugar como proveedora de Internet con 10.814 suscripciones. Cuenta con un mapa interactivo de cobertura nacional que describe cuáles ciudades cuentan con el servicio LTE y HSPA+⁴². Los planes que ofrece este servicio varían entre 27,9 U\$D por 18 Gb de tope de descarga a 1171 U\$D por 2,3 Tb con un contrato mínimo de 18 meses. Otro plan de servicio de Internet con 1 Gb de tope de descargas por el monto de 17 USD sujeto a 12 meses contrato⁴³. Finalmente planes mucho

38 www.claro.com.py

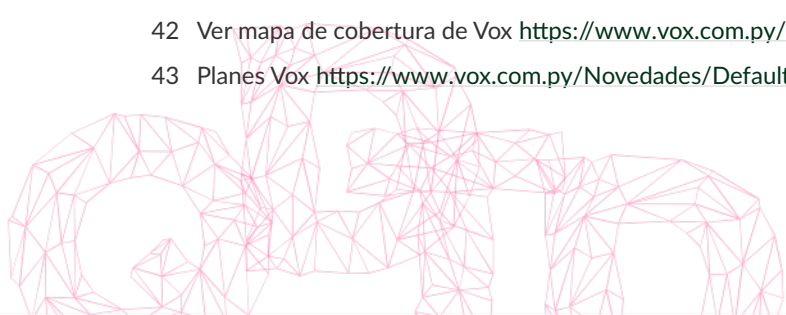
39 Ver promociones banda ancha móvil <http://www.claro.com.py/portal/py/sc/personas/internet/pospago/#info-041>

40 Web oficial de Vox <https://www.vox.com.py>

41 Compra de las acciones por Copaco <http://alparaguay.blogspot.com/2010/07/telefonica-estatal-de-paraguay-copaco.html>

42 Ver mapa de cobertura de Vox <https://www.vox.com.py/Internet/Cobertura>

43 Planes Vox <https://www.vox.com.py/Novedades/Default.aspx?Novedad=115>





más económicos y flexibles de recargas móviles que van desde 0,36 USD con 200 Mb de tope a 9 U\$D con 2750 Mb⁴⁴ de tope.

CHACO COMUNICACIONES⁴⁵

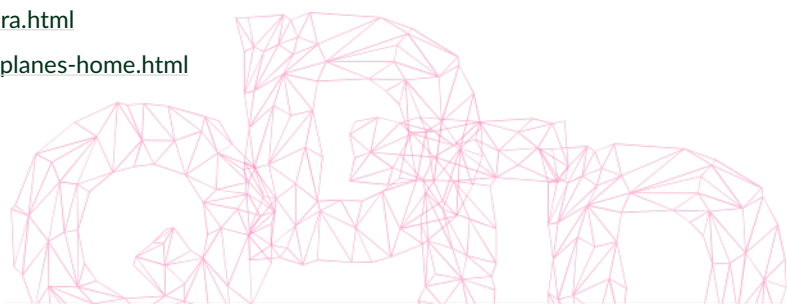
Proveedor de Internet inalámbrica y de banda ancha en el Chaco Central. Su sede administrativa es en Loma Plata y cubre ciudades importantes del Chaco Central⁴⁶. El costo del servicio de IP pública es de 5,5 U\$D mensuales. Ofrece servicios limitados sin capacidad de descargar archivos P2P⁴⁷ y servicios “Full” que oscilan entre 400 Kbps por 25 U\$D a 3 Mbps por 150 U\$D mensuales. La cantidad de abonados al servicio de Internet es de 1.121. Los contratos tienen tiempo mínimo para la obtención de su servicio de Internet que varían entre 12 a 18 meses.

44 Planes prepago <https://www.vox.com.py/Novedades/Default.aspx?Novedad=121>

45 Web oficial de ChacoNet <http://www.chaconet.com.py/>

46 Mapa de cobertura de ChacoNet:
<http://www.chaconet.com.py/productos-y-servicios/cobertura.html>

47 Ver <http://www.chaconet.com.py/productos-y-servicios/planes-home.html>





CRITERIOS DE EVALUACIÓN

Se utilizaron 6 criterios para evaluar las *prácticas y políticas de privacidad* de cada compañía, basados en los siguientes puntos de vista:

- Compromiso público de proteger la privacidad;
- Adopción de prácticas y políticas en favor de los usuarios;
- Transparencia de las prácticas y políticas.

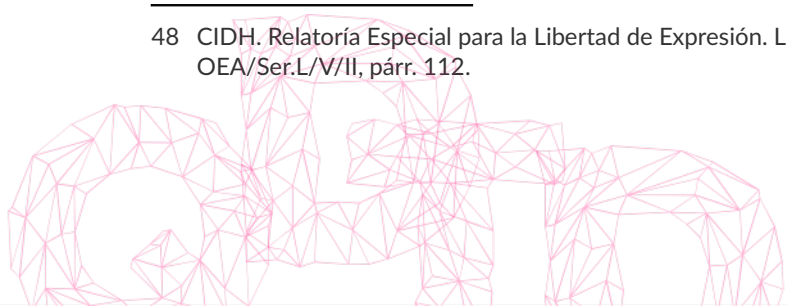
A continuación se desarrollan cada uno de los criterios:

1. POLÍTICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

La compañía cuenta con una política de privacidad y de protección de datos personales, utilizando un lenguaje claro y libre de tecnicismos. Informa a las personas sobre la recolección, uso, almacenamiento, procesamiento de sus datos personales. En particular, este instrumento debe ser visto como una oportunidad para informar de manera clara a los usuarios respecto de sus derechos y no debería ser visto como un mero formalismo legal. La compañía también cuenta con políticas de privacidad frente a las autoridades gubernamentales. La misma describe cual es el procedimiento legal para entregar a la justicia los datos de sus usuarios en el caso que haya una investigación criminal bajo solicitud del juez competente.

Al respecto, tanto la *Constitución de la República* en su artículo 33 —Sobre la Intimidad de las personas— como los *Tratados Internacionales* protegen el derecho a la intimidad como uno de los pilares de las democracias modernas. Asimismo organismos internacionales de protección de *Derechos Humanos* han señalado que las empresas deben establecer e implementar condiciones de servicio que sean transparentes, claras, accesibles, así como apegarse a las normas y principios internacionales de Derechos Humanos; incluyendo las condiciones en las que pueden generarse interferencias con el derecho a la privacidad de los usuarios⁴⁸. Es indispensable que la compañía cuente con políticas que cumplan estos protocolos a la hora de entregar información personal y datos personales a las autoridades.

48 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 112.



Por otra parte, los metadatos forman parte de la comunicación y tienen el carácter de inviolabilidad tal como se desprende del artículo 36 de la Constitución Nacional:

“No podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley...”.

Las empresas deben almacenar los metadatos de sus usuarios por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico 4868/2013. En este escenario, es imprescindible que las ISPs describan y den a conocer qué información personal está siendo retenida, así como las medidas para salvaguardar dichos datos ante posibles ataques o riesgos que puedan afectar dicha información.

El art. 10 de la ley 4858/2013 dice:

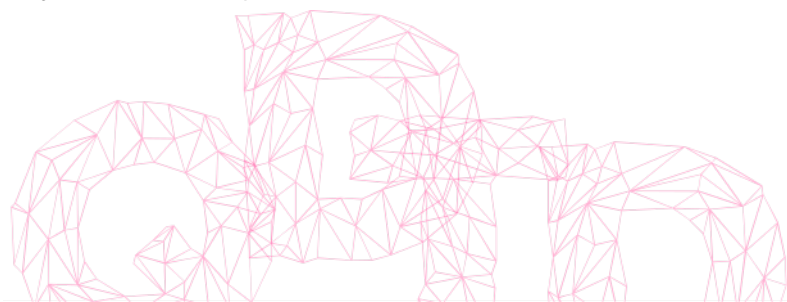
“Los Proveedores de Servicios de Intermediación y los Proveedores de Servicios de Alojamiento de Datos deberán almacenar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio, por un período mínimo de 6 (seis) meses, en los términos establecidos en este artículo. Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.

Los Proveedores de Servicios de Alojamiento de Datos deberán almacenar sólo aquellos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.

No podrán utilizar los datos almacenados para fines distintos a los que estén permitidos por la ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos”.

En un caso contencioso⁴⁹ reciente en el que se condenó al Brasil por el uso ilegal de escuchas telefónicas en un proceso penal, la Corte Interamericana señaló que el derecho a la privacidad protege tanto al *contenido* de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación, como ser los *metadatos* o *datos de tráfico*. Esta jurisprudencia vinculante a la jurisdicción nacional paraguaya, sitúa a estos datos en una instancia de protección constitucional y de derechos humanos.

49 Corte I.D.H. Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas) , párr. 114.





Por otro lado, la ley 4868/2013 de Comercio Electrónico y su decreto reglamentario 1165/14 obliga compulsivamente a informar y proteger los datos de los usuarios:

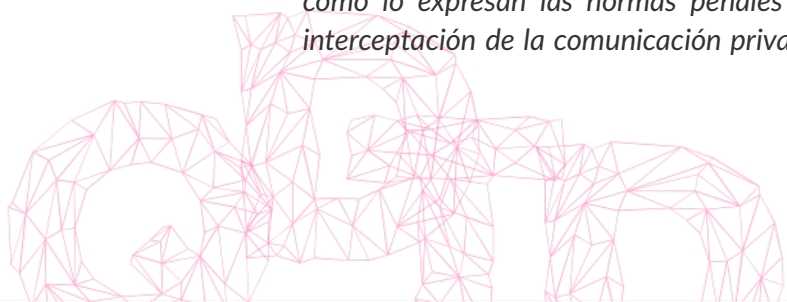
Art 9 de la ley 4868/2013: “Obligación de los Proveedores de Servicios de Intermediación. Los Proveedores de Servicios de Intermediación consistentes en la prestación de servicios de acceso a Internet, estarán obligados, sin perjuicio de las disposiciones vigentes sobre los Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente, a: a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia; Esta obligación de información se tendrá por cumplida si el correspondiente Proveedor incluye la información exigida en su página o sitio principal de Internet. a) suspender el acceso a un contenido o servicio cuando un órgano competente, en ejercicio de las competencias que legalmente tenga atribuidas, requiera que se interrumpa la prestación de un servicio o que se retire algún contenido que vulnere lo dispuesto en el Artículo 6°”.

Art 11 del reglamento 1165/14: “Deber de Informar y Protección de Datos. El proveedor de bienes y servicios por vía electrónica a distancia, debe poner a conocimiento del consumidor o usuario la finalidad y el tratamiento que se le daría sus datos personales, conforme a la Ley vigente relativa a la materia. Así mismo, debe comunicar el destinatario de los datos suministrados y el responsable de custodiar o almacenar la información proporcionada. El proveedor de bienes y servicios empleará sistemas seguros para evitar la pérdida, alteración y acceso de terceros no autorizados a los datos suministrados por el consumidor o usuario.”

La Institución garante y responsable del cumplimiento de la ley de Comercio Electrónico es el Ministerio de Industria y Comercio, que tiene como atribución la coordinación de inspecciones y controles a los distintos proveedores de Internet. Inclusive debe aplicar sanciones por las faltas no previstas específicamente en la ley de *defensa del consumidor* y establecidas en la ley de Comercio Electrónico.

2. AUTORIZACIÓN JUDICIAL

La vigilancia sin consentimiento del afectado conlleva riesgos de abusos por las autoridades, por ello resulta imprescindible la autorización de un juez competente. Para solicitar información personal debe haber una autorización del juez competente tal como lo expresan las normas penales y la Constitución Nacional del Paraguay. La interceptación de la comunicación privada de las personas tiene carácter excepcional

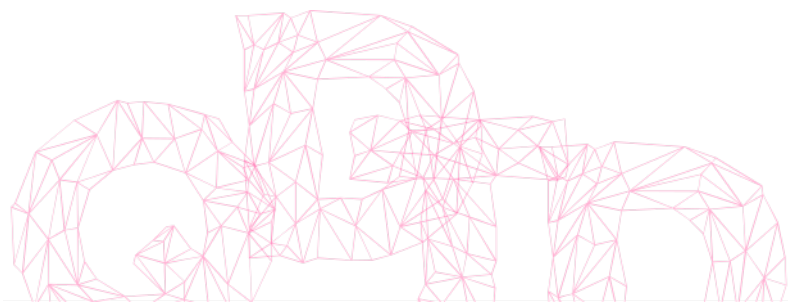


con pena de nulidad en el juicio. Este criterio implica verificar si la compañía cuenta con políticas que cumplan los protocolos para entregar la información a la autoridad judicial. Es decir, detalles del expediente penal, número de causa, datos de la persona, el tipo base penal que incurre el investigado, argumentación legal y firma del juez de la causa.

La Constitucional Nacional en el artículo 36 sobre la inviolabilidad de las comunicaciones obliga a las autoridades del Estado a solicitar información a las compañías sólo a través de una orden judicial debidamente justificada.



El debido proceso para una interceptación de información





3. NOTIFICACIÓN AL USUARIO

La compañía deberá contar con una política de notificación a usuarios afectados por medidas de vigilancia estatal, en el primer momento permitido por la ley. Deberá demostrar que han litigado los impedimentos legales o regulatorios para llevar a cabo la notificación y publicar de forma accesible que ha promovido mecanismos de notificación al usuario al congreso o a otros entes regulatorios.

Cuando a los usuarios se les dice que su información de cuenta o de conexión a Internet fueron exigidas por las autoridades administrativas o judiciales, hay una expansión de las oportunidades de ejercer efectivamente su derecho de defensa contra los abusos e irregularidades. El fuerte impacto de las notificaciones para garantizar una defensa efectiva en el Estado de Derecho no es una idea nueva. A la luz del principio constitucional del debido proceso, muchas leyes establecen la obligación de notificar a las personas sobre las medidas que afectan a sus derechos.

Por su parte el Código Procesal Penal en su artículo 151 y Resolución de la Corte Suprema de Justicia de Paraguay disponen la obligación de notificar a la persona, cuando el Ministerio Público le ha imputado por un supuesto hecho punible.

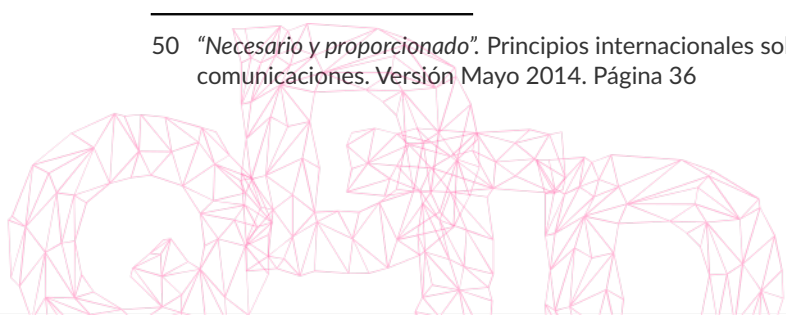
Este derecho de *notificación a las personas afectadas* por medidas de vigilancia ha sido reconocido por especialistas en Derechos Humanos en Internet y fue plasmado en un documento llamado “*Necesario y proporcionados*” y dice lo siguiente:

“Es imposible que una persona impugne efectivamente la interferencia de un gobierno en su vida privada si no sabe si ha sido víctima. En líneas generales, la falta de transparencia respecto a la aplicación de las leyes que rigen la vigilancia encubierta puede impedir el control democrático significativo de esas leyes”⁵⁰.

Por otro lado, la *Relatoría Especial Sobre Derechos Humanos de la Organización de las Naciones Unidas* expresó su opinión al respecto:

“Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accedidas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en

50 “*Necesario y proporcionado*”. Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. Versión Mayo 2014. Página 36



*cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones*⁵¹.

Es decir, la notificación podría no poder llevarse a cabo de inmediato en tanto se podría frustrar el éxito de una investigación, pero debería al menos efectuarse cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento no genere un riesgo inminente de peligro a la vida o integridad de alguna persona. Actualmente existe un vacío legal sobre este punto en el Código Procesal Penal respecto a la protección de los Derechos Humanos en el marco de derecho a la intimidad y un juicio justo. Esto no invalida a la compañía del deber de actuar *de buena fe* para salvaguardar la intimidad de sus usuarios, notificándoles sin poner en peligro el objetivo de la investigación penal.

En casos adversos a la implementación de la política de notificación de la empresa, la compañía deberá combatir judicialmente los impedimentos legales para notificar a usuarios afectados, al menos, luego de que haya transcurrido un tiempo razonable para que no se frustre el objeto de la medida de vigilancia. Otra medida, sería llevar a cabo acciones de incidencia legislativa o regulatoria para la implementación de mecanismos legales de notificación.

En el contexto de las *solicitudes de datos personales*, las proveedoras de Internet adquieren un papel esencial en la protección de las garantías procesales de los usuarios afectados. Es decir, la notificación por la empresa permite al usuario desafiar las solicitudes ilegales: tanto órdenes judiciales sin fundamento, como solicitudes de las autoridades administrativas sin competencia ni justificación. En la situación actual, el usuario depende de los retos realizados por las propias empresas contra las peticiones que consideran abusivo. Si el usuario es notificado, obtiene a la mayor brevedad, la capacidad de defenderse de posibles violaciones de su privacidad.

Con esto en mente, creemos que es importante fomentar la práctica de la notificación al usuario a través del proyecto “¿Quién defiende tus datos?” (WHYB). En los casos en que las solicitudes de datos no van acompañadas de la obligación de confidencialidad, la notificación es permitida por la ley paraguaya (dada la ausencia de prescripción legal en

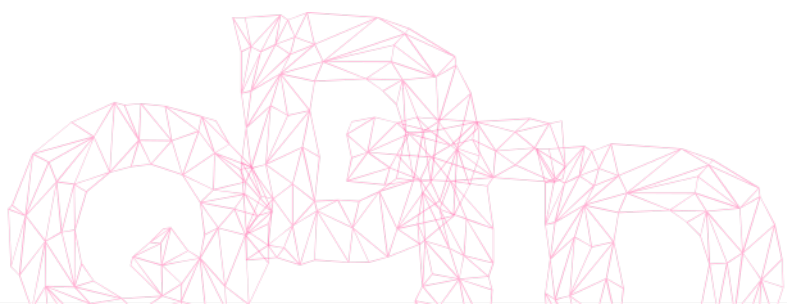
51 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40





contrario). La posibilidad de notificación de usuario puede ser necesaria, no sólo en los casos de solicitudes de datos en procesos civiles, sino también en relación con las solicitudes hechas por otras agencias gubernamentales, tales como el Hacienda o CONATEL. Se fortalece la posibilidad de desafío legal a la presentación de pruebas irrelevantes a los hechos del caso.

En esta edición, hemos decidido esta categoría sería una "prima", porque la notificación no es ni una obligación legal impuesta a las empresas ni una práctica generalizada en el país. Es una medida vista como innovadora y en cierta medida costosa (debido a que requiere personal dedicado a las notificaciones). Por estas razones, su adopción revelaría un compromiso especial con el avance de la protección de los derechos de los usuarios, especialmente digno de ser observado. La *notificación al usuario*, a la primera oportunidad legalmente posible, y preferiblemente antes de la divulgación de los datos, colabora con los principios de defensa legal, y fomenta una cultura de protección de la privacidad.



4. POSICIONAMIENTO PÚBLICO EN CONTRA DE LA VIGILANCIA MASIVA O SIN CONTROL

Es determinante para el respeto y protección de los derechos humanos de los usuarios y generar confianza en torno al ecosistema de Internet, es indispensable el compromiso público y posicionamientos sobre políticas públicas, legislaciones nacionales que afecten la tecnología con perspectiva de Derechos Humanos.

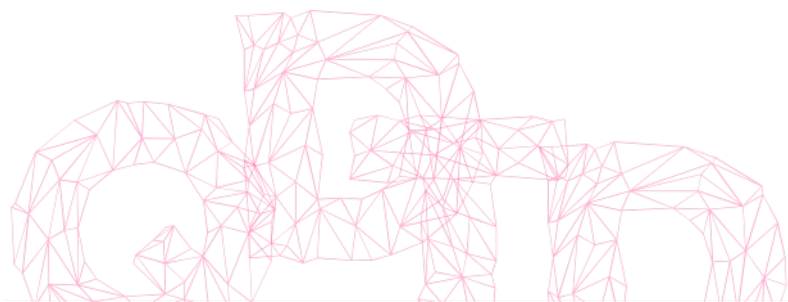
En este parámetro se analiza si la compañía tiene un posicionamiento institucional público en el que haya reconocido sus responsabilidades de *respeto y protección de derechos humanos*, incluyendo el *derecho a la privacidad*. Para este efecto, se analiza si existe algún posicionamiento que cumpla con las características señaladas por el Principio 16 de los Principios Rectores sobre las Empresas y los Derechos Humanos aprobados por el Consejo de Derechos Humanos de la Organización de las Naciones Unidas a través de la resolución 17/4, de 16 de junio de 2011 a saber:

“Compromiso Político

16. Para asumir su responsabilidad de respetar los derechos humanos, las empresas deben expresar su compromiso con esta responsabilidad mediante una declaración política que:

- a) Sea aprobada al más alto nivel directivo de la empresa;*
- b) Se base en un asesoramiento especializado interno y/o externo;*
- c) Establezca lo que la empresa espera, en relación con los derechos humanos, de su personal, sus socios y otras partes directamente vinculadas con sus operaciones, productos o servicios;*
- d) Se haga pública y se difunda interna y externamente a todo el personal, los socios y otras partes interesadas;*
- e) Quede reflejada en las políticas y los procedimientos operacionales necesarios para inculcar el compromiso asumido a nivel de toda la empresa.”*

El posicionamiento político debe ser público y reflejar claramente el compromiso de la empresa de respetar los derechos humanos en el marco de sus actividades empresariales.

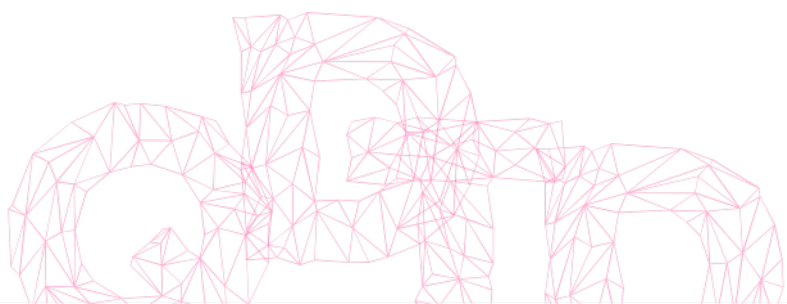




En este criterio se evalúa si la compañía ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad.

También se evalúa, si participa en algún mecanismo sectorial o multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales (Ejemplos: *Global Network Initiative* o *Telecommunications Industry Dialogue*).

Por otro lado, es esencial que la compañía cuente con políticas de participación en las discusiones locales e Internacionales sobre el ecosistema de Internet; los Foros de Gobernanza de Internet (IGF) son espacios de debate público propiciados por Naciones Unidas, donde se discutan de forma abierta los principios compartidos, normas, reglas, procesos de toma de decisión y programas, que modelan la evolución y el uso de Internet.



5. TRANSPARENCIA

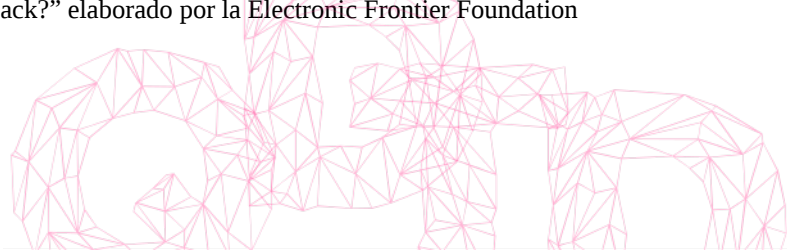
El Principio 21 de los Principios Rectores sobre las Empresas y los Derechos Humanos de Naciones Unidas, exige buenas prácticas a las empresas sobre transparencia desde la perspectiva de los Derechos Humanos.

Los *informes de transparencia* del sector TIC en relación al impacto de la privacidad de los usuarios han sido más frecuentes en los últimos años⁵². La publicación de un informe de transparencia sobre las *solicitudes de acceso a datos* por parte de autoridades de seguridad y justicia debe proveer suficiente información para evaluar el contenido y el alcance de las medidas de vigilancia por parte de las autoridades.

Los *informes de transparencia* son declaraciones emitidas por empresas que contienen una variedad de estadísticas relacionadas con las solicitudes de datos. Las empresas de Internet de todo el mundo han adoptado la práctica de publicar informes de transparencia activa para informar cómo y cuándo cooperan con el gobierno, en general, porque lo exige la ley, mediante la divulgación de información que puede ser utilizada como prueba en los casos civiles y penales. Esta ya es una buena práctica establecida entre empresas de contenidos como Google, Facebook, Twitter y Microsoft y los proveedoras como Vodafone y Verizon.

Este criterio evalúa la publicación de estadísticas respecto a cuántas solicitudes de información han sido recibidas y cumplidas, así como la inclusión de detalles sobre el tipo de solicitudes, instituciones solicitantes y la motivación y fundamentación de las autoridades. El cumplimiento parcial de este criterio es recompensado con media estrella.

52 La Guía de Implementación de los Principios Rectores para el Sector TIC (Tecnologías de la Información y la Comunicación) elaborada por la Comisión Europea; la Guía de Implementación de la Iniciativa de Internet Global (Global Network Initiative); el reporte “Who has your back?” elaborado por la Electronic Frontier Foundation





6. BLOQUEO DE CONTENIDOS EN INTERNET

La ISP publica los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y además indica los soportes legales/contractuales que justifican dichas acciones. Si la compañía aclara las motivaciones que le llevan a filtrar/retirar/bloquear contenidos o a suspender/cancelar servicios.

En este criterio se analiza las políticas que tiene la ISP sobre bloqueos/filtrados/retirada de contenidos sea por carácter judicial en lo penal y/o civil: pornografía infantil, derecho de autor, derecho al olvido, seguridad nacional, entre otros. Así como criterios internos como el principio de *neutralidad en la red*.

En la [Declaración Conjunta](#)⁵³ de 2011 sobre libertad de expresión e Internet, los relatores para la libertad de expresión de la ONU, OSCE, OEA y CADHP, indicaron que:

“La interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional”.

Asimismo, afirmaron que:

“El bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o ciertos tipos de usos (como las redes sociales) constituye una medida extrema—análoga a la prohibición de un periódico o una emisora de radio o televisión—que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual”.

Y finalmente:

“Los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión”.

Por otro lado, según *Internet Society*, el principio de *neutralidad en la red* se conforma como un elemento central del funcionamiento de Internet:

53 <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849>



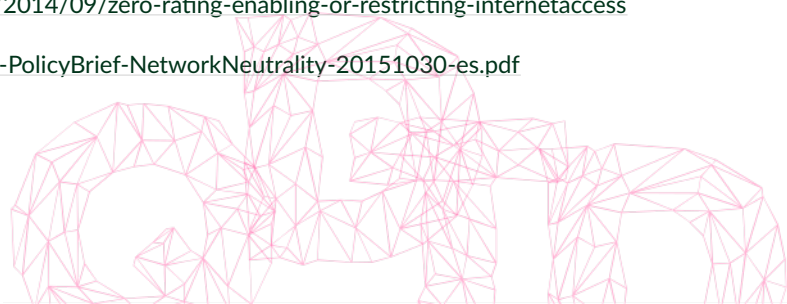
“Un elemento clave de la arquitectura de Internet es que los datos de los usuarios se transmitan en forma de paquetes de información estandarizados, sin considerar su contenido, su emisor ni su destinatario. Este enfoque no discriminatorio frente al tráfico de Internet es una premisa central del funcionamiento de Internet. Permite que los datos fluyan fácilmente a través de las redes sin que su paso sea obstaculizado a causa de la naturaleza de los mismos. Básicamente, este enfoque de interconexión abierta es uno de los pilares que sustentan Internet y que han permitido su éxito”⁵⁴.

Este principio se encuentra regulado en Paraguay, en el artículo 26 de la resolución 190/2009 de CONATEL de la siguiente forma:

“[...] que los datos de los usuarios se transmitan en forma de paquetes de información estandarizados, sin considerar su contenido, su emisor ni su destinatario”.

Este criterio evalúa si La ISP especifica los procedimientos para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios teniendo en cuenta el debido proceso; lo que supone como mínimo: notificación al usuario, oportunidad de defensa, criterios de proporcionalidad, etc..

54 → “Open Inter-networking: Getting the fundamentals right: access, choice, and transparency,” 21 de febrero de 2010, <http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choiceand-transparency>
 → “Network neutrality—let those packets flow,” 30 de marzo de 2015, <http://www.internetsociety.org/blog/asia-pacific-bureau/2015/03/network-neutrality---let-those-packetsflow>
 → “Zero rating: enabling or restricting Internet access?” 24 de septiembre de 2014, <http://www.internetsociety.org/blog/asia-pacific-bureau/2014/09/zero-rating-enabling-or-restricting-internetaccess>
 → “Neutralidad de la red” 30 de octubre de 2015, <https://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030-es.pdf>





METODOLOGÍA

Para esta investigación se analizó documentación sobre cada proveedora de Internet y luego se intentó establecer contacto con cada una de ellas. Se logró socializar los resultados preliminares de evaluación con las empresas Tigo, Personal, Vox y Claro, pero no se tuvo respuesta de Copaco, ni de Chaco Comunicaciones. En estas reuniones se presentó la metodología de evaluación que sería implementada para el año 2017, así como recibir retroalimentación por parte de las propias ISP.

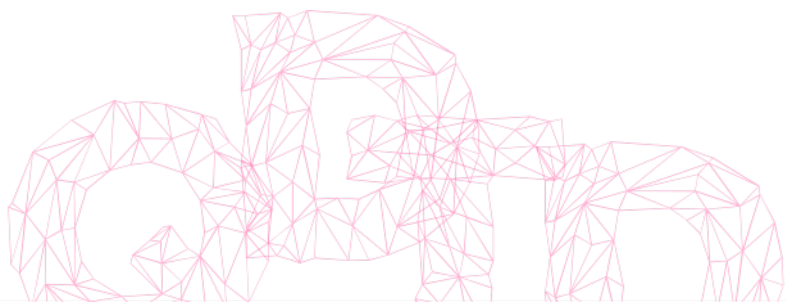
CATEGORÍA 1: POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Lo que precisamos saber es: ¿La ISP proporciona información clara y completa sobre la recopilación, uso, almacenamiento, procesamiento y protección de datos personales del usuario?

En esta categoría, se evalúan las *políticas y avisos de protección de datos y privacidad* de la compañía, disponible públicamente, sobre el tratamiento de los datos personales que obtiene al prestar el servicio de telecomunicaciones, y no únicamente sobre datos que otorga la persona al contratar el servicio o utilizar el sitio web de la compañía. ¿Se establece de manera precisa qué información de usuario y de sus comunicaciones son obtenidas, almacenadas, así como la temporalidad con la que dichos datos son almacenados?

¿Cuáles son los criterios de evaluación?

- I) *La compañía proporciona información y claras referencias legales sobre la recopilación de datos personales, incluyendo los datos personales que se recogen y en qué situaciones se produce la recogida;*
- II) *La compañía proporciona información y claras referencias legales sobre el uso y/o procesamiento de datos personales, incluyendo los fines para los que se utilizan y cómo se produce este;*
- III) *La compañía proporciona información y claras referencias legales en el almacenamiento de datos personales, incluyendo cuánto tiempo se almacenan los datos así como donde se almacenan y cuando se eliminan, si es que se eliminan;*



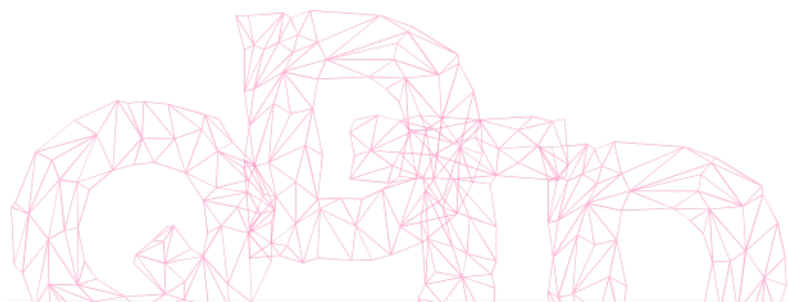
IV) La compañía proporciona información y claras referencias legales sobre protección de datos personales, incluyendo las prácticas de seguridad que se observan en los procedimientos de retención de datos, si existe política de anonimización de datos y quién/es tendría/n acceso a las bases de datos;

V) La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo;

VI) Es fácil acceder a esta información en el sitio web de la compañía.

Estándares de desempeño:

POLÍTICA DE PRIVACIDAD	
★	La ISP cumple 5 a 6 criterios
★	La ISP cumple 3 a 4 criterios
★	La ISP cumple 2 criterios
★	La ISP no cumple ninguno o sólo reúne uno de los criterios





CATEGORÍA 2: AUTORIZACIÓN JUDICIAL

Precisamos saber: ¿La ISP se comprometen a divulgar información del cliente, metadatos y contenidos de las comunicaciones únicamente en presencia de una orden judicial?

En esta categoría se evalúa si la compañía exige a las autoridades, la presentación de autorización judicial de manera previa a la entrega de datos sobre el contenido de las comunicaciones o sus metadatos. Si la compañía, en su contrato o cualquier documento oficial a disposición del público deja claro a los usuarios las circunstancias en que las autoridades judiciales o administrativas pueden tener acceso a sus datos.

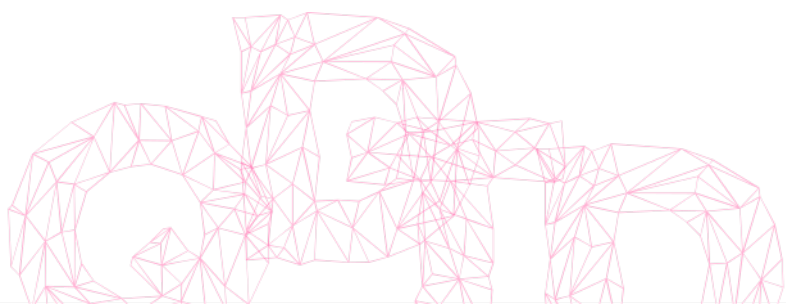
¿Cuáles son los criterios de evaluación?

I) La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa;

II) La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa.

Estándares de desempeño:

AUTORIZACIÓN JUDICIAL	
★	La ISP cumple con ambos criterios
★	La ISP cumple con uno de los criterios
★	La ISP no cumple ninguno de los criterios



CATEGORÍA 3: NOTIFICACIÓN AL USUARIO

Queremos saber: ¿Las ISP notifican a los usuarios afectados por solicitudes de obtención de datos personales por parte de autoridades o si han promovido el retiro de obstáculos para llevar a cabo la notificación?

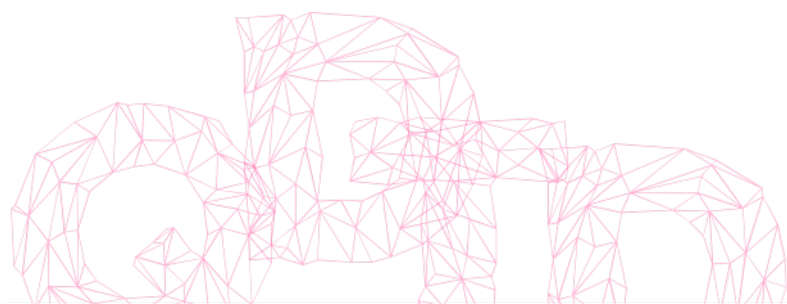
Para obtener una estrella en esta categoría, las empresas deben tener una *política de notificación* a usuarios afectados por medidas de *vigilancia estatal* en el primer momento permitido por la ley o, en su caso, demostrar que han combatido legalmente los impedimentos legales o regulatorios para llevar a cabo la notificación o, alternatively, demostrar que han promovido mecanismos de notificación al usuario al congreso o a otros entes regulatorios.

¿Cuáles son los criterios de evaluación?

1) La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible.

Estándares de desempeño:

NOTIFICACIÓN AL USUARIO	
★	La ISP cumple el criterio
☆	La ISP no cumple el criterio





CATEGORÍA 4: POSICIONAMIENTO PÚBLICO EN CONTRA DE LA VIGILANCIA MASIVA O SIN CONTROL

Precisamos saber: ¿Ha iniciado el ISP un posicionamiento público sobre el respeto y la promoción de los derechos humanos en Internet, en especial contra la vigilancia masiva o vigilancia sin control de las comunicaciones?

En esta categoría se evalúa si las empresas han expresado de manera pública su postura de rechazo a la *vigilancia masiva*, o a la vigilancia sin controles adecuados para impedir vulneraciones a la privacidad de sus usuarios. Si posee una *política institucional* en la que reconoce sus responsabilidades de respeto y protección de los derechos humanos, incluyendo el derecho a la privacidad; y si participa en algún foro o mecanismo para el respeto de derechos humanos en el ámbito de sus responsabilidades empresariales.

Es muy importante conocer las posiciones adoptadas por las empresas en cuanto a privacidad de los usuarios y los derechos de protección de datos. Esta categoría tiene como objetivo evaluar la participación de los ISP en el debate público en relación con las cuentas y las políticas públicas que pueden impactar esos derechos.

También se evalúa si la empresa ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad.

En esta edición de “*Quién defiende tus datos*”, hemos seguido la contribución de los ISP en los debates públicos más importantes recientemente (desde 2015 hasta 2016) entre los que se cuentan: los debates sobre *Retención de datos de tráfico*, la ley de *Protección de la Niñez de Contenidos Nocivos* y el *Plan Nacional de Ciberseguridad*. Para esta evaluación, hemos considerado sólo las contribuciones hechas por los ISP de forma individual y no por las asociaciones que algunos ISP pueden ser parte –como la Cámara de Proveedoras de Internet del Paraguay.

¿Cuáles son los criterios de evaluación?

1) La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por asociaciones que la empresa pueda ser parte no se consideran); es decir, la



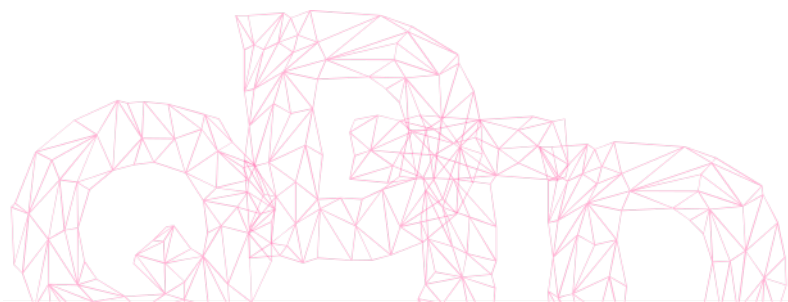
compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”.

II) Participa en algún mecanismo sectorial o multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global)

III) La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISP forman parte del “grupo empresas”, actor clave para el ecosistema de Internet.

Estándares de desempeño:

POSICIONAMIENTO CONTRA VIGILANCIA MASIVA	
★	La ISP cumple con todos los criterios
★	La ISP cumple dos criterios
★	La ISP no cumple ninguno de los criterios





CATEGORÍA 5: TRANSPARENCIA

Precisamos saber: ¿La ISP publica informes de transparencia que contienen información sobre cuántas veces los gobiernos han solicitado datos del usuario y la frecuencia con que la empresa proporcionó esos datos a los gobiernos?

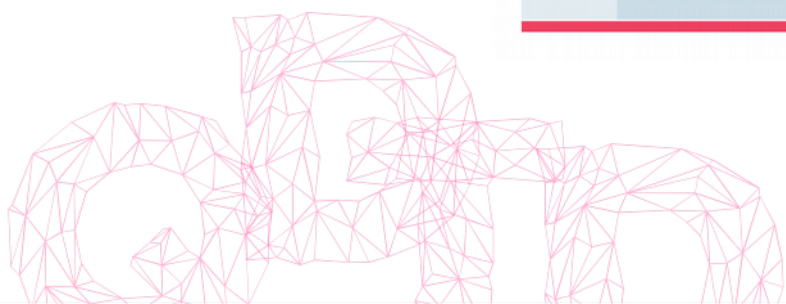
Se evaluará si el informe de transparencia evidencia el número de usuarios y usuarias que han sido notificados en el último año con relación al número de solicitudes por parte del Gobierno. El informe de transparencia notifica el origen de las solicitudes para el bloqueo o retiro de contenidos de Internet –incluyendo pornografía infantil, infracción al derecho de autor, cumplimiento de sus propias políticas, etc.. Si bien las ISP en Paraguay no están bajo ninguna obligación de producir informes de *transparencia activa*, esto podría ser una ventana de oportunidad para mostrar que están preocupadas por la construcción de confianza en sus relaciones con los clientes, basadas en la transparencia.

¿Cuáles son los criterios de evaluación?

- I) La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales;
- II) La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos –si se trata de información de cuenta o de conexión de registros; (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental –presentación de pruebas en materia civil, penal, o los casos administrativos, etc..

Estándares de desempeño:

TRANSPARENCIA	
★	La ISP cumple con ambos criterios
★	La ISP cumple con uno de los criterios
★	La ISP no cumple ninguno de los criterios



CATEGORÍA 6: BLOQUEO DE CONTENIDOS EN INTERNET

Precisamos saber: ¿la ISP es clara con los y las usuarias sobre las formas en que filtra, retira o bloquea contenidos y cancela o suspende servicios?

Se evalúa si la ISP publica los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios y, además, indica los soportes legales/contractuales que justifican dichas acciones. La compañía aclara las motivaciones que lo llevan a filtrar/retirar/bloquear contenidos o a suspender/cancelar servicios. La ISP especifica los procedimientos para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios teniendo en cuenta el debido proceso; lo que supone como mínimo: notificación al usuario, oportunidad de defensa, criterios de proporcionalidad, etc..

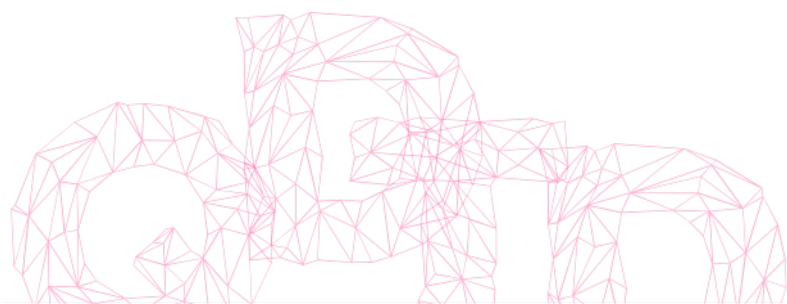
¿Cuáles son los criterios de evaluación?

I) La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican;

II) La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios

Estándares de desempeño:

BLOQUEO DE CONTENIDOS	
★	La ISP cumple con todos los criterios
★	La ISP cumple dos criterios
☆	La ISP no cumple ninguno de los criterios

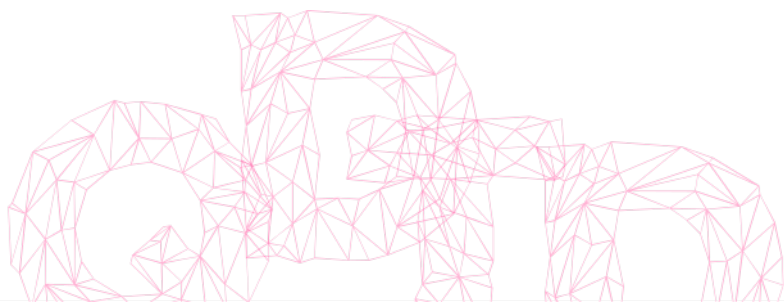


REPORTES DE EVALUACIÓN

REPORTE 0: CUADRO GENERAL COMPARATIVO 2017

CUADRO GENERAL COMPARATIVO 2017

CRITERIOS	Política de privacidad y protección de datos	Autorización Judicial	Notificación	Posicionamiento público en contra de la vigilancia	Informes de transparencia	Bloqueo de contenidos en Internet	Porcentaje de cumplimiento
	★	★	★	★	★	★	41,6 %
	★	★	★	★	★	★	25 %
	★	★	★	★	★	★	33,3 %
	★	★	★	★	★	★	33,3 %
	★	★	★	★	★	★	25 %
	★	★	★	★	★	★	16,6 %



REPORTE 1: POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS

REPORTE 1: Política de privacidad y protección de datos		
TIGO	VOX	CLARO
☆	☆	☆
COPACO	PERSONAL	CHACO COMUNICACIONES
☆	☆	☆

Tigo, Personal, Copaco, Claro, Vox y Chaco Comunicaciones *no tienen una política o aviso de privacidad* disponible en su página principal de Internet por lo que ninguna compañía cumple con el criterio. Algunas cuentan con *Términos y Condiciones* para el uso de la web, como Tigo y Personal; esta información es importante pero no suficiente para la protección del derecho a la intimidad de los que contratan el servicio de telefonía e Internet.

No obstante, en la entrevista realizada con las ISPs Tigo, Personal, Vox y Claro se comprometieron en revisar esta calificación.

Ninguna ISP indica de manera clara qué información se recaba sobre el usuario y sus comunicaciones, ni por cuánto tiempo se conservan los datos personales.

Recomendación:

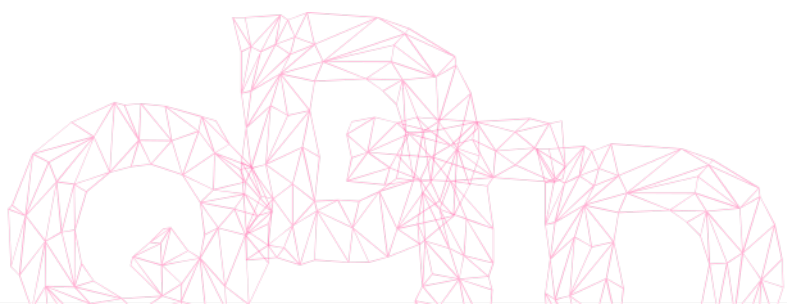
Las ISP deben trabajar en la *transparencia* de tratamiento de datos de sus clientes. La publicación de sus políticas sobre privacidad y datos personales deben ofrecer claridad a sus usuarios.

Estos *avisos de privacidad y tratamiento de datos* forman parte de los estándares de economía digital que promueven los reportes de la OECD –desde este 2017, Paraguay es miembro oficial de esta organización. La adecuaciones mínimas a estas





normas de buenas prácticas visibilizaría a nivel regional y mundial la responsabilidad y compromiso de las empresas locales en la calidad de la conectividad de los habitantes del territorio paraguayo.



REPORTE 2: AUTORIZACIÓN JUDICIAL

REPORTE 2: Autorización judicial		
TIGO	VOX	CLARO
★	★	★
COPACO	PERSONAL	CHACO COMUNICACIONES
★	★	★

La Constitución de la República es clara al exigir que las autoridades designadas por las leyes deben obtener una *autorización judicial* antes de obtener acceso al contenido de las comunicaciones.

Si bien este requisito para la colaboración no se encuentra detallado en ninguna web de las ISP entrevistadas, no existen evidencias que las proveedoras de Internet no hayan entregado información de servicio de Internet sin orden judicial.

Sin embargo es importante destacar que las ISP Tigo, Personal y Claro manifestaron su preocupación por los servicios de telefonía. En ese caso están obligadas a facilitar información de los metadatos de la llamada –conocido como “cruce de llamadas”– por solicitud fiscal. Este mecanismo fue aceptado por la Corte Suprema sin tener en cuenta las sentencias internacionales vinculantes a nuestra jurisdicción nacional que indican la autoridad judicial como único mecanismo posible.

Por otro lado, según ISP entrevistadas, se han dado caso casos en que han rechazado solicitudes de acceso a *datos de llamadas telefónicas* por no cumplir con los requisitos legales, tales como número de expediente, hecho punible, argumentos, etc.. Sin embargo sigue habiendo irregularidades en el acceso y divulgación de los datos de los clientes que





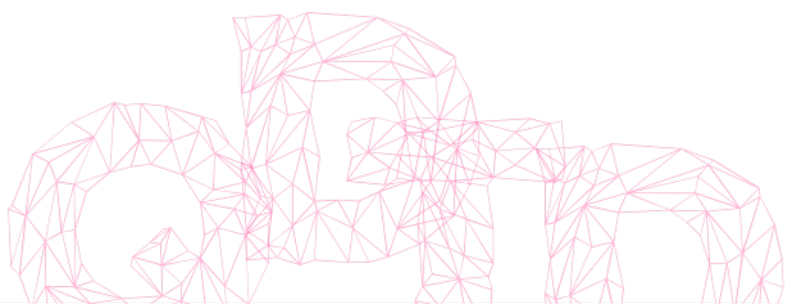
contratan servicios de telefonía, sin los requisitos legales. Un ejemplo de ello es el caso del espionaje sobre la periodista de *ABC Color*, por parte de las fuerzas militares, en el que se comprobó que empleados de Personal filtró información, violentando no solo su privacidad sino también afectando la libertad de expresión en un estado democrático.

Por último, para casos de servicios de Internet, según las entrevistas, Tigo, Personal y Claro no conservan los *datos de tráfico* de sus usuarios. Por su parte, Copaco y Vox no solo retienen sino que facilitan información sobre datos/metadatos de sus usuarios a las autoridades de persecución penal. Esto último es preocupante, ya que por un lado, cumplen la ley de Comercio Electrónico, al almacenar la información, pero la violan al entregarla con finalidades diferentes a la prevista en dicha ley.

Recomendación:

Establecer explícitamente este requisito en el *aviso de privacidad y tratamiento de datos personales* para la colaboración con autoridades de seguridad y justicia que implique la intervención del contenido de comunicaciones privadas.

Asimismo, es deseable que tanto Copaco como Vox incluyan en sus avisos detalles del tratamiento que realizan sobre los metadatos almacenados. Se ha demostrado – por jurisprudencias internacionales vinculantes a nuestro sistema judicial– que los metadatos pueden revelar aspectos sensibles de la vida privada de las personas. Por tanto es indispensable que los titulares de dichos datos tengan acceso a los mismos cuando lo soliciten.



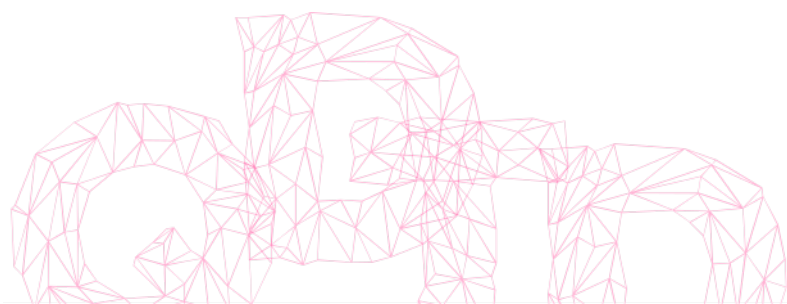
REPORTE 3: NOTIFICACIÓN

REPORTE 3: Notificación		
TIGO	VOX	CLARO
☆	☆	☆
COPACO	PERSONAL	CHACO COMUNICACIONES
☆	☆	☆

En este criterio encontramos una situación compleja: las ISP entrevistadas *no reconocen* el rol central que juegan en la defensa de la intimidad de sus usuarios. Como no existen avisos de privacidad, no hay información sobre la forma de entrega de la información personal a las instituciones autorizadas por el Estado, ni existen detalles sobre el procedimiento que se debe emplear cuando esto sucede.

Recomendación:

Es deseable que las ISP tengan una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia –por ejemplo por poner en riesgo la efectividad de una investigación o comprometer físicamente la integridad de una persona– no se detectó una *política de notificación* para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.



REPORTE 4: POSICIONAMIENTO PÚBLICO EN CONTRA DE LA VIGILANCIA MASIVA O SIN CONTROL

REPORTE 4: Posicionamiento público en contra de la vigilancia masiva o sin control		
TIGO	VOX	CLARO
		
COPACO	PERSONAL	CHACO COMUNICACIONES
		

Únicamente la empresa Claro a través de América Móvil, fue detectada con el compromiso público de reconocimiento de sus responsabilidades empresariales en materia de derechos humanos y ha expresado públicamente su rechazo a medidas de vigilancia masiva y sin controles⁵⁵.

El caso del espionaje de la periodista de ABC por parte de las fuerzas militares con la complicidad de un empleado de Personal, fue un escenario importante para que todas las ISP se posicionen contra este tipo de abuso, además de llevar el caso en instancias penales. Lamentablemente ninguna ISP hizo público su repudio contra este tipo de acciones inconstitucionales e ilegales, ni suscribieron un compromiso de mejorar sus mecanismos de acceso a la información para generar mayor confianza de sus clientes.

No obstante, existen ISP que participaron en análisis legislativos que afectan la regulación de Internet y los derechos Humanos. Tigo, Personal y Claro se posicionaron en contra de la ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” durante las consultas públicas de las mesas de trabajo llevadas a cabo por la *Secretaría Nacional de la Niñez y Adolescencia*.

55 América Móvil Sustainability Report 2015 Pag 52. <http://www.americamovil.com/sites/default/files/2016-09/AMX-IS-2015-espanol.pdf>



En lo referente a *políticas públicas de seguridad digital*, todas las ISP entrevistadas, salvo Chaco Comunicaciones, han participaron de las mesas de trabajo para el desarrollo del *Plan Nacional de Ciberseguridad*.

Asimismo, la Empresa Tigo tiene una alta representación en instancias Internacionales sobre políticas de derechos humanos como *US Global Compact* capítulo Paraguay y *Telecommunications Industry Dialogue* a través de Millicom.

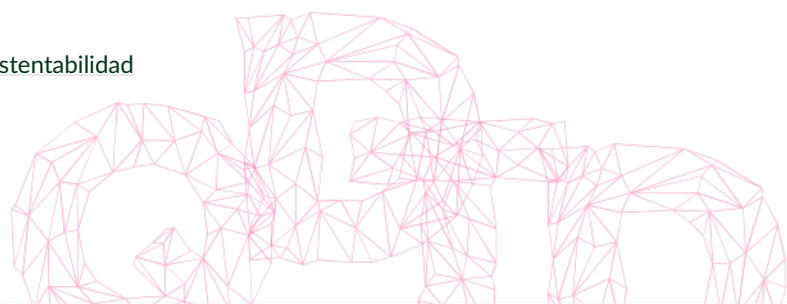
La ISP que le sigue en este criterio es Claro, que participa de *US Global Impact* a nivel internacional⁵⁶.

En lo que respecta a la participación en el Foro de Gobernanza de Internet, solo Copaco y Vox han cumplido con este criterio.

Recomendación:

Es deseable que las ISP formen parte de foros internacional y nacionales sobre los asuntos de Internet (*Foro de Gobernanza de Internet*) y participen en mecanismos para afrontar sus responsabilidades en materia de derechos humanos como *US Global Compact* (*Pacto global* – capítulo nacional o internacional) y *Telecommunications Industry Dialogue*. Asimismo, es clave la participación y opinión pública sobre acontecimientos que involucren a Internet para mejorar la transparencia en el cabildeo político, intereses que afectan a sus usuarios.

56 <http://www.americamovil.com/es/acerca-de-nosotros/sustentabilidad>





REPORTE 5: TRANSPARENCIA

REPORTE 5: Transparencia		
TIGO	VOX	CLARO
		
COPACO	PERSONAL	CHACO COMUNICACIONES
		

Unicamente, Tigo a través del informe anual de Millicom denominado “*Requests from law enforcement in South America*”⁵⁷ publica un informe de solicitudes de datos y metadatos de los usuarios solicitados por las autoridades judiciales. No obstante este informe sólo se encuentra disponible en inglés y no ofrece suficiente información que permita saber el volumen, origen, motivos y alcance de solicitudes. Tampoco el número e identidad de las autoridades que solicitan a acceder a dichos datos por lo que no se cumple el segundo punto del mismo criterio para completar la estrella.

Lamentablemente las demás ISP evaluadas no publicaron informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuario y sus comunicaciones.

Recomendación

El *informe de transparencia* es un elemento positivo para el resguardo de los derechos humanos. Conocer el número global de solicitudes realizadas por las autoridades de persecución penal, estadísticas respecto a las solicitudes realizadas por otras autoridades, identificación de las instituciones solicitantes, tipos de solicitudes y

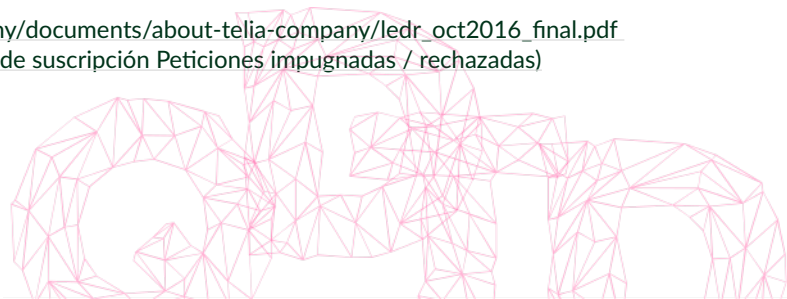
57 <http://www.millicom.com/media/8404741/Millicom-LED-Report-2016.pdf>



razones que fueron otorgadas para hacer la solicitud, son claves para hacer un seguimiento de la vigilancia estatal de las comunicaciones. Un ejemplo a seguir es TELIA Company⁵⁸ de Suecia y Finlandia, que además de clasificar y divulgar los datos de interceptación legal de datos de sus usuarios, también publica informes de sostenibilidad donde expone todos los casos en que ellos defendieron la privacidad y otros derechos humanos de sus usuarios.

Es importante recalcar que empresas intermediarias como Facebook, Google, Twitter divulgan en sus páginas web informes de transparencia donde se especifican las solicitudes de los gobiernos. Un hecho a destacar es que México ha incluido estos informes como una obligación legal.

58 http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/ledr_oct2016_final.pdf
(Clasifica por interceptación legal Datos históricos Datos de suscripción Peticiones impugnadas / rechazadas)





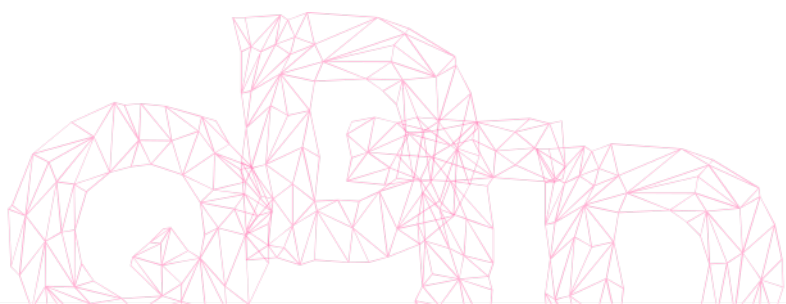
REPORTE 6: BLOQUEO DE CONTENIDOS EN INTERNET

REPORTE 6: Bloqueo de contenidos en Internet		
TIGO	VOX	CLARO
COPACO	PERSONAL	CHACO COMUNICACIONES

La única ISP que no cumple los estándares de servicio de acceso a Internet es Chaco Comunicaciones. En la web oficial se publican medidas de bloqueos contra las descargas mediante tecnologías peer-to-peer (p2p).

Las demás ISP no han adoptado medidas contractuales para el bloqueo de acceso a Internet. Cabe mencionar que en el 2010 ocurrió un caso de bloqueo: a una página web que realizó una parodia sobre el periódico nacional *Abc Color*. Afortunadamente, no se han encontrado evidencias de nuevos bloqueos similares.

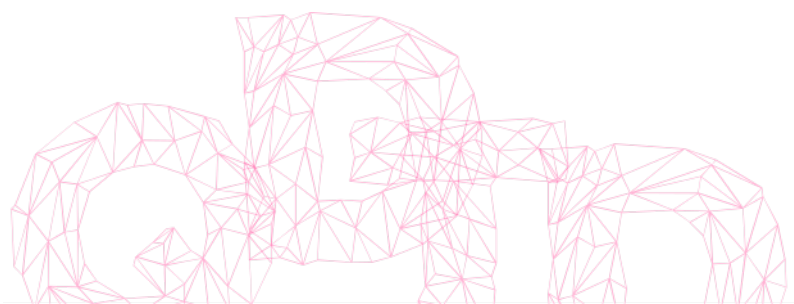
Estas ISP no han logrado de obtener todas las estrellas, porque no se encontraron guías o *códigos de conducta* que especifiquen los comportamientos esperados y los no permitidos por dichas empresas y así evitar sanciones a los usuarios.





Recomendación:

La suspensión preventiva y hasta la interrupción de los servicios de Internet para ciertos casos deben estar estipuladas en una guía o código para justificar el control, bloqueo y retiro de contenidos por parte de las ISP. Por tanto es indispensable que se describan estos criterios para garantizar a sus usuarios que los procedimientos de bloqueos seguirán una norma legítima y acorde a los estándares internacionales de derechos humanos.





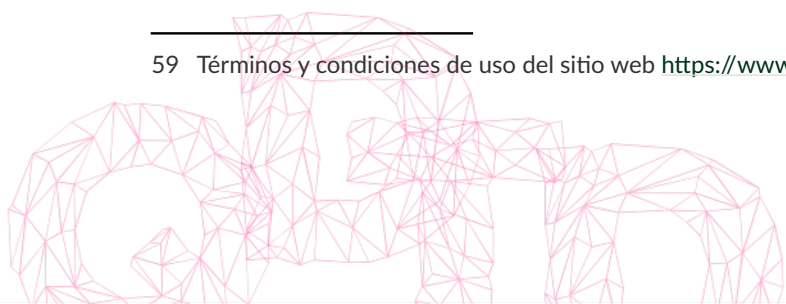
EVALUACIONES POR PROVEEDORA DE INTERNET

TIGO

Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la compañía. (X) No

Para esta evaluación se analizó la página web oficial de la compañía Tigo. La política sobre términos y condiciones se encuentra al pie de la web oficial. Podríamos calificar como accesible pero poco sencillo para la lógica del público en general a diferencia del apartado de “*código de conducta*” que se encuentra con mayor visibilidad y en varias partes del sitio web. La única parte que se refiere a *avisos de privacidad o políticas de la compañía* se encuentra en “*Términos y Condiciones de uso del sitio web*”⁵⁹. Es decir, la *política de privacidad*

59 Términos y condiciones de uso del sitio web <https://www.tigo.com.py/terminos-y-condiciones>



se refiere exclusivamente a la *persona que se encuentra navegando en su portal*. Esto no es un marco general de *política de privacidad o términos y condiciones* para el resto de los servicios que ofrecen.

Si bien, es una compañía que depende de la empresa internacional Millicom, que tiene disponible y accesible su política de privacidad⁶⁰, la misma no se encuentra traducida jurídicamente al español, ni adaptada a las leyes del país, es decir solo se refiere al sistema de *Common Law* del país anglosajón.

Por tanto, no cumple con el requisito de contar con una política de privacidad, ni los demás parámetros que se analizan sustantivamente en la política de privacidad. Se sugiere analizar a su sede **Tigo-Colombia** como un buen ejemplo de buenas prácticas en publicación de Términos y Condiciones Legales.

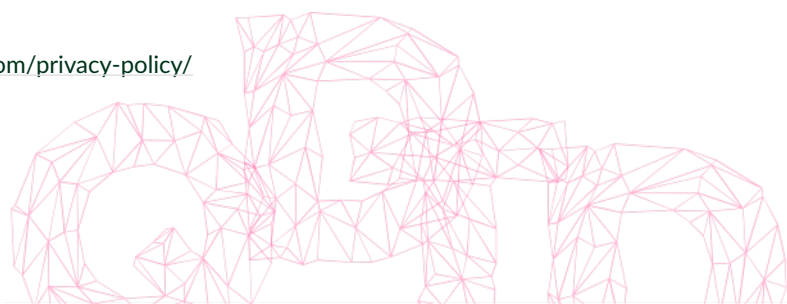


La ISP no cumple ninguno o sólo se reúne uno de los criterios.

Información sobre la divulgación de datos a las autoridades gubernamentales
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si
La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

La Constitución de la República es clara al exigir que las instituciones de persecución penal deban obtener los datos de las comunicaciones bajo la característica exclusiva de orden judicial previa. No hay evidencias concretas que Tigo haya facilitado información sin cumplir el “*debido proceso*” expuesto en el Código Procesal Penal vigente.

60 Política de privacidad de Millicom <http://www.millicom.com/privacy-policy/>





Es indispensable que la compañía Tigo exprese públicamente su política de exigir la autorización judicial cuando le son solicitados los datos y metadatos de las comunicaciones.



La ISP cumple con ambos criterios.

Notificación

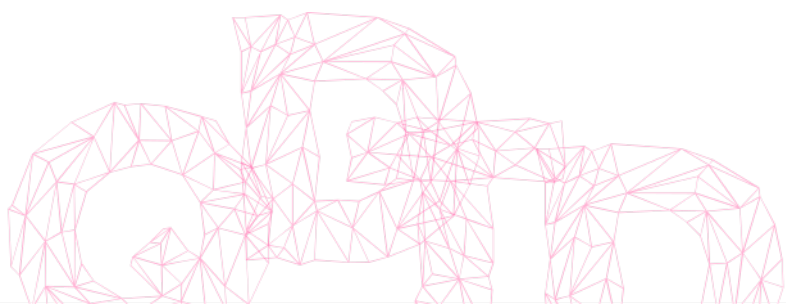
La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró evidencia de que la compañía evaluada tenga una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una política de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.



Informes de transparencias sobre las solicitudes de datos

La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (Y) si

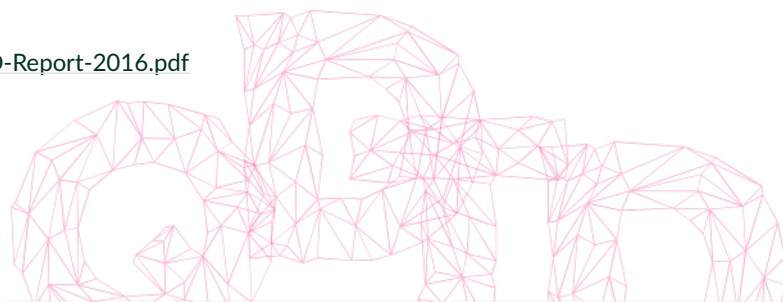
La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

Tigo a través del informe anual de Millicom denominado “*Requests from law enforcement in South America*”⁶¹ publica un informe de solicitudes de datos y metadatos de los usuarios solicitados por las autoridades judiciales. No obstante este informe sólo se encuentra disponible en inglés y no ofrece suficiente información que permita saber el volumen, origen, motivos y alcance de solicitudes, ni el número e identidad de las autoridades que solicitan a acceder a datos de comunicaciones de usuarios por lo que no se cumplen el segundo punto del mismo criterio para completar la estrella.



La ISP cumple uno los criterios.

61 <http://www.millicom.com/media/8404741/Millicom-LED-Report-2016.pdf>





Posicionamiento público en contra de la vigilancia masiva o sin control

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (Y) si

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (Y) si

La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISP forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (X) No

La compañía Tigo ha participado de mesas de trabajo de análisis legislativo sobre la ley “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet”, sin embargo no hay evidencia pública de que se hayan posicionado en contra de proyectos que ponen en riesgo los derechos fundamentales. También se corrobora que ha participado de la mesa de trabajo de la elaboración del Plan de Ciberseguridad según informe de la SENATICs.⁶²

Sobre el segundo punto, la compañía forma parte de los mecanismos para afrontar responsabilidad en materia de derechos humanos, pues participa tanto en el Pacto Global⁶³ capítulo Paraguay (Global Compact) como en el Diálogo de la Industria de las Telecomunicaciones (Telecommunications Industry Dialogue), a través de Millicom⁶⁴.

62 Plan de Ciberseguridad – Participantes
<https://www.senatic.gov.py/application/files/2614/6316/2380/Participantes.pdf>

63 <http://www.pactoglobal.org.py/>

64 <https://www.telecomindustrydialogue.org/about/>





Por último, no existen antecedentes de que la compañía Tigo participe de los Foros de Gobernanza de Internet en Paraguay (en el año 2016 se realizó su tercera edición) ni evidencias que participe en el foro a nivel mundial.

Por tanto se otorga media estrella por el cumplimiento de dos criterios.



La ISP cumple dos parámetros.

Filtro/bloqueo de Contenidos en Internet
La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X) No
La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios (Y) SI

Existen evidencias de bloqueos de acceso de contenidos a Internet en años anteriores⁶⁵ por parte de la compañía Tigo. Actualmente no se encontró evidencia alguna que se haya vuelto a repetir este tipo de bloqueos. Sin embargo es necesaria la política clara y accesible sobre la posibilidad y condiciones de bloqueo o retiro de contenidos.

Por tanto se otorga media estrella en esta categoría por no volver a reincidir en el bloqueo de contenidos.



La ISP cumple uno de los criterios.

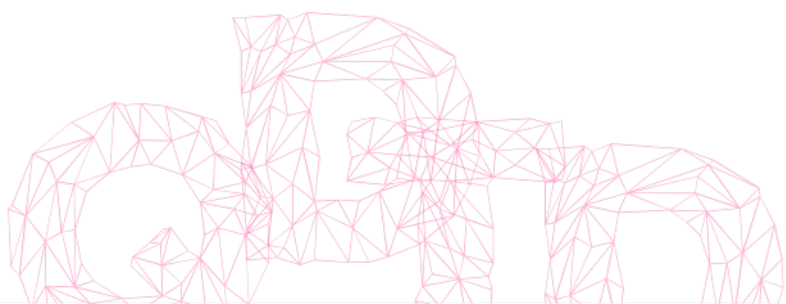
65 ABC.ME página de parodia del periódico ABC fue bloqueado por las ISP: Tigo y Personal <https://www.tedic.org/roben-este-post-neutralidad-en-la-red/>





A continuación se presenta el cuadro resumen de Tigo:

CÓMO PROTEGE TUS DATOS 		
1	Política de privacidad y protección de datos	
2	Autorización judicial	
3	Notificación	
4	Posicionamiento público en contra de la vigilancia masiva o sin control	
5	Transparencia	
6	Bloqueo de contenidos en Internet	





PERSONAL

Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la compañía. (X) No

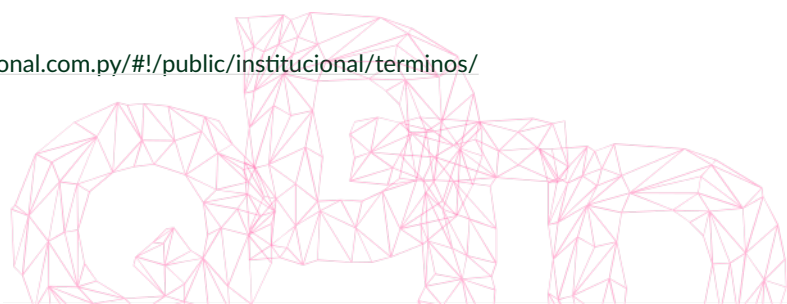
Para esta evaluación se analizó la página web oficial de la compañía Personal. La única parte que se refiere a Avisos de privacidad o políticas de la compañía se encuentra en “*Términos y Condiciones de uso del sitio web*”⁶⁶. Es decir, que la política de privacidad se refiere exclusivamente a la *persona que se encuentra navegando en su portal*. Esto no es un marco general de política de privacidad o términos y condiciones para el resto de los servicios que ofrecen.

Por lo tanto, no cumple con el requisito de contar con una política de privacidad, ni los demás parámetros que se analizan sustantivamente en la política de privacidad.



La ISP no cumple ninguno o sólo se reúne uno de los criterios.

66 Términos y condiciones de uso del sitio web <https://personal.com.py/#!/public/institucional/terminos/>





Información sobre la divulgación de datos a las autoridades gubernamentales

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si

La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

La Constitución de la República es clara al exigir que las Instituciones de persecución penal deban obtener los datos de la comunicación bajo la característica exclusiva de orden judicial previa. Este año la Fiscalía confirmó la vigilancia de una periodista del periódico ABC y se encontraron evidencias que la compañía Personal facilitó los datos sin el debido proceso⁶⁷, si bien este caso corresponde al servicio de telefonía y no al servicio de Internet de la empresa, es importante resaltar que el hecho ocurrido sobre los metadatos de los servicios de telecomunicaciones afecta indefectiblemente a nuestros derechos humanos, además de ser considerada inconstitucional⁶⁸.

Es indispensable que la compañía Personal exprese públicamente un posicionamiento contra la vigilancia Estatal de las comunicaciones, para reflejar el compromiso de respetar los derechos humanos y repudiar el hecho que involucra a la empresa. Asimismo debería exponer públicamente su política de exigir la autorización judicial cuando le son solicitados los datos y metadatos de las comunicaciones.

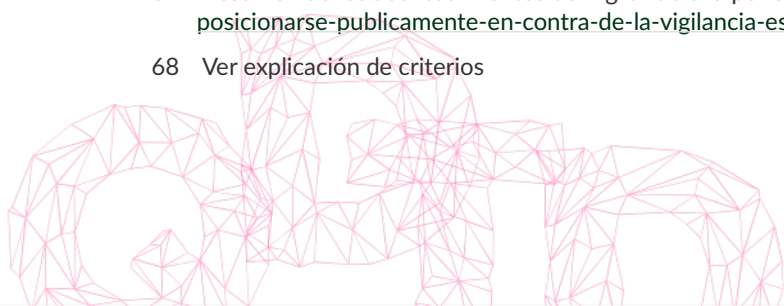
Por lo tanto se otorga una estrella, ya que la evaluación solo afecta a los servicio de Internet.



La ISP no cumple ninguno de los criterios.

⁶⁷ Resumen de los acontecimientos de Vigilancia a la periodista de ABC <https://www.tedic.org/personal-debe-posicionarse-publicamente-en-contra-de-la-vigilancia-estatal-ilegal/>

⁶⁸ Ver explicación de criterios





Notificación

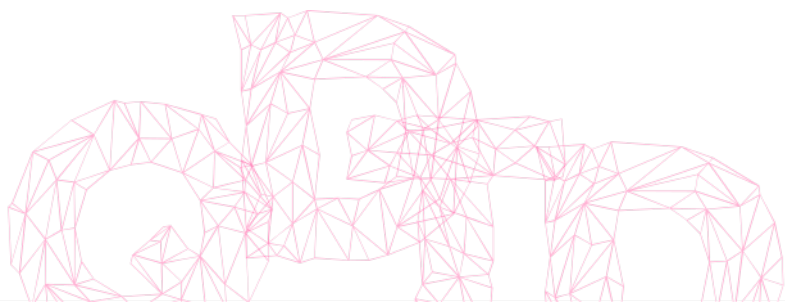
La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró que la compañía evaluada tenga una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una política de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.





Informes de transparencia sobre solicitudes de datos

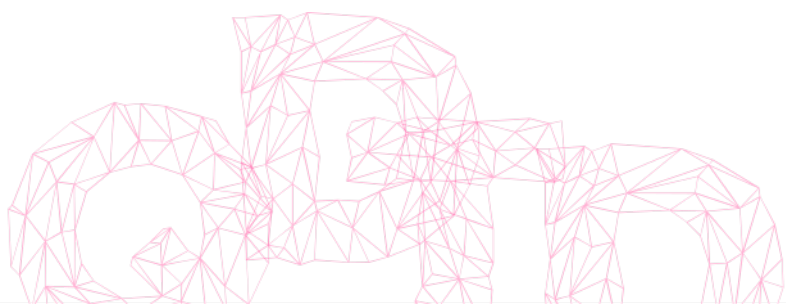
La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (X) No

La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

La compañía Personal no publica un informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones.



La ISP no cumple ninguno de los criterios.



Posicionamiento público en contra de la vigilancia masiva o sin controles, compromiso público

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (Y) si

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (X) No

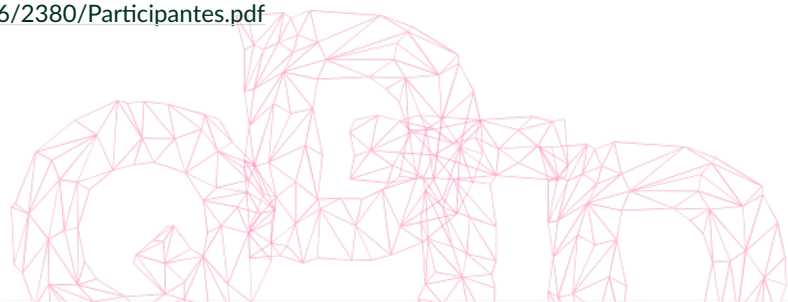
La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISP forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (X) No

La compañía Personal ha participado de mesas de trabajo de análisis legislativo sobre la ley “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet”, sin embargo no hay evidencia pública de que se haya posicionado en contra del proyecto y de otros que ponen en riesgo derechos fundamentales. También se corrobora que ha participado de la mesa de trabajo de la elaboración del Plan de Ciberseguridad según informe de la SENATICS.⁶⁹

Sobre el segundo punto, no se observa que la compañía forme parte de los mecanismos para afrontar responsabilidades en materia de derechos humanos, pues no participa ni del Pacto Global⁷⁰ capítulo Paraguay (Global Compact) ni de otros espacios internacionales donde se discuten estos temas.

⁶⁹ Plan de Ciberseguridad – Participantes
<https://www.senatics.gov.py/application/files/2614/6316/2380/Participantes.pdf>

⁷⁰ <http://www.pactoglobal.org.py/>





Y por último, no existen antecedentes de que la compañía Personal participe de los Foros de Gobernanza de Internet en Paraguay (en el año 2016 se realizó su tercera edición) ni de que participe en el foro a nivel mundial.

Por tanto no se otorga estrella alguna.



La ISP no cumple ninguno de los criterios.

Filtro/bloqueo de contenidos en Internet
La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X) No
La ISP tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios (Y) SI

Existen evidencias de bloqueos de acceso de contenidos a Internet en años anteriores⁷¹ por parte de la compañía Personal actualmente no se encontró evidencia alguna que se haya vuelto a repetir este tipo de bloqueos. Sin embargo es necesaria la política clara y accesible sobre la posibilidad y condiciones de bloqueo o retiro de contenidos.

Por tanto se otorga media estrella en esta categoría por no volver a reincidir en el bloqueo de contenidos.



La ISP cumple uno los criterios.

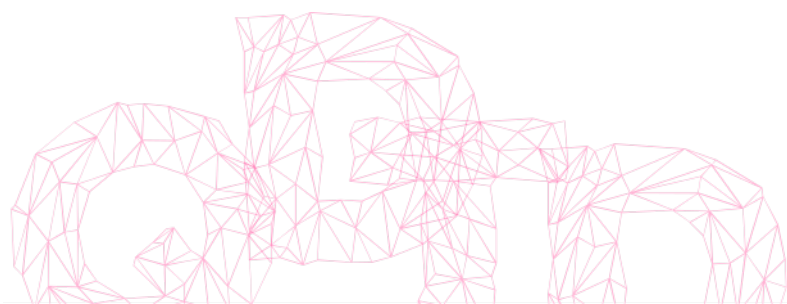
71 ABC.ME página de parodia del periódico ABC fue bloqueado por las ISP: Tigo y Personal <https://www.tedic.org/roben-este-post-neutralidad-en-la-red/>





A continuación se presenta el cuadro resumen de Personal:

CÓMO PROTEGE TUS DATOS <i>Personal</i>		
1	Política de privacidad y protección de datos	☆
2	Autorización judicial	★
3	Notificación	☆
4	Posicionamiento público en contra de la vigilancia masiva o sin control	☆
5	Transparencia	☆
6	Bloqueo de contenidos en Internet	★





CLARO

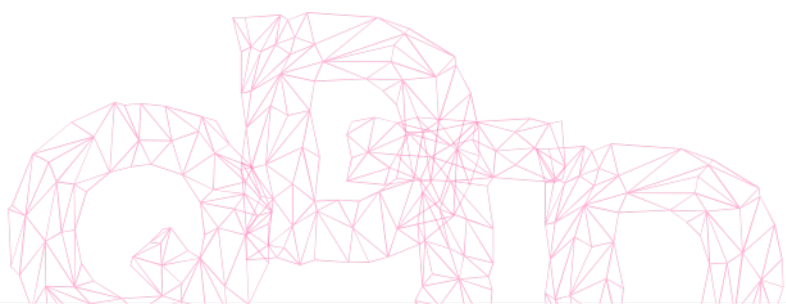
Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de internet de la compañía. (X) No

Para esta evaluación se analizó la página web oficial de la compañía Claro: la política sobre *términos y condiciones* no se encuentra disponible para acceso público.

Entonces, no cumple con el requisito de contar con una política de privacidad, ni los demás parámetros que analizan se sustentivamente en la política de privacidad. Se sugiere analizar a su sede [Claro-ARGENTINA](#) como ejemplo de buenas prácticas en publicación de Términos y Condiciones Legales.



La ISP no cumple ninguno o sólo se reúne uno de los criterios.





Información sobre la divulgación de datos a las autoridades gubernamentales

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si

La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

La Constitución de la República es clara al exigir que las instituciones de persecución penal deban obtener los datos de la comunicación bajo la característica exclusiva de orden judicial previa. No hay evidencias concretas que Claro haya facilitado información sin cumplir el “debido proceso” expuesto en el *Código Procesal Penal* vigente.

Es indispensable que la compañía Claro exprese públicamente su política de exigir la autorización judicial cuando le son solicitados los datos y metadatos de las comunicaciones. Por lo tanto se otorga una estrella.

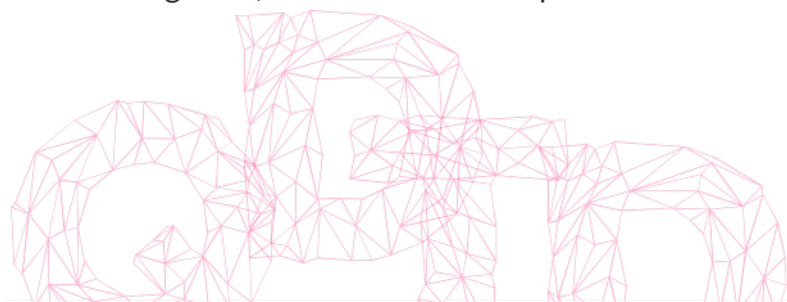


La ISP cumple con ambos criterios.

Notificación

La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró que la compañía evaluada tenga una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una política





de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.

Informes de transparencias sobre las solicitudes de datos

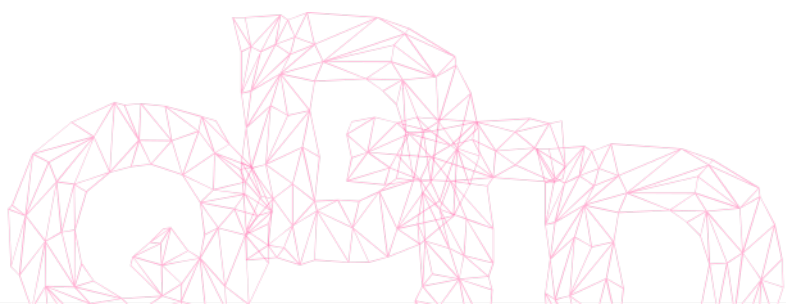
La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (X) No

La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

La compañía Claro no publica un *informe individual de transparencia* respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones.



La ISP no cumple ninguno de los criterios.



Posicionamiento público en contra de la vigilancia masiva o sin controles,
compromiso público

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (Y) si

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (Y) si

La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISP forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (X) No

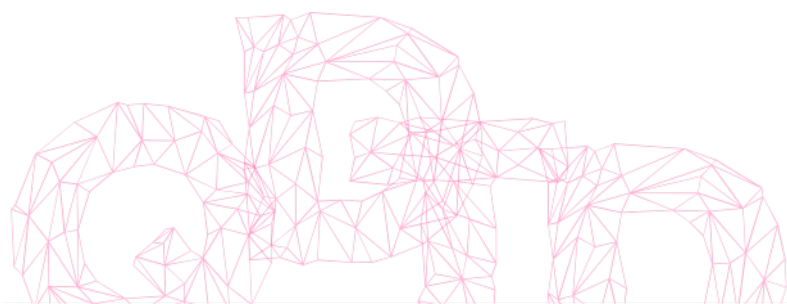
La compañía Claro no ha participado de mesas de trabajo de análisis legislativo sobre proyectos de ley, ni leyes vigentes que afectan Internet en Paraguay. No se encuentran evidencia pública de que se haya posicionado en contra de proyectos que ponen en riesgo derechos fundamentales. Sin embargo, ha participado de la mesa de trabajo de la elaboración del Plan de Ciberseguridad según informe de la SENATICs⁷².

Sobre el segundo punto, se observa que la compañía forma parte de Global Compact International⁷³ espacio internacional de dialogo sobre los Derechos Humanos y de los mecanismos para afrontar responsabilidad en materia de derechos humanos, aunque no participa ni en el Pacto Global⁷⁴ capítulo Paraguay (Global Compact).

72 Plan de Ciberseguridad – Participantes
<https://www.senatic.gov.py/application/files/2614/6316/2380/Participantes.pdf>

73 <http://www.americamovil.com/about-us/sustainability>

74 <http://www.pactoglobal.org.py/>





Y por último, no existen antecedentes de que la compañía Claro participe de los Foros de Gobernanza de Internet en Paraguay –en el año 2016 se realizó su tercera edición– ni evidencias que participe en el Foro a nivel mundial.

Según este parámetro de evaluación, a Claro se le puede otorgar media estrella.



La ISP cumple dos criterios.

Filtro/bloqueo de Contenidos en Internet
La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X) No
La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios Y (si)

No hay evidencias de que la compañía Claro haya realizado bloqueos de contenidos en Internet en años anteriores⁷⁵. De todos modos, es necesaria una política clara y accesible sobre la posibilidad y condiciones de bloqueo o retiro de contenidos.

Por tanto se otorga media estrella en esta categoría.



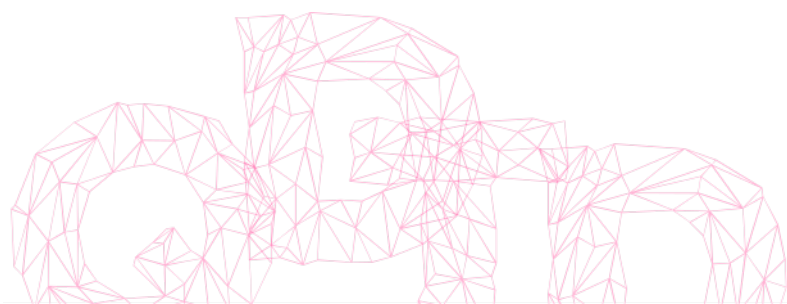
La ISP cumple uno de los criterios.

75 ABC.ME página de parodia del periódico ABC fue bloqueado por las ISP: Tigo y Personal <https://www.tedic.org/roben-este-post-neutralidad-en-la-red/>



A continuación se presenta el cuadro resumen de Claro:

CÓMO PROTEGE TUS DATOS 		
1	Política de privacidad y protección de datos	
2	Autorización judicial	
3	Notificación	
4	Posicionamiento público en contra de la vigilancia masiva o sin control	
5	Transparencia	
6	Bloqueo de contenidos en Internet	





Vox

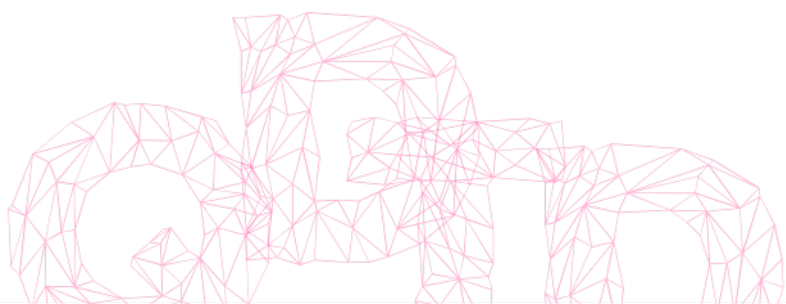
Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la compañía. (X) No

Para esta evaluación se analizó la página web oficial de la compañía Vox. La política sobre *términos y condiciones* no se encuentra disponible para acceso público.

Por lo que no cumple con el requisito de contar con una *política de privacidad*, ni los demás parámetros que se analizan sustantivamente en la política de privacidad.



La ISP no cumple ninguno o sólo reúne uno de los criterios.





Información sobre la divulgación de datos a las autoridades gubernamentales

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si

La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

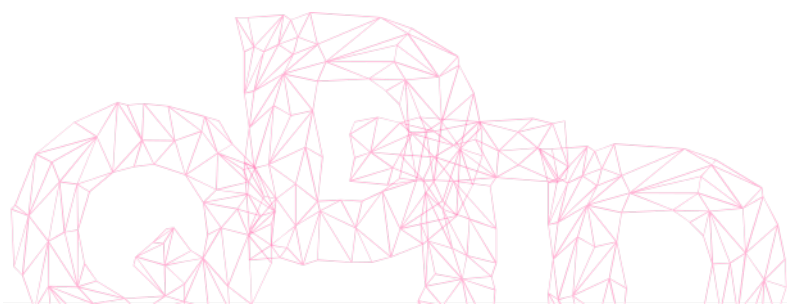
La Constitución de la República es clara al exigir que las instituciones de persecución penal deben obtener los *datos de las comunicaciones* bajo la característica exclusiva de *orden judicial previa*. No hay evidencias concretas de que Vox haya facilitado información sin cumplir el “*debido proceso*” expuestos en el *Código Procesal Penal* vigente.

Es indispensable que la compañía Vox exprese públicamente su política de exigir la autorización judicial cuando le son solicitados los datos y metadatos de las comunicaciones.

Por lo tanto se le otorga una estrella.



La ISP cumple con ambos criterios.





Notificación

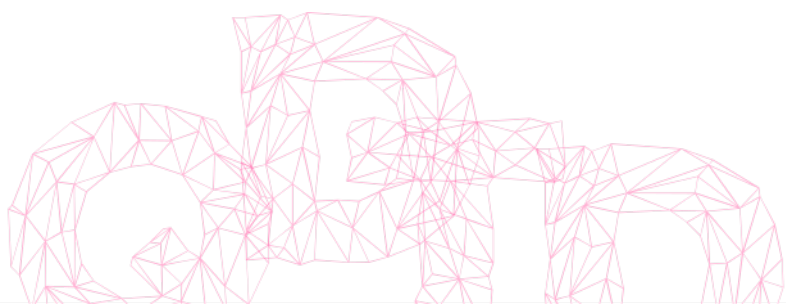
La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró evidencias de que Vox tenga una política pública de notificación a usuarios afectados por medidas de *vigilancia*. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una política de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.





Informes de transparencias sobre las solicitudes de datos

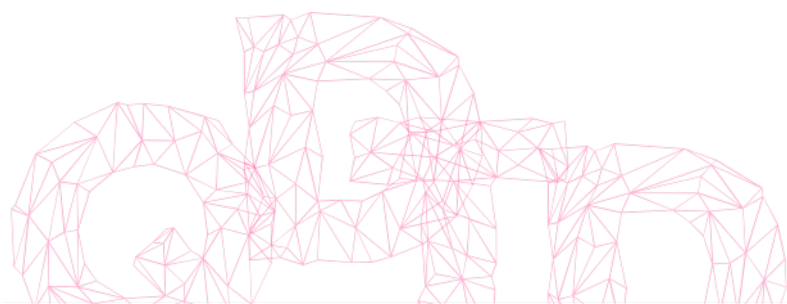
La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (X) No

La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

La compañía Vox no publica un informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones.



La ISP no cumple ninguno de los criterios.





Posicionamiento público en contra de la vigilancia masiva o sin controles

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los DDHH en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (Y) si

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (X) No

La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de multiples partes interesadas de Naciones Unidas por el cual las ISPs forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (Y) si

La compañía Vox no participado de mesas de trabajo de análisis legislativo sobre proyectos de ley, ni y leyes vigentes que afectan Internet en Paraguay. No se encuentran evidencias de que se hayan posicionado públicamente en contra de proyectos que pongan en riesgo los derechos fundamentales. Sin embargo la compañía, ha participado de la discusión en la construcción del *Plan Nacional de Ciberseguridad* durante los años 2015 y 2016⁷⁶.

Sobre el segundo punto, no se observa que compañía forme parte de los mecanismos para afrontar responsabilidad en materia de derechos humanos, pues no participa ni en el Pacto Global⁷⁷ capítulo Paraguay (Global Compact) ni en otros espacios internacionales donde se discuten estos temas.

Por último, se constata que en el año 2016, la compañía Vox participó del *Foro de Gobernanza de Internet* en Paraguay.

Se le otorga media estrella.



La ISP cumple dos criterios.

76 Informe de la SENATICs <https://www.senatic.gov.py/application/files/2614/6316/2380/Participantes.pdf>

77 <http://www.pactoglobal.org.py/>





Filtro/bloqueo de Contenidos en Internet

La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X) No

La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios (Y)Si

No hay evidencias de bloqueos de acceso a contenidos de Internet en años anteriores⁷⁸ por parte de la compañía Vox. Es necesaria la política clara y accesible sobre bloqueo o retiro de contenidos.

Por tanto se otorga media estrella en esta categoría.



La ISP cumple uno de los parámetros.

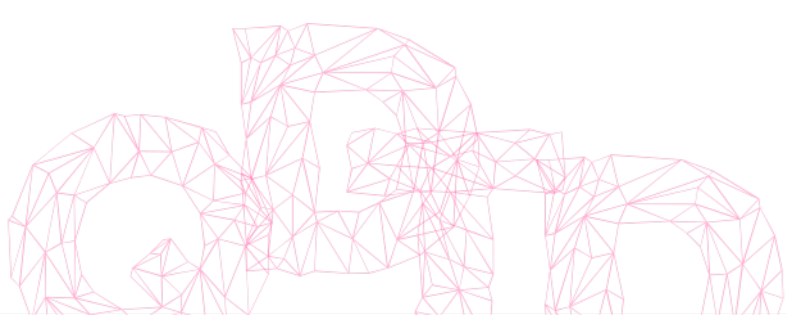
78 ABC.ME página de parodia del periódico ABC fue bloqueado por las ISP: Tigo y Personal <https://www.tedic.org/roben-este-post-neutralidad-en-la-red/>





A continuación se presenta el cuadro resumen de Vox:

CÓMO PROTEGE TUS DATOS 		
1	Política de privacidad y protección de datos	
2	Autorización judicial	
3	Notificación	
4	Posicionamiento público en contra de la vigilancia masiva o sin control	
5	Transparencia	
6	Bloqueo de contenidos en Internet	





COPACO

Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a 3ros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la compañía. (X) No

Para esta evaluación. TEDIC analizó la página web oficial de la compañía Copaco. La política sobre *términos y condiciones* no se encuentra disponible para acceso público.

En la sección “*Condiciones Generales de Uso*”⁷⁹, es en el único lugar donde aparecen referencias a “*Avisos de privacidad*” o políticas de la compañía. Sin embargo la política de privacidad se refiere exclusivamente a la *persona que se encuentra navegando en su sitio web*. Esto no es un marco general de política de privacidad o términos y condiciones para el resto de los servicios que ofrecen.

Por lo tanto no cumple con el requisito de contar con una *política de privacidad*, ni los demás parámetros que se analizan sustantivamente en la política de privacidad.



La ISP no cumple ninguno o sólo se reúne uno de los criterios.

79 Condiciones generales de uso del sitio web <https://www.copaco.com.py/portal/index.php/condiciones-generales-de-uso.html>





Información sobre la divulgación de datos a las autoridades gubernamentales.

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si

La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

La Constitución de la República es clara al exigir que las Instituciones de persecución penal deban obtener los datos de la comunicación bajo la característica exclusiva de *orden judicial previa*. No hay evidencias concretas que Copaco haya facilitado información sin cumplir el “*debido proceso*” expuesto en el *Código Procesal Penal* vigente.

Es indispensable que la compañía Copaco exprese públicamente su política de exigir la *autorización judicial* cuando le son solicitados los *datos y metadatos de las comunicaciones*. Por lo tanto se otorga una estrella.

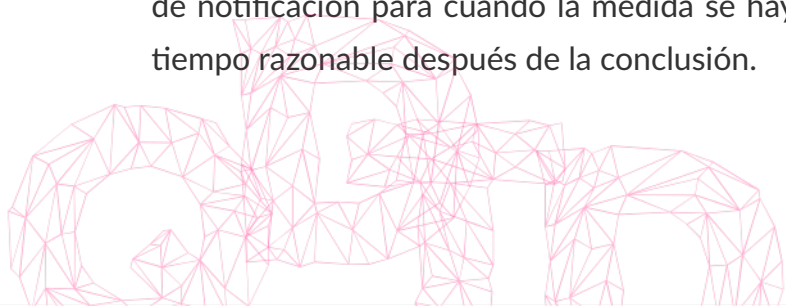


La ISP cumple con ambos criterios.

Notificación

La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró que la compañía evaluada tenga una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una política de notificación para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.





Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.

Informes de transparencias sobre las solicitudes de datos

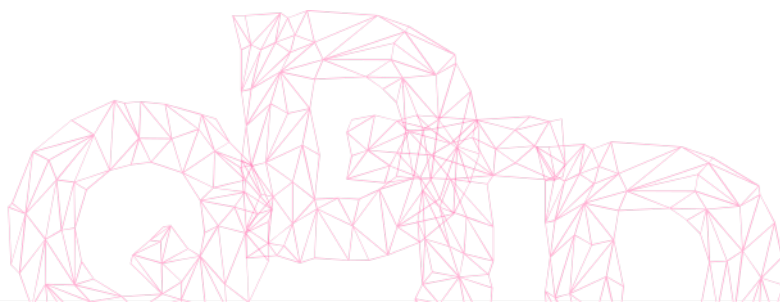
La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (X) No

La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

La compañía Copaco no publica un informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones.



La ISP no cumple ninguno de los criterios.





Posicionamiento público en contra de la vigilancia masiva o sin controles

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (Y) si

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (x) No

La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISPs forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (X) No

La compañía Copaco no ha participado de mesas de trabajo de análisis legislativo sobre proyectos de ley, ni leyes vigentes que afectan Internet en Paraguay. No se encuentran evidencias públicas de que se hayan posicionado en contra del proyecto que pone en riesgo los derechos fundamentales. Sin embargo, ha participado de la mesa de trabajo de la elaboración del Plan de Ciberseguridad según informe de SENATICs⁸⁰.

Sobre el segundo punto, no se observa que compañía forme parte de mecanismos para afrontar responsabilidad en materia de derechos humanos, pues no participa ni en el *Pacto Global*⁸¹ capítulo Paraguay (*Global Compact*) ni en otros espacios internacional en que se discuten estos temas.

80 Plan de Ciberseguridad – Participantes
<https://www.senatics.gov.py/application/files/2614/6316/2380/Participantes.pdf>

81 <http://www.pactoglobal.org.py/>





Por último, no existen antecedentes de que la compañía Copaco participe de los *Foros de Gobernanza de Internet* en Paraguay –en el año 2016 se realizó su tercera edición– ni evidencias que participe en el Foro a nivel mundial.

Por tanto no se otorga estrella alguna.



La ISP no cumple ninguno de los criterios.

Filtro/bloqueo de Contenidos en Internet
La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X) No
La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios (Y) Si

No existen evidencias de bloqueos de acceso de contenidos a Internet en años anteriores⁸² por parte de la compañía Copaco. Sin embargo es necesaria una política clara y accesible la posibilidad y condiciones de bloqueos o retiro de contenidos.

Por tanto se otorga media estrella en esta categoría.



La ISP cumple uno de los criterios.

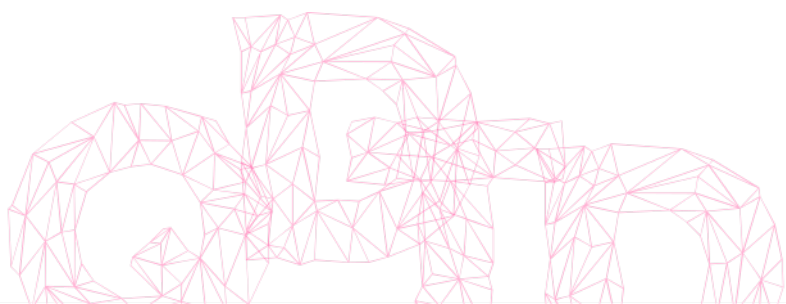
82 ABC.ME página de parodia del periódico ABC fue bloqueado por las ISP: Tigo y Personal <https://www.tedic.org/roben-este-post-neutralidad-en-la-red/>





A continuación se presenta el cuadro resumen de Copaco:

CÓMO PROTEGE TUS DATOS  COPACO S.A.		
1	Política de privacidad y protección de datos	☆
2	Autorización judicial	☆
3	Notificación	☆
4	Posicionamiento público en contra de la vigilancia masiva o sin control	☆
5	Transparencia	☆
6	Bloqueo de contenidos en Internet	☆



CHACO COMUNICACIONES (CHACONET)

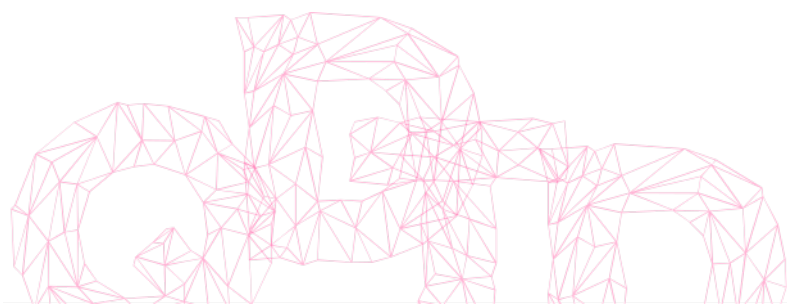
Política de privacidad y protección de datos
La compañía tiene una política de privacidad (X) No
La política de privacidad establece de manera precisa que información del usuario y sus comunicaciones es obtenida y almacenada (X) No
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados. (X) No
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades. (X) No
La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo. (X) No
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la compañía. (X) No

Para esta evaluación se analizó la página web oficial de la compañía ChacoNet. La política sobre *términos y condiciones* no se encuentran disponibles en acceso al público.

Por lo tanto, no cumple con el requisito de contar con una *política de privacidad*, ni los demás parámetros que se analizan sustantivamente en la política de privacidad.



La ISP no cumple ninguno o sólo se reúne uno de los criterios.





Información sobre la divulgación de datos a las autoridades gubernamentales

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa; (Y) si

La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa. (Y) si

La Constitución de la República es clara al exigir que las Instituciones de persecución penal deban obtener los datos de la comunicación bajo la característica exclusiva de *orden judicial previa*. No hay evidencias concretas que ChacoNet haya facilitado información sin cumplir el “*debido proceso*” expuestos en el *Código Procesal Penal* vigente.

Es indispensable que la compañía ChacoNet exprese públicamente su política de exigir la autorización judicial cuando le son solicitados los datos y *metadatos de las comunicaciones*. Por lo tanto se otorga una estrella.

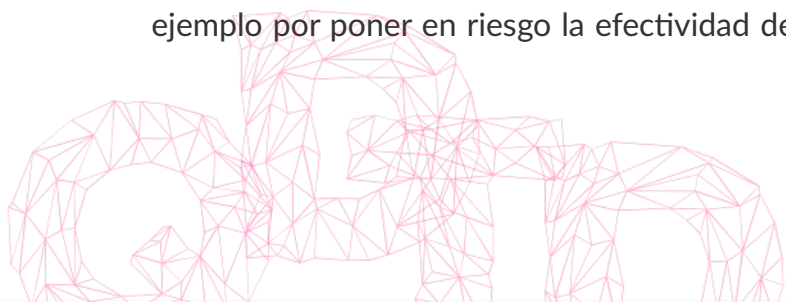


La ISP cumple con ambos criterios.

Notificación

La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible. (X) No

No se encontró que la compañía evaluada tenga una *política pública de notificación* a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia, por ejemplo por poner en riesgo la efectividad de una investigación, no se detectó una *política*





de *notificación* para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Tampoco se detectó que la compañía haya enfrentado judicialmente impedimentos de tipo legal para efectuar notificaciones, ni que haya promovido el establecimiento de mecanismos de notificación a usuarios ante el Congreso o CONATEL. Por lo tanto, no fue otorgada estrella alguna en esta categoría de evaluación.



La ISP no cumple ninguno de los criterios.

Informes de transparencias sobre las solicitudes de datos

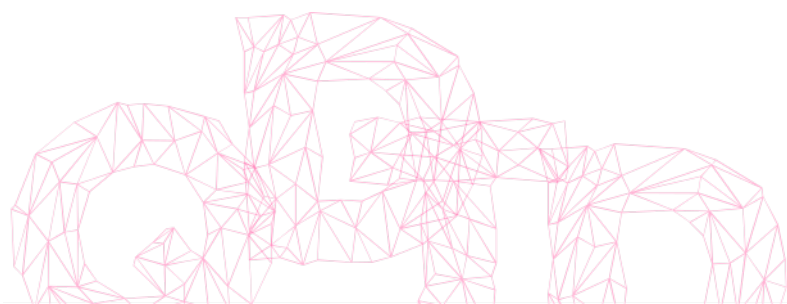
La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales; (X) No

La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos (si se trata de información de cuenta o de conexión de registros); (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental (presentación de pruebas en materia civil, penal, o los casos administrativos, etc.) (X) No

La compañía ChacoNet no publica un informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuarios y sus comunicaciones.



La ISP no cumple ninguno de los criterios.





Posicionamiento público en contra de la vigilancia masiva o sin controles

La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los DDHH en Internet (contribuciones realizadas por las asociaciones que la empresa puede ser la parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de “Obligación de Conservar tráficos de datos en Internet” o Proyecto de ley de “Protección de niños, niñas y adolescentes de contenidos nocivos en Internet” y el Plan de “Ciberseguridad en Paraguay”. (x) No

Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative o Telecommunications Industry Dialogue, Pacto Global (Global Compact) (x) No

La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISPs forman parte del grupo de Empresas, actor clave para el ecosistema de Internet. (X) No

La compañía ChacoNet no ha participado de mesas de trabajo de análisis legislativo sobre proyectos de ley, ni leyes vigentes que afectan Internet en Paraguay. No se encuentran evidencias públicas de que se haya posicionado en contra de proyectos que ponen en riesgo derechos fundamentales.

Sobre el segundo punto, no se observa que compañía forme parte de mecanismos para afrontar responsabilidad en materia de derechos humanos: no participa en el *Pacto Global*⁸³ capítulo Paraguay (*Global Compact*) ni otros espacios internacionales en donde se discuten estos temas.

Y por último, no existen antecedentes de que la compañía ChacoNet participe de los *Foros de Gobernanza de Internet* en Paraguay –en el año 2016 se realizó su tercera edición– ni evidencias que participe en el Foro a nivel mundial.

Por tanto no se otorga estrella alguna.



La ISP no cumple ninguno de los criterios.

83 <http://www.pactoglobal.org.py/>





Filtro/bloqueo de Contenidos en Internet

La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican. (X)no

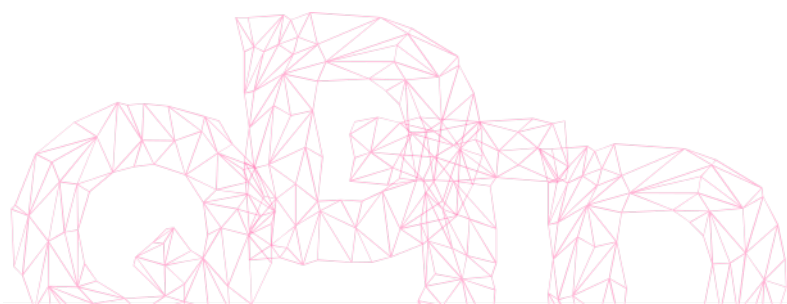
La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios (X) no

En la página oficial la compañía ChacoNet se ofrecen servicios de Internet con restricciones a las redes p2p. Además no cuenta con una la política clara y accesible sobre bloqueo o retiro de contenidos.

Por tanto no se otorga estrella en esta categoría.



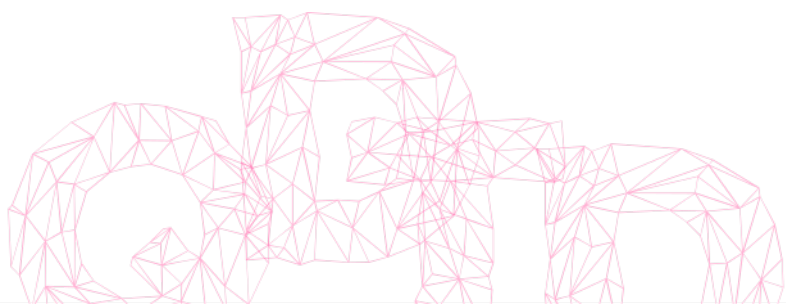
La ISP no cumple ninguno de los criterios.





A continuación se presenta el cuadro resumen de ChacoNet:

CÓMO PROTEGE TUS DATOS CHACONET		
1	Política de privacidad y protección de datos	☆
2	Autorización judicial	☆
3	Notificación	☆
4	Posicionamiento público en contra de la vigilancia masiva o sin control	☆
5	Transparencia	☆
6	Bloqueo de contenidos en Internet	☆



QUIEN DEFIENDE TUS DATOS

www.tedic.org



Este informe fue diagramado
con LibreOffice 5

