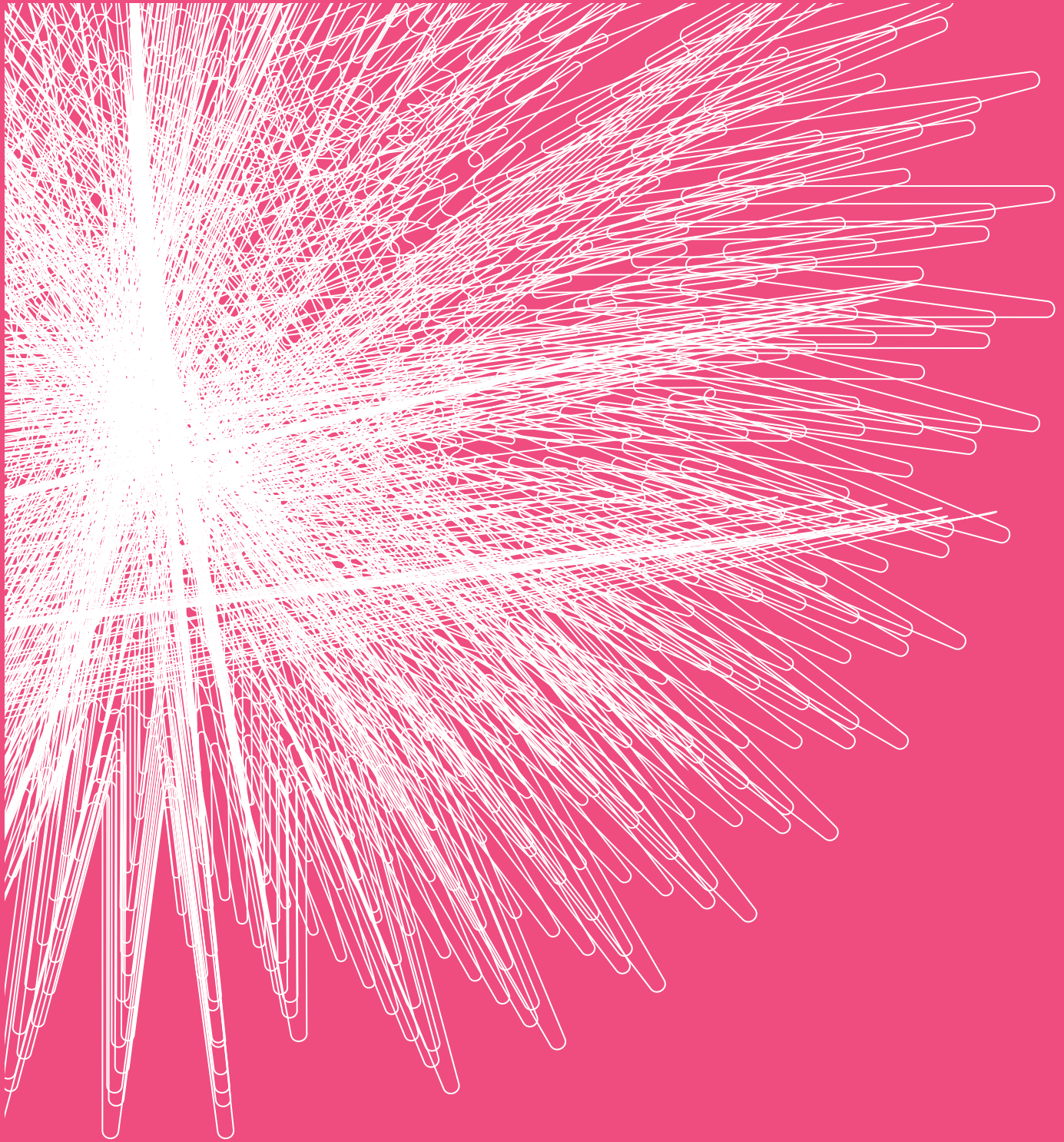


¿QUIÉN DEFIENDE TUS DATOS?

Paraguay 2024



¿QUIÉN DEFIENDE TUS DATOS?

Paraguay 2024

“¿Quién defiende tus datos?” tiene como objetivo promover la transparencia y las mejores prácticas en los ámbitos de la privacidad y la protección de datos por parte de las empresas que proporcionan acceso a Internet en Paraguay. Se lleva a cabo anualmente y cada nueva evaluación va precedida de un examen de la metodología, de modo que los resultados puedan reflejar con mayor precisión el marco jurídico existente, considerar las cuestiones que vayan surgiendo y abarcar las buenas prácticas en las esferas de la privacidad y la protección de los datos personales.



TEDIC es una organización sin fines de lucro que defiende y promueve los derechos humanos en entornos digitales al tiempo que avanza la tecnología con foco en desigualdades de género y sus intersecciones.

Electronic Frontier Foundation (EFF) es una organización internacional sin fines de lucro líder en la defensa de los derechos digitales. Trabaja con tecnólogos, activistas y abogados para defender la libertad de expresión en línea, combatir la vigilancia ilegal y abogar por las personas usuarias y la innovación.

¿QUIÉN DEFIENDE TUS DATOS? Paraguay 2024

ENERO 2025

INVESTIGACIÓN

Antonia Bogado
Maricarmen Sequera

COORDINACIÓN

Maricarmen Sequera

ELABORACIÓN Y REVISIÓN

Veridiana Alimonti (EFF)

DISEÑO Y DIAGRAMACIÓN

Horacio Oteiza

COMUNICACIÓN

Araceli Ramírez

Consultá esta investigación en:

<https://qtdt.tedic.org>



Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0) <https://creativecommons.org/licenses/by-sa/4.0/deed.es>
Esta licencia permite distribuir, remezclar, retocar, y crear a partir de esta obra incluso de modo comercial, siempre y cuando se de crédito y se licencien nuevas creaciones bajo las mismas condiciones.

TABLA DE CONTENIDO

INTRODUCCIÓN	6
CUADRO GENERAL COMPARATIVO	8
METODOLOGÍA	9
CONTEXTO NACIONAL	10
CRITERIOS DE EVALUACIÓN	21
REPORTE POR CADA ISP	30
REPORTE POR EMPRESA SOBRE LA POLÍTICA DE PRIVACIDAD Y DATOS PERSONALES	31
CLARO – AMX PARAGUAY S.A	31
COPACO S.A. - COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	33
PERSONAL - NÚCLEO S.A.	35
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	37
VOX - HOLA PARAGUAY S.A.	40
REPORTE - AUTORIZACIÓN JUDICIAL	42
CLARO - AMX PARAGUAY S.A.	42
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	44
PERSONAL - NÚCLEO S.A.	45
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	46
VOX - HOLA PARAGUAY S.A.	48
REPORTE - NOTIFICACIÓN A LA PERSONA USUARIA	50
CLARO - AMX PARAGUAY S.A.	50
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A	51
PERSONAL - NÚCLEO S.A.	52
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	53
VOX - HOLA PARAGUAY S.A.	54
REPORTE - POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS	56
CLARO - AMX PARAGUAY S.A.	56
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	58
PERSONAL - NÚCLEO S.A.	59
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	60
VOX - HOLA PARAGUAY S.A.	62
REPORTE - TRANSPARENCIA	64
CLARO - AMX PARAGUAY S.A.	64
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	66
PERSONAL - NÚCLEO S.A.	67
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	68
VOX - HOLA PARAGUAY S.A.	69

REPORTE - GUÍAS PARA LA SOLICITUD DE INFORMACIÓN PERSONAL	71
CLARO - AMX PARAGUAY S.A.	71
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	72
PERSONAL - NÚCLEO S.A.	73
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	74
VOX - HOLA PARAGUAY S.A.	75
REPORTE - ACCESIBILIDAD	77
CLARO - AMX PARAGUAY S.A.	77
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	79
PERSONAL - NÚCLEO S.A.	81
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	83
VOX - HOLA PARAGUAY S.A.	85
CONCLUSIÓN	87
RECOMENDACIONES	90

INTRODUCCIÓN

El proyecto “**Quién defiende tus datos**” está inspirado en la iniciativa “Who has your back” de la Electronic Frontier Foundation (EFF)¹, aunque la metodología aplicada para este estudio difiere de la utilizada en los Estados Unidos, ya que la realidad legal de Paraguay es notablemente distinta a la estadounidense.

En su cuarta edición, el proyecto evaluó a las mismas empresas de telefonía y servicios de Internet que se habían evaluado en las ediciones anteriores. Específicamente, se consideraron las empresas con un mercado superior a 15,000 clientes a nivel nacional, incluyendo a: COPACO², VOX³, PERSONAL⁴, TIGO⁵ y CLARO^{6,7}.

La investigación en el marco de este proyecto se centra en responder a las siguientes preguntas: ¿Cómo protegen nuestra privacidad las Proveedoras de Servicios de Internet (con su sigla en inglés ISP)? ¿De qué manera resguardan nuestros datos personales? ¿Existen procedimientos claros al respecto? ¿Participan activamente en la defensa de nuestros derechos en las mesas de debate público?

Diversos informes y resoluciones de las Naciones Unidas han enfatizado la importancia del acceso a Internet como instrumento indispensable para el ejercicio pleno de los derechos humanos, al mismo tiempo que contribuye a lograr mayores niveles de beneficios sociales e inclusión⁸⁹. En este contexto, la evaluación recurrente de la tecnología y las telecomunicaciones desde una perspectiva de derechos se vuelve esencial, ya que estas son fundamentales en nuestra actual forma de interacción y comunicación, desempeñando un papel crucial en garantizar el acceso equitativo a la información, la participación social y la conectividad global.

Desde la edición pasada, se realizó un pequeño ajuste que permite la comparación de criterios a nivel regional, modificación que se mantiene en esta investigación. Se ha incorporado una tabla de resultados para comparar el rendimiento de las empresas en las distintas categorías y criterios de evaluación de las cuatro ediciones de esta investigación (2017¹⁰, 2020¹¹, 2022¹² y 2024). Los cuales se basan en su

1 Web oficial de EFF: <https://www.eff.org>

2 COPACO <https://www.copaco.com.py>

3 Hola Paraguay - VOX <https://www.vox.com.py>. Comentarios de las autoras: Es importante destacar que, en 2020, VOX fue adquirida por COPACO. A lo largo de la investigación, se percibe que ambas empresas estatales manejan información similar y presentan un bajo nivel de cumplimiento con los criterios evaluados.

4 PERSONAL – NUCLEO <https://www.personal.com.py>

5 TIGO – TELECEL <https://www.tigo.com.py>

6 CLARO- AMX Paraguay. <https://www.claro.com.py>

7 No existen datos públicos de suscripción del ISP starlink hasta la fecha. Mas información sobre esta ISP en: <https://www.tedic.org/starlink-en-paraguay-existen-riesgos-o-preocupaciones-sobre-esta-tecnologia/>

8 Naciones Unidas. Consejo de Derechos Humanos. Resolución sobre Promoción y protección de derechos humanos en Internet. UN Doc. A/HRC/32/L.20. 27 de junio de 2016. Disponible para consulta en: <http://www.ohchr.org/EN/HRBodies/HRC/Pages/Documents.aspx>; Naciones Unidas. Asamblea General. Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. UN Doc. A/RES/70/125. 1 de febrero de 2016. Párr. 9. Disponible para consulta en: http://unctad.org/es/PublicationsLibrary/ares70d125_es.pdf.

9 Naciones Unidas (2011). Principios rectores sobre las empresas y los de derechos humanos. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

10 ¿Quién defiende tus datos? Edición 2017: <https://qtdt.tedic.org/imagenes/pdfs/QDTD-2017.pdf>

11 ¿Quién defiende tus datos? Edición 2020: <https://qtdt.tedic.org/imagenes/pdfs/QDTD-2020.pdf>






12 ¿Quién defiende tus datos? Edición 2022: https://qtdt.tedic.org/imagenes/pdfs/QDTD-2022_v2.pdf

compromiso público con el cumplimiento de la ley, la adopción de buenas prácticas favorables a las personas usuarias de servicio de Internet, la transparencia en sus prácticas y políticas, la accesibilidad en sus plataformas web, entre otros aspectos.

Cada empresa fue evaluada en base a las 7 categorías señaladas y justificadas en el apartado de criterios de evaluación, cuya elaboración tuvo en cuenta los requisitos del marco normativo vigente en Paraguay y las buenas prácticas internacionales en materia de protección de la privacidad y tratamiento de datos personales. Para esta evaluación, se analizaron los acuerdos de servicio, informes de sustentabilidad y otros documentos que estuvieron disponibles en los sitios web de las empresas hasta enero de 2024. También se evaluaron noticias de prensa y medios especializados en la materia.

Con los resultados preliminares en mano, TEDIC contactó con las empresas y solicitó revisión y comentarios sobre los mismos, con especial énfasis en las metodologías y resultados obtenidos hasta mayo de 2024. Finalmente, estos comentarios y opiniones de las empresas fueron ajustados en la conclusión y en los puntajes correspondientes.

CUADRO GENERAL COMPARATIVO

Cuadro general comparativo								
ISP	Criterios							Porcentaje de cumplimiento*
	Políticas de privacidad	Autorización judicial	Notificación a la persona usuaria	Políticas de promoción y defensa de los derechos humanos	Transparencia	Guías para requerimiento de información personal	Accesibilidad	
	★	★	★	★	★	★	★	55%
	★	★	★	★	★	★	★	14%
	★	★	★	★	★	★	★	41%
	★	★	★	★	★	★	★	73%
	★	★	★	★	★	★	★	5%

* El cálculo de porcentajes se realizó considerando el número total de criterios cumplidos por cada ISP en relación con el número total de criterios existentes (22 criterios en total) y los valores fueron redondeados al entero superior más cercano.

METODOLOGÍA

Esta investigación se centró en el análisis de las principales empresas de telefonía y proveedoras de Internet en Paraguay: Vox, Copaco, Personal, Tigo y Claro. Estas firmas proveen a sus usuarios servicios de Internet, telefonía, televisión y algunas de ellas también billeteras electrónicas, más conocidas como mobile financial services. Se eligió examinar específicamente a estas empresas entre un total de 231¹³ proveedoras de servicios de Internet en Paraguay, basándose en el criterio de que tengan un mercado superior a 15.000 clientes a nivel nacional. La información sobre la cantidad de personas usuarias por cada empresa fue obtenida del informe indicador de mercados publicado por la CONATEL en su página web¹⁴, actualizado hasta el año 2023.

Las entidades proveedoras de servicios de Internet recopilan datos de sus usuarios con fines comerciales y para cumplir con normativas legales, siendo responsables del tratamiento y uso de esta información. Partiendo de este contexto, la investigación se enfocó en analizar cualitativamente las políticas de privacidad y otros documentos relevantes de las empresas mencionadas. Dicho análisis se realizó dentro del marco de las siete categorías definidas en esta investigación. Las políticas de privacidad analizadas actúan como marcos orientadores para el tratamiento de la información recopilada sobre las personas usuarias. Estas políticas tienen como propósito informar a las personas usuarias sobre cómo se gestionan sus datos personales. En particular, detallan qué datos se recopilan, cómo se obtienen, su finalidad, los límites del tratamiento, los derechos de las personas usuarias y cómo pueden ejercerlos. Además, especifican con quiénes se comparten los datos y describen el proceso de compartición.

Los datos recolectados fueron extraídos de las políticas de privacidad enunciadas por cada empresa en su página web. No obstante, también se analizaron informes de sustentabilidad publicados durante los últimos 5 años. Estos informes fueron divulgados por Millicom International Cellular S.A.¹⁵ y por América Móvil¹⁶, empresas matrices de Tigo y Claro, respectivamente.

Asimismo, se analizaron noticias de prensa y se recolectaron datos de organismos sectoriales o multi-sectoriales que promuevan el respeto y la protección de los derechos humanos desde el ámbito empresarial, tales como Global Network Initiative¹⁷, la Telecommunications Industry Dialogue¹⁸ o GSMA¹⁹.

Después de analizar y contextualizar los datos recolectados, con la correspondiente justificación a los criterios expuestos, las empresas fueron puntuadas en cada una de las categorías que más adelante se enuncian.

13 CONATEL. Registro Nacional De Servicios De Telecomunicaciones. Listado de licenciatarios de Servicio De Internet Y Transmisión De Datos. Recuperado de https://www.conatel.gov.py/conatel/wp-content/uploads/2024/01/rnst_internet-tx-datos_5_ene-ro_2024.pdf

14 CONATEL. Indicadores de mercado. Periodo 2023. Recuperado de: <https://www.conatel.gov.py/conatel/indicadores/>

15 Millicom. Annual Report 2023. Recuperado de: <https://www.millicom.com/media/5769/ar-2023-w-mic-sa.pdf>

16 América Móvil. Informe de Sustentabilidad 2023. págs. 88-90. Recuperado de: <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

17 Global Network Initiative. Recuperado de <https://globalnetworkinitiative.org>

18 Telecommunications Industry Dialogue. Recuperado de www.telecomindustrydialogue.org

19 GSMA Membership. Recuperado de <https://www.gsma.com/membership/membership-types/operating-member-ship/>

CONTEXTO NACIONAL

1. ACCESO Y CONECTIVIDAD

Para abordar esta investigación y aplicar la metodología diseñada, así como comprender su enfoque y los resultados de este trabajo resulta fundamental contextualizarnos en la situación nacional.

Según el Instituto Nacional de Estadísticas (INE)²⁰ en el 2023, el 78,1% de la población utiliza Internet, de ese conjunto, el 76,9% (1.831.038) correspondía a hombres y 79,2% (1.985.009) a mujeres. Por su parte, según área de residencia, 83,8% (2.593.093) de la población urbana accedió a Internet en contraposición a 68,2% (1.222.954) de población rural.

En cuanto a los avances en índices de conectividad, cabe referir que, según el Plan Nacional de Telecomunicaciones Paraguay 2021-2025 (PNT 21-25)²¹, elaborado por la Comisión Nacional de Telecomunicaciones²² (CONATEL) en octubre de 2021, se han registrado importantes progresos en los últimos años. En el 2023, la penetración de Internet de banda ancha fija alcanzó el 14% por cada 100 habitantes, lo que representa un incremento del 4% respecto a 2022. Por otro lado, la penetración de Internet de banda ancha móvil fue del 84,4% en 2023, significativamente superior al 64,5% registrado en 2022. Si bien no se reporta un dato actualizado a la fecha del 2024, estos son de suma importancia para el contexto nacional, ya que reflejan la evolución de la conectividad en el país.

El PNT 21-25 también señala que las tecnologías de acceso predominantes en banda ancha fija por cable son actualmente las conexiones HFC, seguidas por las conexiones FTTX y finalmente las conexiones ADSL²³. Análisis que permite una comprensión más completa de la capacidad y eficiencia de la red en el país y podría contribuir a la formulación de estrategias y políticas para mejorar la conectividad y garantizar un acceso equitativo y eficiente a los servicios de telecomunicaciones en el ámbito nacional.

En las siguientes tablas se exponen los datos realizados por CONATEL²⁴ sobre banda ancha fija, móvil, cantidad de personas que acceden a Internet móvil, así como sus ingresos brutos.

20 Gobierno de Paraguay. (2024). Portal Unificado de Información Pública. Solicitud de información pública número 85665. <https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/85665>

21 Plan Nacional de Telecomunicaciones 2021-2025 (PNT 21-25). Recuperado de <https://www.conatel.gov.py/conatel/wp-content/uploads/2022/01/pnt21-25-1.pdf>

22 Ente regulador de las telecomunicaciones en Paraguay.

23 PNT 21-25, p. 35.

24 Gobierno de Paraguay. (2024). Portal Unificado de Información Pública. Solicitud de información pública número 85730. <https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/85730>

TABLA 1. Banda ancha fija y banda ancha móvil

PENETRACIÓN DE INTERNET BANDA ANCHA FIJA*

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1,4%	1,8%	2,0%	2,3%	2,7%	3,1%	3,6%	4,0%	4,8%	5,3%	7,8%	9,9%	10%	14%

* Suscripciones a banda ancha fija / población x 100

PENETRACIÓN DE INTERNET BANDA ANCHA MÓVIL**

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1,4%	1,8%	2,0%	2,3%	2,7%	3,1%	3,6%	4,0%	4,8%	5,3%	7,8%	9,9%	10%	14%

** Suscripciones a banda ancha móvil / población x 100

Fuente: COPACO (2024).

TABLA 2. Personas usuarias de Internet móvil

PRESTADORA DE SERVICIOS	TECNOLOGÍA DE ACCESO MÓVIL	DIC-19	DIC-20	DIC-21	DIC-22	JUN-23	DIC-23
TELECEL S.A.	SMARTPHONE - 3G	600.123	438.675	337.776	260.725	230.461	195.627
	FEATURE PHONE - 3G	73.744	25.653	26.599	18.887		
	MODEM / DATACARD - 3G	14.195	2.199	1.437	828		
	MODEM / TABLET - 3G	2.962	2.054	1.118	764	930	785
	SMARTPHONE - 4G	1.405.764	1.826.795	2.141.687	2.354.176	2.311.423	2.471.414
	FEATURE PHONE - 4G	57.355	33	26	24		
	MODEM / DATACARD - 4G	4.211	4.922	4.533	5.199		
	MODEM / TABLET - 4G	1.268	2.656	3.635	3.871	4.676	4.922
	FEATUREPHONES (GPRS)					111.463	108.029
	TABLETAS 2G					387	413
	SMARTPHONE - 2G					7.251	10.571
	Otros (Dongles)					81.915	85.489
	TOTAL TELECEL S.A.		2.159.622	2.302.987	2.516.811	2.644.474	2.748.506
NÚCLEO S.A.	SMARTPHONES 4G/LTE	1.091.384	1.163.490	1.263.514	1.272.778	1.289.574	1.323.861
	SMARTPHONES 3G	157.471	89.052	51.014	32.496	25.622	20.910
	TABLETS 4G	1.338	1.851	3.007	3.235	3.476	3.273
	TABLETS 3G	2.262	1.468	835	535	450	362
	Featurephones (GPRS)						23.039
	Otros (Dongles)						113.552
	TOTAL NÚCLEO S.A.	1.252.455	1.255.861	1.318.370	1.309.044	1.319.122	1.484.997
AMX PARAGUAY S.A.	SMARTPHONES 4G/LTE	765.988	828.217	811.335	842.469	9.612	882.987
	SMARTPHONES 3G	75.128	45.026	22.412	11.784	839.153	6.856
	TABLETS 4G	505	2.178	2.809	2.798	243	2.910
	TABLETS 3G	13	2.121	301	191	2.723	136
	TOTAL AMX PY S.A.	841.634	877.542	836.857	857.242	851.731	892.889
HOLA PARAGUAY S.A.	3G	42.994	-	-	-	16.580	16.524
	4G	17.029	-	-	-	570	564
	TOTAL HOLA PARAGUAY S.A.*	60.023	-	-	-	17.150	17.088

* Estimado en base a la evolución del año 2018

TOTAL GENERAL Smartphones+Tablets	4.313.734	4.436.390	4.672.038	4.810.760	4.936.509	5.272.224
--	------------------	------------------	------------------	------------------	------------------	------------------

Fuente: CONATEL (2024).

TABLA 3. Ingresos brutos

CATEGORÍA	2019	2020	2021	2022	2023
TELEFONÍA FIJA	₡ 237.477.501.909	₡ 184.099.712.051	₡ 159.548.131.244	₡ 107.846.752.601	₡ 18.609.789.900
TELEFONÍA MÓVIL (incluye Internet móvil 3G)	₡ 2.347.175.260.029	₡ 2.077.073.263.425	₡ 1.956.472.685.933	₡ 1.902.909.356.836	₡ 1.988.262.795.800
INTERNET MÓVIL 4G/LTE	₡ 1.207.241.636.012	₡ 1.118.258.524.407	₡ 1.300.359.257.326	₡ 1.500.443.071.163	₡ 1.645.006.517.200
INTERNET FIJO	₡ 1.239.386.495.561	₡ 1.297.025.979.759	₡ 1.512.569.906.432	₡ 1.612.103.123.142	₡ 1.498.272.574.100
CABLE DISTRIBUCIÓN (Tv cable)	₡ 511.660.035.132	₡ 452.179.640.357	₡ 314.142.490.807	₡ 281.169.221.990	₡ 509.154.125.500
DATDH (TV Satelital)	₡ 597.373.795.592	₡ 584.569.359.761	₡ 570.789.818.816	₡ 549.186.605.732	₡ 506.550.488.100
RADIO DISTRIBUCIÓN (TV UHF de pago)	₡ 60.776.659.113	₡ 13.194.487.406	₡ 1.977.716.000		---
Total Tv Paga	₡ 1.169.810.489.837	₡ 1.049.943.487.524	₡ 886.910.025.623	₡ 830.355.827.722	₡ 1.015.704.613.600

Fuente: CONATEL (2024).

Cabe destacar que el Ministerio de Tecnología de la Información y Comunicación (MITIC) en el 2022 diseñó un Plan Nacional TIC 2022-2030 (PNTIC)²⁵ de Paraguay por el cual propone una transformación digital ambiciosa para un acceso a Internet plena para toda la población, así como la elaboración de marcos regulatorios para otras tecnologías. Sin embargo su implementación enfrenta aún ciertas limitaciones²⁶.

En indicadores internacionales se destaca que Paraguay ocupa el nivel 3 (puntaje entre 55 y 85) en el Índice Mundial de Ciberseguridad 2024 elaborado por la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés).²⁷

Con relación a los indicadores de brecha digital de género, las diferencias en el acceso y uso de dispositivos digitales, Internet y otras tecnologías son prácticamente imperceptibles²⁸. Según los datos de la tabla N° 1, tanto el indicador de uso de Internet (UIT) como el de acceso móvil combinado y la brecha de género (GSMA) alcanzan un valor de 1, lo que refleja un alto nivel de igualdad entre hombres y mujeres en el ámbito tecnológico. Además, los demás indicadores también se ubican, en su mayoría, en niveles sobresalientes.

25 MITIC (2022). Plan Nacional de Tecnologías de la Información y la Comunicación 2022-2030: Recuperado de: <https://mitic.gov.py/plan-nacional-de-tic-2022-2030/>

26 El PNTIC incluye la necesidad de sanciones, mecanismos de reparación y evaluaciones basadas en estándares de derechos humanos, pero carece de detalles sobre cómo se llevarán a cabo estas medidas y quién será responsable de supervisarlas. La falta de acciones concretas y claridad en la ejecución genera dudas sobre la capacidad del país para abordar los desafíos tecnológicos, proteger los derechos de las personas y mantener su competitividad digital. Un enfoque más coordinado y estructurado sería clave para garantizar una adopción ética y efectiva de las TIC y reducir las desigualdades.

27 International Telecommunication Union (2024). *Global Cybersecurity index 2024. 5th Edición*. ISBN 978-92-61-38751-8 (Electronic version). https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

28 World Economic Forum. 2024. Global Gender Gap. <https://www.weforum.org/publications/global-gender-gap-report-2024/> En el año 2024, Paraguay obtuvo una puntuación de 0.707 en el Índice Global de Brecha de Género. Este índice, que evalúa la paridad en 146 países, mide el progreso hacia la igualdad de género a través de diversas dimensiones: participación económica y oportunidades, logros educativos, salud, y empoderamiento político.

TABLA 4. Brecha de género digital

INDICADOR	ÍNDICE
Brecha de género - Internet – Online	0,984
Brecha de género - Internet – Offline	0,868
Brecha de género - Internet – Combinado	0,978
Brecha de género - Internet – UIT	1
Brecha de género - Móvil – Online	0,999
Brecha de género - Móvil – Offline	0,94
Brecha de género - Móvil – combinado	1
Brecha de género – GSMA	1

Fuente: World Economic Forum (2024).²⁹

Como se puede observar CONATEL, MITIC y el INE tienen el desafío de realizar estudios actualizados de conectividad para que las políticas de acceso y conectividad tengan coherencia con relación a las necesidades y los derechos de las personas usuarias. Estos estudios son esenciales para identificar brechas reales de acceso y uso de las tecnologías digitales, así como para comprender las demandas específicas de los diversos sectores de la población.

2. CONTEXTO NORMATIVO

Para este estudio, es fundamental realizar un análisis breve pero sustancial de las leyes relacionadas con la privacidad y la protección de datos personales de las personas usuarias de servicios de Internet. Este análisis también debe incluir las regulaciones específicas sobre telecomunicaciones y otros instrumentos legales pertinentes que influyen directamente en la gestión y tratamiento de la información de las personas usuarias. Estos marcos normativos establecen las obligaciones de los proveedores de servicios y los derechos de las personas usuarias, proporcionando el contexto legal en el que se desarrolla esta investigación

2.1. Marco legal internacional

En el marco legal internacional vigente aprobado y ratificado por el Paraguay, instrumentos como la Declaración Universal de los Derechos Humanos³⁰ y la Convención Americana de Derechos Humanos³¹, protegen el derecho a la privacidad y la inviolabilidad de las comunicaciones. La jurisprudencia de la Corte Interamericana de Derechos Humanos (CIDH) ha reforzado estas protecciones, estableciendo precedentes relevantes para los Estados parte, incluido Paraguay, en relación con la protección de la privacidad y la vigilancia estatal, como los citados a continuación:

29 Digital Gender Gaps. (2024). Brecha de género en el acceso a Internet de la UIT y combinada. <https://www.digitalgendergaps.org/>

30 Naciones Unidas, Declaración Universal de Derechos Humanos. Recuperado de https://paraguay.un.org/sites/default/files/2020-01/declaracion_universal_de_derechos_humanos_-_version_castellano.pdf

31 Ley Nº 1/1992, que aprueba y ratifica La Convención Americana Sobre Derechos Humanos O Pacto De San José De Costa Rica. <https://www.bacn.gov.py/leyes-paraguayas/2619/aprueba-y-ratifica-la-convencion-americana-sobre-derechos-humanos-o-pacto-de-san-jose-de-costa-rica>

Caso Escher vs Brasil (2009)

Este caso resuelto por la Corte Interamericana de los Derechos Humanos (CIDH) en 2009³², examinó las violaciones de derechos humanos cometidas durante interceptaciones telefónicas realizadas a miembros de las organizaciones Coana y Adecon en Paraná entre mayo y junio de 1999. Aunque las grabaciones fueron autorizadas judicialmente, carecían de fundamentos adecuados, se extendieron más allá del plazo permitido y fueron filtradas a medios de comunicación.

La Corte condenó a Brasil por violar los derechos a la intimidad, la libertad de asociación y las garantías judiciales, ordenando indemnizaciones, investigaciones y la publicación de la sentencia. El Estado pagó 22.000 dólares a cada víctima y cumplió parcialmente con las disposiciones, pero no responsabilizó a nadie debido a la prescripción de los hechos. Finalmente, la Corte archivó el caso, siendo este el único de Brasil considerado cumplido.

En esa sentencia se destaca por primera vez que la Convención Americana protege no sólo el contenido de las comunicaciones, sino también cualquier información relacionada, como el origen, la duración y la hora de la comunicación. La Corte dejó claro en esta sentencia que tanto el contenido como los metadatos están protegidos por las leyes interamericanas de derechos humanos:

114. Como esta Corte ha señalado anteriormente, aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación incluida dentro del ámbito de protección de la vida privada. El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación.

32 CIDH (2009) Sentencia 6 de julio de 2009. Caso Escher y otros contra Brasil. Versión completa: https://corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf

Caso Restrepo (CAJAR) vs Colombia (2023)

La Corte emitió una sentencia histórica contra Colombia, declarando al Estado responsable de una campaña de vigilancia, acoso y persecución de miembros del Colectivo de Abogados “José Alvear Restrepo” (CAJAR) durante más de dos décadas^{33,34}. Estas acciones, que incluyeron amenazas y hostigamiento, violaron derechos fundamentales como la vida, la integridad personal, la privacidad, la libertad de expresión y de asociación, afectando especialmente a las defensoras y a quienes se vieron obligados a exiliarse.

La decisión marca un precedente al ser la primera en declarar a un Estado responsable por violar el derecho a defender derechos humanos. Además, destacó la necesidad de supervisión independiente de los servicios de inteligencia, límites claros en sus facultades y estándares estrictos para el manejo y protección de datos personales.

El tribunal subrayó que el marco jurídico colombiano no impidió prácticas abusivas de vigilancia contra el CAJAR y otros defensores de derechos humanos, incluso tras reformas legales. La sentencia avanza en la protección de la privacidad, la libertad de expresión y la autodeterminación informativa bajo la Convención Americana sobre Derechos Humanos, sentando estándares clave para las actividades de inteligencia en la región.

La Corte destacó que prácticas como la vigilancia encubierta, la interceptación de comunicaciones y la recopilación de datos personales constituyen una seria injerencia en los derechos humanos. Estas acciones requieren normativas claras y controles efectivos para prevenir abusos. Citando la jurisprudencia europea, subrayó que incluso la existencia de leyes que permitan vigilancia secreta representa una amenaza para la libertad de comunicación.

La Corte reafirmó que la vigilancia debe estar sujeta a autorización judicial previa, incluyendo límites estrictos en alcance, tiempo y método. Esto aplica tanto a la recolección de información personal de empresas privadas como al uso de técnicas para acceder a bases de datos no públicas, rastrear usuarios en línea o localizar dispositivos electrónicos. También abarca el acceso a metadatos sensibles, como correos electrónicos, ubicaciones GPS, direcciones IP y datos de aplicaciones.

Sin embargo, la Corte no diferenció claramente entre vigilancia selectiva y masiva, perdiendo la oportunidad de condenar explícitamente esta última, lo que deja margen para interpretaciones ambiguas sobre estas prácticas.

La Corte reconoció la autodeterminación informativa como un derecho humano autónomo, garantizado por la Convención Americana. Este derecho permite a las personas decidir cuándo y cómo revelar aspectos de su vida privada, incluyendo el control sobre sus datos personales.

33 CIDH (2024) Resumen oficial emitido por la Corte Interamericana.
https://corteidh.or.cr/docs/casos/articulos/resumen_506_esp.pdf

34 CIDH (2024) Sentencia 18 de octubre de 2023. Caso miembros de la corporación colectivo de abogados “José Alvear Restrepo” vs Colombia. Versión completa: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

El tribunal señaló que la autodeterminación informativa incluye varios componentes clave: el derecho a conocer qué datos se recopilan, su origen, uso, tiempo de conservación y posible transferencia; el derecho a corregir, actualizar o eliminar datos inexactos; el derecho a oponerse a su tratamiento; y el derecho a la portabilidad de los datos. Además, cualquier restricción a este derecho debe estar justificada, limitada en el tiempo y cumplir con principios de necesidad y proporcionalidad, excluyendo justificaciones genéricas como la seguridad nacional.

El tribunal concluyó que Colombia violó este derecho al restringir arbitrariamente el acceso y control de los miembros del CAJAR sobre sus datos personales en los archivos de inteligencia. Rechazó que la pertenencia de documentos a organismos de inteligencia sea suficiente para clasificarlos como reservados, exigiendo que las restricciones se basen en su contenido específico³⁵.

Ambas sentencias subrayan la importancia de proteger los derechos humanos, asegurar la protección de la privacidad y limitar la vigilancia estatal para prevenir abusos. Paraguay³⁶, al igual que muchas legislaciones de la región de América Latina protegen menos los metadatos que el contenido. Sin embargo, con estos casos, y bajo el principio de convencionalidad, el Estado paraguayo debe implementar medidas para evitar la vigilancia masiva y desproporcionada, garantizar la protección de datos personales, ofrecer garantías judiciales para que las personas, en especial los defensores de derechos humanos puedan desempeñar su labor sin temor a represalias o interferencias arbitrarias.

2.2. Marco legal nacional

Además del marco legal internacional vigente mencionado anteriormente, la Constitución de la República del Paraguay establece disposiciones específicas para proteger la privacidad documental e intrínseca de las personas frente a terceros y frente a la autoridad, salvo cuando se vea comprometido el orden público. Entre estas disposiciones destacan el Derecho a la Intimidad (artículo 33) y el Derecho a la Inviolabilidad del Patrimonio Documental y la Información Privada (artículo 36). Este último adquiere especial relevancia al analizarlo en el contexto del Criterio de Evaluación Nº 2: Autorización Judicial.

La Constitución Nacional también reconoce el Hábeas Data (artículo 135) como garantía constitucional, asegurando a las personas el derecho a acceder, rectificar, solicitar la cancelación u oponerse al tratamiento de sus datos, entre otros, siendo estas disposiciones complementarias esenciales para la protección de datos personales en el país.

Es importante destacar que, según el artículo 45 de la propia Constitución, la falta de regulación legal no puede ser invocada para negar ni menoscabar derechos o garantías inherentes a la personalidad humana que no estén expresamente enunciados. Esto cobra particular relevancia en Paraguay, donde aún no se cuenta con una ley general de protección de datos personales. Si bien, en mayo de 2021, se presentó un proyecto de ley en Paraguay conocido como la Ley de Protección de Datos Personales³⁷, que busca establecer un marco integral para la regulación del manejo de datos y el mismo fue reciente-

35 EFF (2024). En victoria histórica para los derechos humanos en Colombia, la Corte Interamericana declara que organismos estatales violaron derechos humanos de abogados que defendían a activistas. <https://www.eff.org/deeplinks/2024/04/historic-victory-human-rights-colombia-inter-american-court-finds-state-agencies?language=es>

36 En Paraguay, el principio de convencionalidad tiene implicaciones significativas debido a que el país es parte de la CADH desde 1989 y ha aceptado la jurisdicción de la Corte IDH. El país ha sido condenado por la Corte IDH en varios casos, como el de la Comunidad Indígena Yakye Axa y otros relacionados con violaciones de derechos de comunidades indígenas y derechos laborales. Estas sentencias han llevado a reformas legales y políticas públicas para alinear el marco normativo paraguayo con los estándares internacionales. Versión completa de la sentencia: https://corteidh.or.cr/docs/casos/articulos/seriec_125_esp.pdf

37 Para más información, visitar la página de la Coalición de Datos Personales: <https://www.datospersonales.org.py>, y el Sistema de Información Legislativa del Paraguay: <https://silpy.congreso.gov.py/web/expediente/123459>

mente aprobado en general por la Cámara de Diputados, su estudio en detalle ha sido postergado hasta 2025, dejando al país, por el momento, sin una legislación específica en esta materia.

La regulación actual más directa al respecto es la Ley Nº 6.534/2020 de Protección de Datos Personales Crediticios. Esta ley, que deroga la anterior Ley Nº 1.682/2001 y sus modificaciones³⁸, establece un nuevo marco para la protección de datos e información personal en Paraguay, poniendo más énfasis en tratar los aspectos vinculados a la información crediticia de toda persona, cualquiera sea su nacionalidad, residencia o domicilio, en entidades bancarias, financieras, burós de créditos. Si bien esta ley es sectorial, prevé definiciones relevantes en la materia como la de datos personales y datos personales sensibles, y complementa otras leyes y disposiciones dentro del marco normativo nacional.

En el contexto normativo mencionado, es importante destacar la Resolución Nº 3/2023 del Banco Central del Paraguay y la Resolución Nº 1502/2022 de la Secretaría de Defensa al Consumidor, que reglamentan y suman a la Ley de Protección de Datos Personales Crediticios, en carácter de autoridades de aplicación. Estas normativas no solo definen los procedimientos aplicables a estos entes regulados por la ley, sino también los mecanismos para garantizar los derechos de los titulares de datos. Su importancia radica en que las ISP, al incluir la verificación de la capacidad crediticia en sus contratos de prestación de servicios de Internet, deben cumplir con los estándares establecidos por la legislación vigente sobre el tratamiento de la información y teniendo en cuenta la naturaleza de estos contratos.

Asimismo, en concordancia con las disposiciones constitucionales mencionadas, cabe citar a la Ley 642/95 “De telecomunicaciones”, la cual también garantiza la inviolabilidad del secreto de la correspondencia y del patrimonio documental, salvo por orden judicial (Artículo 89). Esta disposición es aplicable tanto al personal de telecomunicaciones como a cualquier persona o usuario que tenga conocimiento de la existencia o contenido de dichas comunicaciones. Además, la normativa precisa que la inviolabilidad implica la prohibición de abrir, sustraer, interferir, cambiar texto, desviar curso, publicar, usar, tratar de conocer o facilitar a una persona ajena al destinatario tener conocimiento de la existencia o contenido de las comunicaciones confiadas a prestadores de servicios, así como dar ocasión para cometer tales actos (Artículo 90).

En igual sentido, debemos considerar la Ley Nº 4.868/2.013 de Comercio Electrónico; y sus disposiciones complementarias, al igual que la Ley Nº 6.822/2.021 De los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos y sus disposiciones complementarias. Según la Ley Nº 6.738/2021 que regula el teletrabajo en relación de dependencia, estas normativas tienen un alcance limitado y no abordan de manera integral la protección de datos en el país.

La Ley de Comercio Electrónico, en su artículo 9, establece que las ISP deben cumplir ciertas obligaciones adicionales, además de las normas vigentes sobre Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente. Estas obligaciones incluyen informar de manera permanente, fácil, directa y gratuita a sus clientes sobre diferentes herramientas técnicas que mejoren la seguridad de la información, como protección contra virus informáticos y programas espía, y la res-

38 Esta ley derogó a la Ley Nº 1682/2001 y sus modificaciones (Ley Nº 1969/2002 y Ley Nº 5543/2015) por el cual se ofrecía una regulación parcial sobre la información privada, aunque con limitaciones. Actualmente esta derogación ha dejado un vacío en la normativa actual.

tricción de correos electrónicos no solicitados. También deben informar sobre las herramientas disponibles para filtrar y restringir el acceso a contenidos y servicios no deseados en Internet o perjudiciales para la niñez y la adolescencia. La ISP puede cumplir con esta obligación de información si incluye la información requerida en su página principal de Internet.

En la misma línea, el Decreto Reglamentario Nº 1.165/14 de la Ley de Comercio Electrónico, en su artículo 11, establece el Deber de Informar y Protección de Datos, indicando que el proveedor de bienes y servicios por vía electrónica a distancia está obligado a informar al consumidor o usuario sobre la finalidad y tratamiento de sus datos personales, de acuerdo con la legislación vigente en la materia. Además, debe comunicar quién recibirá los datos proporcionados y quién será responsable de la custodia o almacenamiento de la información suministrada. Asimismo, se le exige utilizar sistemas seguros para prevenir la pérdida, alteración y acceso no autorizado por parte de terceros a los datos proporcionados por el consumidor o usuario.

En vista a que aún no existe una Ley Integral de Protección de Datos Personales, se identifican igualmente esfuerzos fragmentados para una protección proactiva en algunas instituciones del Estado. Por ejemplo, la Resolución MITIC Nº 733/2019 establece un modelo de gobernanza de seguridad de la información para mejorar la ciberseguridad y la gestión de riesgos en el sector público.

Adicionalmente, normativas como el Decreto Nº 8709/2018, que regula el Sistema de Intercambio de Información (SII), incluyen principios clave como la limitación de la finalidad, la minimización de datos y los derechos ARCO (acceso, restricción, cancelación y oposición). Este sistema maneja tanto datos públicos como privados, diferenciándose de los datos abiertos, que solo abarcan información pública gubernamental.

Por otro lado, el Decreto Nº 4845/2021, que reglamenta la Ley Nº 6562/2020 sobre la reducción del uso de papel en la administración pública, establece disposiciones para garantizar la trazabilidad y protección de datos personales, permitiendo su acceso únicamente para trámites específicos y bajo la supervisión de funcionarios responsables. Aunque estas normativas ofrecen lineamientos útiles, no constituyen un marco general para la protección integral de datos en el país.

En relación con el marco normativo penal, el Código Procesal Penal establece en su artículo 200 que la intervención de comunicaciones requiere una resolución fundada del juez, cualquiera sea el medio técnico utilizado para conocerlas. El resultado de la intervención debe ser entregada únicamente al Juez que la ordenó, quien podrá requerir la versión escrita de la grabación y ordenar la destrucción de toda la grabación o de aquellas partes que no guarden relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. El mismo cuerpo normativo, en su artículo 228, otorga al juez y al Ministerio Público la facultad de requerir informes a personas o entidades públicas o privadas. Estos informes pueden solicitarse de forma verbal o escrita, detallando el procedimiento, el nombre del imputado, el lugar de entrega del informe, el plazo para su presentación y las consecuencias por incumplimiento.

Estas normas subrayan la excepcionalidad de la intervención de comunicaciones y la protección de éstas contra la divulgación de su contenido, en consonancia con las disposiciones internacionales y constitucionales que garantizan un enfoque garantista en la legislación penal. Por su parte, aunque no es vinculante, la jurisprudencia reciente también destaca la importancia de la orden judicial como requisito para la legalidad de la intervención, asegurando la salvaguarda de la garantía constitucional de la inviolabilidad de la comunicación privada³⁹.

Igualmente, cabe mencionar que los contratos para la adquisición de servicios de Internet se encuentran en la categoría de contratos de consumo, por lo que están amparados por la Ley Nº 1.334/1998 De Defensa del Consumidor y Del Usuario, y sus modificaciones. Esta legislación protege a los consumidores frente a cláusulas establecidas unilateralmente por el proveedor, sin posibilidad de modificación por parte del consumidor. En este contexto, la misma resulta relevante al evaluar cómo las ISP protegen los derechos de los usuarios y considerar aspectos como la transparencia en las prácticas comerciales, la resolución de reclamos o disputas y los derechos de acceso a la información.

Por su parte se encuentra la Resolución de CONATEL Nº 2583/2024⁴⁰ que establece la obligatoriedad para todos los licenciatarios del servicio de acceso a Internet y transmisión de datos de conservar los registros de conexión. Esta resolución busca registrar los tráficos de datos tales como la dirección de IP (fecha y hora de asignación y liberación de la dirección), en caso de NAT (Network Address Translation) la correspondiente entre las direcciones privadas y pública, así como su almacenamiento obligatorio de hasta 6 meses como periodo mínimo, y habrá sanciones graves aplicadas en el caso que la ISP no colabore. Sin embargo, la resolución no especifica qué autoridades están facultadas para solicitar y tratar estos datos, ni los procedimientos legales necesarios, como la obtención de una orden judicial, para garantizar el respeto al principio del debido proceso. Este vacío regulatorio plantea preocupaciones sobre posibles vulneraciones a los derechos de privacidad y la protección de los datos personales.

La jurisprudencia nacional también ha abordado casos significativos en el ámbito de la protección de datos personales, estableciendo valiosos precedentes. Un caso relevante es el litigio presentado ante la Sala Civil de la Corte Suprema de Justicia⁴¹, donde una persona demandó a una entidad financiera por la divulgación no autorizada de sus datos financieros y crediticios. Este caso adquiere importancia al examinar los contratos de servicios entre ISP y personas usuarias, ya que dichos contratos suelen ser estandarizados, con cláusulas similares a las del caso mencionado. La resolución destaca la importancia de la Ley de Defensa del Consumidor, que exige que las cláusulas en estos contratos sean explícitas y detalladas, especialmente aquellas relacionadas con la cesión de datos.

En relación con el criterio de privacidad y protección de datos personales, especialmente en cuanto al almacenamiento, ubicación y eliminación de los datos, destaca el pionero fallo del Tribunal de Apelaciones en lo Civil y Comercial, Tercera Sala de la Capital⁴². Este aborda el concepto del derecho al olvido y distingue su alcance del derecho a la protección de datos personales. Subraya que este derecho no se limita únicamente a proteger la privacidad, sino que aborda el riesgo real de la creación y manipulación

39 CSJ, Sala Penal, Acuerdo y Sentencia Nº 777 del 30 de noviembre de 2022, opinión del ministro Manuel Ramírez Candia.

40 CONATEL (2024). Resolución directorio Nº 2583/2024. Recuperado de <https://www.conatel.gov.py/conatel/resolucion-directorio-n-2583-2024/>

41 J.D.B. c. Banco Itaú s/ Indemnización de Daños y Perjuicios (Ac. y Sent. Nº 89/2021)

42 R., L. G. y E. A., N. G. c. ABC Color y Ultima Hora s/ Hábeas Data (Ac. y Sent. Nº 152) (PY/JUR/448/2021).

de perfiles detallados, que podrían ser utilizados por terceros, especialmente organizaciones con diversos intereses. Además, destaca la conexión entre la temporalidad de los datos y la autodeterminación informativa, definiéndose como variantes del derecho a la privacidad adaptadas a la sociedad de la información. En esencia, el derecho al olvido busca evitar la difusión indiscriminada de datos personales e información en Internet cuando su publicación carece de relevancia o interés público.

La adopción de estándares más elevados por parte de las empresas analizadas, que van más allá de los requisitos de la normativa nacional y a menudo se alinean con las prácticas de sus pares internacionales, como la publicación de informes de transparencia y políticas de privacidad, se destaca como una buena práctica que refleja su compromiso con la transparencia. En cuanto a su participación en el debate público, cuatro de las cinco empresas ISP estudiadas (TELECEL S.A., NÚCLEO S.A., AMX PARAGUAY S.A. y COPACO S.A.) estuvieron involucradas en la aprobación del reglamento de protección al usuario de telecomunicaciones junto a la autoridad competente, CONATEL⁴³. Sin embargo, hasta el momento, no han emitido dictámenes ni se han involucrado en iniciativas para fortalecer el marco normativo sobre protección de datos personales, indicando la necesidad de un mayor involucramiento en temas de privacidad y protección de datos.

En suma, la legislación, la participación pública y las normativas específicas en Paraguay influyen en cómo las empresas de telecomunicaciones gestionan entre otros aspectos, la privacidad y protección de datos de sus usuarios y usuarias. Esta comprensión contextual es importante para evaluar de manera precisa su desempeño y contribuir a estrategias que fortalezcan la protección de los derechos de las personas usuarias en el ámbito paraguayo.

43 CONATEL, Resolución Nº 871/2014. Recuperado de <https://www.conatel.gov.py/conatel/wp-content/uploads/2019/10/rd.530.2016-reglamento-proteccion-al-usuario.pdf>

CRITERIOS DE EVALUACIÓN

En la presente investigación, la evaluación consta de siete criterios, cada uno con sus correspondientes parámetros que permiten analizar la medida en que las empresas cumplen o no con el mismo. Entre los criterios se encuentran: política de privacidad y protección de datos personales, autorización judicial, notificación a la persona usuaria, políticas de promoción y defensa de los derechos humanos, transparencia, guías para requerimiento de información personal y accesibilidad.

Los criterios sobre “política de privacidad” y “requerimiento de autorización judicial” son los únicos que contemplan legislación aplicable actualmente, para el resto de los criterios no existe un marco normativo que aborde todos los parámetros evaluados. En tal sentido, los criterios examinarán la implementación de buenas prácticas que se han ido desarrollando a nivel internacional —principalmente a partir de la iniciativa de la organización Electronic Frontier Foundation (EFF)— y que las empresas están dispuestas a incorporar a sus políticas.

Para esta evaluación se revisaron los contratos de prestación de servicios, informes de sustentabilidad y otros documentos que estaban disponibles en los sitios web de las empresas hasta el 05 de marzo de 2024. También se buscó noticias que circularon en la prensa y los medios especializados y se revisaron los informes de Quién Defiende Tus Datos de años anteriores⁴⁴ para verificar actualizaciones y avances cualitativos y realizar una comparación final.

En una primera etapa se llevó a cabo una evaluación preliminar con el fin de obtener un primer puntaje para cada una de las empresas analizadas en este estudio y, así, comprender en qué parámetros de cada criterio podrían mejorar para alcanzar una mayor puntuación. Este proceso duró 3 meses y abarcó hasta el 30 de abril del 2024.

Luego de la evaluación preliminar TEDIC se puso en contacto con las empresas para solicitarles una reunión con el propósito de explicar en qué consiste el estudio y presentar los resultados preliminares obtenidos del análisis del 2024 y su comparativo en el tiempo con las ediciones anteriores. En esta reunión se buscó que las empresas pudieran brindar información precisa sobre su trabajo por el resguardo de la privacidad de las personas usuarias, así como también complementar la información que se encuentra disponible públicamente o, incluso, aclarar cualquier ambigüedad que pudiera surgir a partir de la misma.

Todas las empresas fueron contactadas vía email. Este primer paso es considerado fundamental para conocer la perspectiva de la empresa y dar la oportunidad para esclarecer cualquier tipo de dudas respecto a sus políticas de privacidad.

44 Disponible en: <https://qdt.tedic.org/#investigacion>

A continuación, se desarrollan cada uno de los siete de los criterios de evaluación de las empresas:

1. POLÍTICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

La ISP 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 las personas usuarias respecto de sus derechos y no debería ser visto como un mero formalismo legal. La ISP 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 y usuarias 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 apearse 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 las personas usuarias⁴⁵. Es indispensable que la ISP cuente con políticas que cumplan estos protocolos a la hora de entregar información y datos personales a las autoridades.

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 las personas usuarias por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico N° 4868/2013 y la Resolución de CONATEL N° 2583/2024. En este escenario, es imprescindible que los ISP 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.

En un caso contencioso⁴⁶ 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.

45 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.

46 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.

En el caso CAJAR contra Colombia⁴⁷, la sentencia de la Corte IDH concluyó que Colombia había violado los derechos fundamentales del colectivo de abogados como la privacidad, libertad de expresión y el derecho a defender los derechos humanos. También reconoció la autonomía informativa como derecho humano autónomo, enfatizando que las personas tienen control sobre quién accede y usa sus datos personales. También subrayó que la vigilancia masiva y el acceso a metadatos sensibles, como ubicación, direcciones IP y comunicaciones privadas, requieren estricta autorización judicial para prevenir abusos y garantizar la proporcionalidad de estas medidas. El tribunal condenó las técnicas de espionaje expansivo utilizadas por Colombia, que incluyen la recopilación indiscriminada de información personal y el acceso a bases de datos no públicas. Además, destacó la importancia de estándares claros en la recolección y tratamiento de metadatos, estableciendo que estos contienen información sensible que puede revelar hábitos, relaciones y movimientos de las personas. Al igual que el caso Escher, esta jurisprudencia nacional sitúa a estos datos en una instancia de protección constitucional y de derechos humanos.

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 las distintas ISP. 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.

Además de analizar cómo se presenta la información en los contratos u otros documentos, esta investigación también busca evaluar la publicación de protocolos específicos que regulen la entrega de datos personales a agentes del Estado. Estos protocolos deben definir claramente las formas y condiciones de acceso a los datos personales en el marco de investigaciones o actuaciones similares. La existencia de protocolos claros y públicos, como los que adoptan varias empresas tecnológicas, es un indicador clave del compromiso de la empresa con la privacidad y la protección de los datos de sus usuarios y usuarias. Este aspecto será abordado específicamente en el criterio 6 de esta investigación.

En este primer criterio, por tanto, al tratarse de una cuestión de controversia jurídica, la cuestión se desarrolla en diferentes puntos, que buscan discriminar diferentes niveles de protección, claridad y compromiso en cuanto al acceso a los datos para las investigaciones. Los criterios tratan de reflejar el compromiso de transparencia de la empresa con respecto a las autoridades consideradas competentes, las disputas normativas actuales y las limitaciones establecidas en la legislación (en particular en lo que respecta a cuya investigación estaría exenta de la necesidad de una orden judicial de acceso a los datos del registro) acceso a los datos del registro, además del compromiso expresado en sus directivas sobre datos de localización, conexión registros de conexión y la publicación de protocolos para la entrega de datos en las investigaciones judiciales.

Por último, en esta edición, en el marco de este criterio, también se considera si las compañías cumplen con las disposiciones establecidas en cuanto a la notificación de riesgo o fugas de datos personales⁴⁸. Se evaluará si tienen acciones de mitigación implementadas y protocolos de notificación a las autoridades en caso de fallas de seguridad que comprometan la información personal de los usuarios de servicios.

47 Corte I.D.H. Caso miembros de la corporación colectiva de abogados “José Alvear Restrepo” vs Colombia. Sentencia 18 de octubre de 2023. Versión completa: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

48 La Política Online. (2024) Tigo es víctima de un hackeo de su base de datos y se reaviva el debate sobre regulación en ciberseguridad. <https://www.lapoliticaonline.com/paraguay/economia-py/tigo-es-victima-de-un-hackeo-de-su-base-de-datos-y-se-reaviva-el-debate-sobre-regulacion-en-ciberseguridad/>

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 de la República 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 ISP 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.

El poder judicial, tanto en los litigios individuales como en los colectivos, es un espacio importante para la defensa y consolidación de los derechos de las personas usuarias frente a los abusos e ilegalidades. Teniendo esto en cuenta, hemos tratado de evaluar la posición de las empresas en los juicios sobre privacidad y protección de datos.

La Constitución Nacional en su artículo 36 sobre la inviolabilidad de las comunicaciones obliga a las autoridades del Estado a solicitar información a los ISP sólo a través de una orden judicial debidamente justificada.

La vigilancia sin consentimiento 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 de la República del Paraguay. En el siguiente cuadro se explica cual el procedimiento para el acceso cumpliendo con los estándares del principio del debido proceso, así como las aplicaciones del código procesal penal paraguayo:



El debido proceso para una interceptación de información o acceso a datos personales (incluyendo metadatos).

3. NOTIFICACIÓN A LA PERSONA USUARIA

La ISP deberá contar con una política de notificación a las personas usuarias afectadas 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 a la persona usuaria al congreso o a otros entes regulatorios. Cuando se notifica a las personas usuarias que sus datos personales o registros de conexión a Internet han sido solicitados por las autoridades administrativas o judiciales se proporcionan condiciones de amplia defensa contra los abusos e irregularidades.

A la luz del principio constitucional del debido proceso, muchas leyes establecen el deber de notificar a los afectados las medidas que afectan a sus derechos. Por su parte el Código Procesal Penal en su artículo 303 dispone, en concordancia con los artículos 75 y 151 del mismo cuerpo legal, la obligación de notificar a la persona, cuando el Ministerio Público le ha imputado por un supuesto hecho punible.

En el contexto de las solicitudes de datos, las ISP desempeñan un rol crucial en la protección de las garantías procesales de las personas usuarias afectadas. Esto se debe a que, al notificarles sobre dichas solicitudes, las empresas permiten que las personas usuarias puedan, en primera instancia, impugnar solicitudes ilegales. Estas incluyen tanto órdenes judiciales infundadas como requerimientos de autoridades administrativas que carecen de competencia o fundamento suficiente.

Sin notificación, la persona usuaria depende de que las propias empresas impugnen contra las solicitudes que consideran abusivas. Si son notificadas por las empresas, las personas usuarias tienen la posibilidad de defenderse de posibles violaciones de su intimidad. 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.⁴⁹

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 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.⁵⁰

49 “Necesario y proporcionado”. Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. Versión mayo 2014. p 36

50 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

La Relatoría Especial sobre Derechos Humanos de la ONU ha enfatizado que la notificación podría no 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. No obstante, en Paraguay, la ya referida normativa vigente establece que, ante la noticia de un hecho presuntamente delictivo y en casos excepcionales, se podrá solicitar autorización judicial para intervenir las comunicaciones⁵¹; empero, no hay obligación de notificar a la persona investigada durante esta etapa inicial, salvo cuando se formaliza una imputación y se identifica a la presunta persona responsable.

Atendiendo a las recomendaciones internacionales en materia de derechos humanos, las ISP tienen la responsabilidad de actuar con buena fe para salvaguardar la privacidad de las personas usuarias. Esto incluye notificarles sobre eventuales intervenciones en sus comunicaciones, en la medida en que dicha notificación no comprometa los objetivos de la investigación penal. Esta práctica, además, facilita que las personas puedan ejercer su derecho a buscar reparación en caso de que sus derechos hayan sido indebidamente afectados. En casos adversos a la implementación de la política de notificación de la empresa, la ISP deberá combatir judicialmente los impedimentos legales para notificar a las personas usuarias afectadas, 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 las personas usuarias afectadas. Es decir, la notificación por la empresa permite a la persona usuaria desafiar las solicitudes ilegales: tanto órdenes judiciales sin fundamento, como solicitudes de las autoridades administrativas sin competencia ni justificación. En la situación actual, la persona usuaria depende de los retos realizados por las propias empresas contra las peticiones que consideran abusivas. Si la persona usuaria es notificada, obtiene a la mayor brevedad, la capacidad de defenderse de posibles violaciones de su privacidad.

Con esto en mente, es importante fomentar la práctica de la notificación a la persona usuaria a través del proyecto “¿Quién defiende tus datos?” (QDTD). 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 contrario). La posibilidad de notificación de la persona usuaria 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 Ministerio de Hacienda o CONATEL. La notificación a la persona usuaria fortalece su capacidad de impugnar legalmente la inclusión de pruebas que sean irrelevantes o no estén relacionadas con los hechos del caso.

En esta edición, se vuelve a poner a esta categoría como una “prima”, porque la notificación no es ni una obligación legal impuesta a las empresas ni una práctica generalizada en Paraguay. 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 las personas usuarias. La notificación a la persona usuaria 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.

51 Código Procesal Penal (1998), Art. 200.

4. POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS

Es determinante para el respeto y protección de los derechos humanos de las personas usuarias y para generar confianza en torno al ecosistema de Internet 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 ISP tiene un posicionamiento institucional público en el que hayan 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 Unidas⁵² a través de la resolución 17/4, del 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.

Para ser considerado, 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 ISP ha participado, ya sea de forma individual o colectiva, en procesos públicos de incidencia legislativa o ante organismos reguladores, con el objetivo de defender el derecho a la privacidad. También se analiza si ha llevado a cabo acciones judiciales en defensa de la privacidad de sus usuarios y usuarias.

También se evalúa si la misma participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales como pueden ser la Global Network Initiative⁵³ o Telecommunications Industry Dialogue⁵⁴.

52 Naciones Unidas. (2011) Principios Rectores sobre las Empresas y los Derechos Humanos: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

53 Global Network Initiative <https://globalnetworkinitiative.org>

54 Telecommunications Industry Dialogue www.telecomindustrydialogue.org

Por otro lado, también se considera que la ISP cuente con políticas de participación en las discusiones locales e Internacionales sobre el ecosistema de Internet; los Foros de Gobernanza de Internet (IGF), donde se discuten 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 de las TIC en relación con el impacto en la privacidad de las personas usuarias han sido más frecuentes en los últimos años⁵⁵. 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 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. En sí misma esta ya es una buena práctica establecida entre empresas de contenidos como Google, Facebook, X (antes Twitter) y Microsoft y los proveedores como Vodafone, Verizon y Telefónica.

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.

6. GUÍAS DE REQUERIMIENTO DE INFORMACIÓN PERSONAL

La ISP cuenta con lineamientos, guías o protocolos orientados a las fuerzas de seguridad y otros organismos gubernamentales que expliquen cómo deben solicitar la información personal de los clientes, cuáles son las condiciones para la entrega de dicha información personal.

Este parámetro se distingue de la publicación de informes de transparencia, ya que estos últimos se centran en presentar datos estadísticos sobre las solicitudes de información recibidas y cumplidas. En cambio, los lineamientos analizados buscan evaluar cómo cada empresa define los procedimientos que las fuerzas policiales o de investigación deben seguir para solicitar información y qué especificaciones deben cumplir en dicho proceso. Asimismo, se examina si la empresa, al establecer sus reglas para las autoridades locales, considera el contexto nacional o si adopta lineamientos predefinidos de origen extranjero. En este último caso, se verifica si dichos procedimientos son más estrictos y protegen mejor

55 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

la privacidad de sus usuarios y usuarias. Algunos buenos ejemplos son la de Telefónica⁵⁶, Entel⁵⁷, VTR⁵⁸ y Comcast⁵⁹ que cuentan con una lista de requerimientos y procedimientos internos globales ante solicitudes de las autoridades locales.

7. ACCESIBILIDAD

La accesibilidad de la información disponible en la web, independientemente de la discapacidad o diversidad funcional de las personas usuarias, es esencial para fortalecer el compromiso con la transparencia y garantizar el respeto a los derechos humanos. La Convención de los Derechos de Personas con Discapacidad⁶⁰, a través de su artículo 9, reconoce al acceso a las tecnologías de la información y comunicación, incluyendo la web, como un derecho humano básico.

La accesibilidad de la web consiste en facilitar el contenido a través de un diseño e infraestructura que funcione para todas las personas usuarias, sin importar el hardware, software, idioma, ubicación, habilidad cognitiva o sensorial. Esto remueve las barreras a la comunicación e interacción que muchas personas enfrentan de manera cotidiana y contribuye a que los espacios digitales también sean más inclusivos para el uso de un rango diverso de las personas usuarias.

Que las ISP en Paraguay cuenten con datos que sean accesibles es parte de ampliar el compromiso con la transparencia y respetar los derechos humanos. El diseño de sitios y herramientas web que sean accesibles es crucial para empresas proveedoras de Internet, ya que habilita a que más personas puedan usar e informarse sobre sus productos y servicios de manera hábil y satisfactoria. Las empresas también deben promover la participación de las personas con discapacidad en la oferta de servicios TIC, asegurando su derecho a la plena participación ciudadana y social.

Para este criterio se evalúan los sitios web oficiales de las proveedoras de Internet utilizando la guía de principios de Accesibilidad⁶¹ de la Web Accessibility Initiative (WAI), parte del W3C (World Wide Web Consortium).

56 Telefónica “define el procedimiento interno global ante requerimientos de las autoridades de acuerdo con cada legislación nacional. Los Principios que rigen el proceso son: Confidencialidad, Exhaustividad, Fundamentación, Proporcionalidad, Neutralidad Política, Respuesta Diligente y Seguridad”: <https://www.telefonica.com/wp-content/uploads/sites/7/2021/11/resumen-reglamento-peticiones-autoridades-competentes-19.pdf>

57 Entel, 2022: <https://www.entel.cl/legales/centro-privacidad/public/pdf/guia%20solicitud%20judiciales.pdf?v=1592022.183832>

58 VTR, 2022: <https://lla-cms-prod.directus.app/assets/683541ba-08f6-485f-8ae7-7fb0bdfa81e7.pdf>

59 Según su Informe de Transparencia 2023, Comcast advierte estar legalmente obligada a responder a solicitudes de información realizadas por agencias gubernamentales, siempre que sean legítimas. Sin embargo, la empresa se compromete a proteger la privacidad y los derechos de sus clientes, revisando cuidadosamente cada solicitud. Antes de proporcionar cualquier información, Comcast dice verificar que la solicitud tenga una base legal válida y esté debidamente delimitada. En caso de que una solicitud sea legalmente cuestionable, poco clara, inapropiada o excesivamente amplia, Comcast solicitará aclaraciones o la rechazará. Además, cuando un cliente solicita información sobre este tipo de requerimientos gubernamentales, Comcast, en general, intenta compartir dicha información, salvo que existan prohibiciones legales, riesgos para investigaciones en curso, personas, o la seguridad y el bienestar de menores. Ver: Comcast. (2023). Transparency report. Recuperado de https://assets.xfinity.com/assets/dotcom/projects/cix-2605_irr-re-platform/2H2023%20Transparency%20Report.pdf; y, Comcast. (2022). Guide for Law Enforcement. Recuperado de https://assets.xfinity.com/assets/dotcom/projects/cix-4479_legal_documentation_sitecore_migration/Comcast%20Guide%20for%20Law%20Enforcement%20-%20August%202022.pdf

60 Naciones Unidas, Convención de los derechos de personas con discapacidad <https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf>

61 Guía de principios de Accesibilidad de la Web Accessibility Initiative (WAI), parte del W3C (World Wide Web Consortium) <https://www.w3.org/WAI/fundamentals/accessibility-principles/es>

REPORTE POR CADA ISP

CRITERIO 1. Política de privacidad y protección de datos personales





¿Proporciona la ISP evaluada información clara y completa sobre la recopilación, uso, almacenamiento, procesamiento y protección de datos personales de la persona usuaria? ¿Se establece de manera precisa qué información de la persona usuaria y de sus comunicaciones son obtenidas, almacenadas, así como la temporalidad con la que dichos datos son almacenados?

En esta categoría, se evalúan las políticas y avisos de protección de datos y privacidad de la ISP que se encuentren disponibles públicamente. Así también, se evalúa el tratamiento de los datos personales que la ISP obtiene al prestar a la persona usuaria el servicio de telecomunicaciones, sin que por ello se limite a los datos que la persona otorga voluntariamente al contratar el servicio.

Criterios de evaluación

- I. La ISP proporciona información y referencias legales claras sobre la recopilación de datos personales, incluyendo los datos personales que se recogen y en qué situaciones se produce la recogida;
- II. La ISP proporciona información y referencias legales claras sobre el uso y/o procesamiento de datos personales, incluyendo los fines para los que se utilizan y cómo se produce este;
- III. La ISP proporciona información y referencias legales claras 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 ISP proporciona información y referencias legales claras 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 quiénes tendrían acceso a las bases de datos;
- V. La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que pasaría, y/o la necesidad de autorización del cliente para hacerlo;
- VI. Es fácil acceder a esta información en el sitio web de la ISP.

Estándar de desempeño:

Estrella llena		La ISP cumple 5 a 6 criterios
Media estrella		La ISP cumple 3 a 4 criterios
Un cuarto de estrella		La ISP cumple 1 a 2 criterios
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE POR EMPRESA SOBRE LA POLÍTICA DE PRIVACIDAD Y DATOS PERSONALES



CLARO – AMX PARAGUAY S.A

Política de privacidad y datos personales		
	Sí	No
La ISP tiene una política de privacidad	•	
La política de privacidad establece de manera precisa qué información de la persona usuaria y sus comunicaciones es obtenida y almacenada	•	
La política de privacidad establece la temporalidad con la que los datos de la persona usuaria son almacenados		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de las personas usuarias son transmitidos a terceros y a autoridades	•	
La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias y/o la necesidad de autorización del cliente para hacerlo	•	
La política de privacidad utiliza un lenguaje sencillo, sin tecnicismos y comprensible para la persona usuaria. La política está disponible en la web de la empresa.	•	

Claro dispone de una política de privacidad accesible desde su página web institucional mediante un proceso sencillo de tres clics.⁶² En ediciones anteriores de QDTD se ha evidenciado un progreso significativo. Por ejemplo, en 2017 no contaban con una política de privacidad, limitándose únicamente a una política de cookies. Sin embargo, a partir de 2020 se incorporó una política de privacidad en su sitio web. Cabe destacar que para el informe de 2022 no se registraron cambios ni actualizaciones en este aspecto. A diferencia de la edición de 2022, anteriormente era posible consultar la fecha de la última modificación de la política de privacidad. No obstante, en la revisión actual dicha información ya no está disponible, a pesar de que la política vigente indica expresamente que se proporcionará la fecha de la última versión.

62 Claro. Políticas de privacidad: <https://www.claro.com.py/personas/legal-y-regulatorio/politicas-de-privacidad>

La política ofrece detalles sobre los tipos de datos recabados y garantiza la no manipulación de datos sensibles. Entre los datos recabados y almacenados se incluyen información personal de identificación, contacto, referencias, profesionales y/o patrimoniales. Ahora bien, la política no especifica la temporalidad del almacenamiento de dicha información. Este vacío puede generar incertidumbre entre los usuarios, quienes podrían beneficiarse de una aclaración sobre el período durante el cual sus datos serán retenidos por la empresa.

En relación con las finalidades del uso de datos, la política establece tanto finalidades primarias como secundarias. Respecto a estas últimas, se identifican tres razones para su cumplimiento: el marketing dirigido a los usuarios, estudios sobre el consumo y actividades destinadas a mejorar los servicios ofrecidos. La política también subraya que las personas usuarias tienen la opción de descartar estas finalidades secundarias, brindándoles la oportunidad de ponerse en contacto con la entidad para solicitar su eliminación.

La ISP menciona explícitamente que compartirá los datos almacenados con terceros por tres razones específicas: el consentimiento del usuario, el procesamiento externo de datos y motivos legales. Además, señala que la información puede compartirse con empresas externas a Claro cuando sea necesario cumplir con las leyes o garantizar el cumplimiento de obligaciones. La ISP establece la obligación de notificar a sus usuarios y usuarias antes de transferir información personal, aunque esta notificación solo se realizará en el contexto de fusiones, adquisiciones o venta de activos de Claro.

Un aspecto destacado es la inclusión de opciones para limitar la divulgación de datos personales, así como la posibilidad de cancelar o revocar el consentimiento para el tratamiento de estos. Sin embargo, no queda claro si estas opciones solo se aplican a la recepción de promociones de la compañía o abarcan otros aspectos relacionados con el tratamiento de datos de las personas usuarias.

Finalmente, la política de privacidad menciona que se ajusta al cumplimiento exhaustivo de las leyes relacionadas con la protección de datos personales en el país, aunque no especifica cuáles leyes concretamente.

Conforme al estándar de desempeño establecido, Claro cumple con 5 de los 6 criterios por lo que califica con una estrella.





COPACO S.A.

COPACO S.A. - COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Política de privacidad y datos personales		
	Sí	No
La ISP tiene una política de privacidad		•
La política de privacidad establece de manera precisa qué información de la persona usuaria y sus comunicaciones es obtenida y almacenada		•
La política de privacidad establece la temporalidad con la que los datos de la persona usuaria son almacenados		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de las personas usuarias son transmitidos a terceros y a autoridades		•
La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias y/o la necesidad de autorización del cliente para hacerlo		•
La política de privacidad utiliza un lenguaje sencillo, sin tecnicismos y comprensible para la persona usuaria. La política está disponible en la web de la empresa.		•

COPACO presenta en su sitio web una política de privacidad limitada exclusivamente al uso de sus aplicaciones móviles⁶³. Esta observación se ha señalado desde las ediciones anteriores, a partir de 2020, y hasta la fecha no se han realizado ajustes ni actualizaciones significativas para mejorar la protección de la privacidad de las personas usuarias. Además, en comparación con la edición anterior, no se identifican cambios evidentes en la política de privacidad previamente analizada, ni se especifica la fecha de su última actualización. Por lo tanto, estas condiciones generales de uso no pueden considerarse una política de privacidad integral que cumpla con los estándares aplicables a una ISP.

63 Condiciones Generales de Uso – APPs Oficiales: <https://www.copaco.com.py/index.php/condiciones-apps.html>

En cuanto al segundo criterio referido en el cuadro, notamos que la mentada política de privacidad de esta ISP no aborda detalladamente cuáles serán los datos recabados por las aplicaciones oficiales ni la temporalidad del almacenamiento de dicha información. Este vacío es consistente con el contrato de prestación de servicios disponible en la página web de la ISP⁶⁴. Aunque se menciona en el punto 6.4. el manejo confidencial y privado de los datos personales de los usuarios y usuarias no se ofrece detalles adicionales sobre el tratamiento de estos datos.

En relación con la transmisión de datos COPACO prohíbe expresamente la cesión de datos a terceros, salvo por requerimiento judicial. Dicha cláusula establece: “Esta compañía no venderá, cederá ni distribuirá la información personal que es recopilada sin su consentimiento, salvo que sea requerido por un juez con una orden judicial”. Sin embargo, esta restricción está limitada al uso de aplicaciones oficiales como se especifica al inicio del documento: “La presente Política de Privacidad establece los términos en que Copaco S.A. usa y protege la información que es proporcionada por sus usuarios, usuarias y/o clientes al momento de utilizar sus APPs oficiales”. Aunque la enunciación “Esta compañía no venderá” podría interpretarse como una prohibición general de transmisión de datos en toda la empresa, el alcance de la política está explícitamente restringido a las aplicaciones oficiales, excluyendo información que podría ser obtenida a través de otros servicios como telefonía, servicios de Internet y televisión.

En este contexto, el enfoque limitado no permite evaluar los demás criterios de privacidad establecidos en los estándares de desempeño por lo que se otorga una estrella vacía debido a que la ISP no cumple con ninguno de los criterios evaluados en este punto.



64 COPACO. Personas y Hogares. Internet: <https://www.copaco.com.py/index.php/personas-y-hogares/internet/internet-adsl.html>

Personal

PERSONAL - NÚCLEO S.A.

Política de privacidad y datos personales		
	Sí	No
La ISP tiene una política de privacidad	•	
La política de privacidad establece de manera precisa qué información de la persona usuaria y sus comunicaciones es obtenida y almacenada	•	
La política de privacidad establece la temporalidad con la que los datos de la persona usuaria son almacenados		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de las personas usuarias son transmitidos a terceros y a autoridades	•	
La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias y/o la necesidad de autorización del cliente para hacerlo	•	
La política de privacidad utiliza un lenguaje sencillo, sin tecnicismos y comprensible para la persona usuaria. La política está disponible en la web de la empresa.	•	

La empresa no contaba con políticas de privacidad según los informes de 2017 y 2020. Esto cambió en 2022, aunque inicialmente la política no estaba disponible en su sitio web. Sin embargo, en la edición más reciente de QDTD, se destaca que Personal ahora facilita el acceso a su política de privacidad con tan solo un clic, ubicado en la parte inferior de su página web institucional⁶⁵. La empresa menciona que esta nueva versión ha sido desarrollada de acuerdo con sus políticas globales de protección de datos de Personal y en estricto cumplimiento con las leyes y normativas aplicables en Paraguay.

En cuanto a la recopilación y almacenamiento de datos, la ISP detalla los tipos de datos que se recolectarán, subrayando que no procesan información de personas menores de 18 años. Además, proporciona información sobre los medios a través de los cuales se obtienen los datos personales de sus usuarios y usuarias mencionando canales de contacto disponibles, el uso de fuentes públicas y otras tecnologías como las “cookies”. Un aspecto por destacar es la referencia a la consulta de información crediticia en sociedades o burós, con la otorgación de un mandato irrevocable para este propósito.

65 Personal. Privacidad de Datos: <https://www.personal.com.py/institucional/privacidad-de-datos.html>

Por otro lado, en la sección de términos y condiciones aplicables a las aplicaciones de la ISP, como Personal ID, Personal APP, Tienda Personal APP, MiPersonal WEB, Mi Personal Empresa Web, Tienda Personal – Ecommerce y Billetera Personal, se detallan de manera más específica los datos personales que serán recopilados⁶⁶. Esto incluye, además de los ya mencionados, datos biométricos como huellas dactilares, voz, imagen facial u otros de naturaleza similar. En este apartado, la ISP aclara que la recopilación de estos datos sensibles se realiza exclusivamente para validar la identidad en procesos específicos, como ventas, postventa o concesión de créditos, con el objetivo de prevenir actividades ilícitas y permitir la autenticación electrónica, siempre y cuando la persona usuaria lo decida en determinados productos y servicios ofrecidos por Personal. Asimismo, la ISP reconoce explícitamente los derechos de sus personas usuarias tales como el acceso, la actualización, la rectificación, la supresión, la oposición y la portabilidad de sus datos, entre otros. Se informa detalladamente sobre cómo ejercer estos derechos, de acuerdo con el Aviso de Privacidad y la legislación vigente.

En relación con el tercer criterio, se observa la ausencia de información acerca de la temporalidad de la retención de datos. A pesar de abordar las finalidades del tratamiento de datos, que incluyen la prestación de servicios, objetivos comerciales, cumplimiento de requisitos legales, mejora de los servicios, determinación de perfiles de riesgo del cliente, cumplimiento normativo, prevención de fraude y riesgos, revisión de calidad, y mejora de la funcionalidad de las aplicaciones, no se especifica el tiempo de retención de dichos datos.

En el cuarto criterio, la ISP admite la posibilidad de delegar la custodia y almacenamiento de datos a terceros así como de compartir información personal de las personas usuarias con entidades de su grupo empresarial y terceros que presten servicios a la misma, especialmente en casos de fusión, adquisición, venta de activos o transición del servicio. Además, la ISP menciona que puede compartir datos con jurisdicciones que tengan leyes de protección de datos diferentes a las de Paraguay, por orden judicial o cuando lo permita la ley. La ISP también aclara la facultad de proporcionar información sobre deudas a sociedades de información crediticia. Por último, destaca que todas las comunicaciones y usos de datos personales se protegen contra alteraciones, destrucciones o accesos no autorizados.

Respecto al quinto criterio, la ISP hace referencia a la Ley 6534/2020 de “Protección de Datos Personales Crediticios”, norma vigente en materia de protección de datos personales en Paraguay. La ISP utiliza esta ley para respaldar los derechos de las personas usuarias como consultar, acceder y rectificar sus datos personales, oponerse al uso con fines publicitarios y otros derechos autorizados por la legislación. La ISP indica que, en caso de conflictos, serán aplicables otras leyes vigentes en el país para la interpretación, uso, alcance y terminación del aviso de privacidad. Igualmente, menciona a la Secretaría de Defensa del Consumidor y el Usuario como autoridad de aplicación, en consonancia con las disposiciones de la Ley 6534/2020.

Cabe resaltar el esfuerzo de esta ISP en proporcionar un aviso de privacidad accesible a diferencia de la edición anterior de esta investigación. Por ello, conforme al estándar de desempeño establecido, Personal cumple con 5 de los 6 criterios por lo que califica con una estrella.



66 Personal. Términos y Condiciones de Aplicaciones de Personal: <https://www.personal.com.py/institucional/terminos-y-condiciones-apps.html>



TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Política de privacidad y datos personales		
	Sí	No
La ISP tiene una política de privacidad	•	
La política de privacidad establece de manera precisa qué información de la persona usuaria y sus comunicaciones es obtenida y almacenada	•	
La política de privacidad establece la temporalidad con la que los datos de la persona usuaria son almacenados		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de las personas usuarias son transmitidos a terceros y a autoridades	•	
La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias y/o la necesidad de autorización del cliente para hacerlo	•	
La política de privacidad utiliza un lenguaje sencillo, sin tecnicismos y comprensible para la persona usuaria. La política está disponible en la web de la empresa.	•	

La política de privacidad de Tigo se encuentra fácilmente accesible desde la portada de su sitio web, ubicada en el pie de página y a tan solo un clic⁶⁷. Es destacable que esta ISP provee información sobre las fechas de las actualizaciones de su política, siendo la última actualización de este documento el 26 de mayo de 2023.

Este cambio resulta relevante porque, según los informes de 2017, TIGO no disponía de una política de privacidad visible en su sitio web. Lo que sí estaba disponible se encontraba en los “Términos y condiciones de uso del sitio web”, los cuales aplicaban exclusivamente a las personas usuarias que navegaban por su portal. En contraste, para la edición de 2020, se observó que TIGO ya contaba con una política de privacidad claramente accesible, disponible incluso con un solo clic. En la edición de 2022 se constató que dicha política seguía vigente y correspondía a la versión publicada el 8 de septiembre de 2020.

En cuanto al segundo criterio, en el aviso de privacidad también se señalan de manera detallada los datos a ser recolectados, aclarando que no procesan información de personas menores de 18 años. En este punto es importante destacar que Tigo ofrece la previsualización de su contrato de prestación de servicios en su página web⁶⁸, actualizado al 25 de mayo de 2023. En este documento se aborda la temá-

67 Tigo. Aviso de Privacidad. Recuperado de <https://www.tigo.com.py/legales#terminos-y-condiciones-aviso-de-privacidad>

68 Tigo. Contrato de suscripción de servicios de telecomunicaciones. Punto 9. Recuperado de https://assets.tigocloud.net/j1bxozgharz5/3e69JpNDplHw6aQGGFnb2H/155811241e933df7960971d67e061f44/Contrato_De_Suscripci__n_De_Servicios_De_Telecomunicaciones.pdf?_ga=2.186110569.1774162512.1708956346-1194848194.1708361641&_gac=1.17007563.1708361669.CjwKCAiALcyuBhBnEiwAOGZ2S8dv7pN2eQxjDb_7JnR2qXTMLfm_zEXJLR2kqpVL-JyZQDs8Nye-QBoCKUwQAvD_BwE

tica de los datos personales recopilados de forma aún más detallada, incluyendo referencias a datos biométricos como huellas dactilares, voz y reconocimiento facial, pero apelando en partes a términos poco claros.

Es relevante recordar que, al ser un contrato estandarizado, las condiciones son establecidas de manera unilateral por la ISP, sin dar margen a la persona usuaria para oponerse en caso de que desee utilizar el servicio sin facilitar datos sensibles para su tratamiento. Por lo que se advierte la importancia de que el aviso de privacidad sea coherente con la política de tratamiento de datos personales que se expone en el contrato. Aunque la ISP establece que el aviso prevalecerá sobre otros términos y políticas, incluso al contrato, en caso de conflicto.

La política de privacidad estudiada detalla de manera específica los medios por los cuales recolectan información sobre sus usuarios y usuarias, abarcando diversos canales de contacto, así como la mención a la posibilidad de adquirir datos de manera automática mediante el uso de “cookies” u otras tecnologías. Sin embargo, no establece explícitamente la duración exacta por la cual los datos personales recolectados serán almacenados. Aunque la ISP menciona que guarda los datos “por el período de tiempo que sea necesario para cumplir con la finalidad por la cual se recopilaron, y conforme a lo requerido por la regulación local vigente”, no proporciona una especificación clara respecto al lapso temporal específico.

En los informes de 2017, 2020 y 2022, se destacó que la recolección de información por parte de la empresa no era clara, y tampoco se especificaba el tiempo de almacenamiento de los datos. Aunque esta práctica cumplía parcialmente con la Ley de Comercio Electrónico al almacenar la información según lo exigido, infringía la normativa al compartirla para fines no contemplados, como persecuciones penales. Esto evidencia una falta de avances significativos en la implementación de medidas proactivas para proteger la información y los derechos de las personas usuarias.

En relación al cuarto criterio, Tigo refiere que comparte datos personales con terceros para servicios internos y externos, como almacenamiento, cobranza y atención al cliente. Además, la compañía puede compartir datos con otras entidades de Tigo o en situaciones como fusiones, adquisiciones o venta de activos. Igualmente, menciona que puede transferir información a jurisdicciones con leyes de protección diferentes a Paraguay, bajo autorización judicial o conforme a la ley.

Sobre el quinto criterio, la ISP no menciona en el aviso de privacidad la necesidad de autorización del cliente para compartir datos con terceros, sin embargo, contempla la posibilidad de revocar dicha autorización. Ahora bien, es necesario mencionar aquí que se observa una discrepancia con el contrato de suscripción de servicios de telecomunicaciones. Este último documento, en el punto 9.3. literal d), establece expresamente que la persona usuaria debe autorizar el suministro de sus datos personales a terceros proveedores de servicios o productos, socios comerciales, entidades afiliadas y subsidiarias de ISP, o empresas del mismo grupo empresarial, tanto dentro como fuera de Paraguay. A este respecto, la ISP podría facilitar una comprensión más transparente de los términos relacionados con la autorización de datos a terceros.

En las ediciones de 2017 y 2020, los ítems de los criterios no eran tan desagregados ni comparables como en las ediciones de 2022 y la actual. Sin embargo, se observó que desde el 2022 no se mencionaba la necesidad de autorización explícita del cliente para compartir datos con terceros, aunque sí se contemplaba la posibilidad de revocar dicha autorización. Estos puntos expuestos tampoco observan cambios sustanciales con relación al informe actual.

Por último, aunque en el aviso de privacidad se mencionan referencias legales, dicha mención es genérica. Se establece la aplicabilidad de las leyes paraguayas al uso e interpretación de esta, pero no se especifica qué leyes en particular. Esta misma falta de precisión ya se había identificado en el informe de 2022, donde las referencias legales también eran generales y se limitaban a indicar la aplicación de las leyes paraguayas, sin ofrecer mayores detalles.

Según el análisis realizado para esta edición, Tigo cumple con 5 de los 6 criterios evaluados, lo que le otorga una calificación de una estrella. Aunque se reconoce que ha habido ciertos avances en algunos aspectos, los desafíos pendientes siguen siendo significativos. La empresa debe emprender cambios sustanciales para garantizar una mayor protección a la privacidad y alinearse plenamente con las mejores prácticas en la protección de derechos de sus usuarios y usuarias.





VOX - HOLA PARAGUAY S.A.

Política de privacidad y datos personales		
	Sí	No
La ISP tiene una política de privacidad		•
La política de privacidad establece de manera precisa qué información de la persona usuaria y sus comunicaciones es obtenida y almacenada		•
La política de privacidad establece la temporalidad con la que los datos de la persona usuaria son almacenados		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de las personas usuarias son transmitidos a terceros y a autoridades		•
La ISP proporciona información y referencias legales claras en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias y/o la necesidad de autorización del cliente para hacerlo		•
La política de privacidad utiliza un lenguaje sencillo, sin tecnicismos y comprensible para la persona usuaria. La política está disponible en la web de la empresa.		•

Al igual que en todas las ediciones anteriores de esta investigación, esta ISP carece de una política de privacidad, la cual no está disponible ni en su página web ni pudo ser localizada mediante motores de búsqueda en Internet. Aunque dispone de una sección denominada “Mis Datos, Mi Seguridad”⁶⁹, esta se limita a proporcionar recomendaciones básicas sobre seguridad digital.

En consecuencia, la ISP no puede ser evaluada en los restantes criterios dada la ausencia de información relevante en este aspecto, por lo que califica con cero estrellas.



69 Vox. Chembae. Recuperado de <https://www.vox.com.py/empresa/chembae>

CRITERIO 2. Autorización judicial




¿Se compromete la ISP 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 ISP 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 empresa en su contrato o cualquier documento oficial a disposición del público deja claro a las personas usuarias las circunstancias en que las autoridades judiciales o administrativas pueden tener acceso a sus datos.

Criterios de evaluación

- I. La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa;
- II. Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.

Estándar de desempeño:

Estrella llena		La ISP cumple con todos los criterios
Media estrella		La ISP cumple con uno de los criterios
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - AUTORIZACIÓN JUDICIAL



CLARO - AMX PARAGUAY S.A.

Autorización judicial		
	Sí	No
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.		•

Aunque Claro Paraguay menciona que compartirá datos personales por motivos legales, no especifica claramente si esto se limita a órdenes judiciales. Para obtener detalles adicionales sobre el servicio proporcionado por esta ISP y evaluar este criterio, revisamos el informe de sustentabilidad del 2023 proporcionado por América Móvil⁷⁰, empresa matriz de Claro Paraguay, que destaca su compromiso de respetar la privacidad y seguridad de las comunicaciones de los usuarios, evitando intervenciones, escuchas o monitoreos.

De hecho, en este informe de sustentabilidad 2023, el grupo afirma que antes de compartir información con autoridades, verifican que las solicitudes cumplan con los requisitos legales. Asimismo, informa que recibió 810.956 solicitudes, el 97.26% se proporcionó tras verificar su cumplimiento con la legislación, y el 2.74% restante no se procesó debido a incumplimientos de regulaciones u otros supuestos no especificados. Cabe señalar, además, que, en el mentado informe, se proporciona un enlace al Informe de Transparencia en Comunicaciones⁷¹, donde se detalla la legislación específica en la que se basa América Móvil para la entrega de datos. En el caso de Paraguay se especifica, entre otras cuestiones, que las autoridades competentes para la entrega de datos, bloqueo de líneas telefónicas, localización geográfica e intervención en comunicaciones son los jueces y el Ministerio Público indistintamente. Sin embargo, este último órgano carece de competencia para dictar órdenes judiciales.

70 América Móvil. Informe de Sustentabilidad 2023. págs. 88-90. Recuperado de: <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

71 América Móvil. Informe de Transparencia en las Comunicaciones 2023. Recuperado de: <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>

En lo que respecta al primer y segundo criterio, los informes previos de 2017, 2020 y 2022 ya evidenciaban prácticas similares a las observadas en este periodo 2024, lo que refleja una falta de progreso significativo en estas áreas críticas. Continúa existiendo una preocupante ausencia de claridad en los procedimientos relacionados con la entrega de información bajo orden judicial, particularmente en lo que concierne al manejo de metadatos.

Actualmente, estos datos se proporcionan incluso a solicitud del Ministerio Público, sin una supervisión judicial adecuada ni un proceso transparente que garantice el cumplimiento de los principios del debido proceso establecidos en la Constitución. De hecho, en el mencionado Informe de Transparencia, se puede observar que la ISP reportó 4794 requerimientos totales por autoridad, de los cuales 4494 corresponden a requerimientos de las fiscalías y solo 300 al Poder Judicial. Asimismo, refieren haber considerado válidos todos y cada uno de estos requerimientos⁷². Este enfoque no solo incumple los estándares nacionales, sino que también vulnera las disposiciones contenidas en sentencias de la Corte Interamericana de Derechos Humanos, que son de carácter vinculante para nuestra jurisdicción y exigen que cualquier limitación al derecho a la privacidad esté debidamente fundamentada y supervisada por la autoridad judicial competente.

La falta de alineación con estos estándares no solo pone en riesgo los derechos fundamentales de las personas, sino que también subraya la necesidad urgente de implementar cambios estructurales en los protocolos de manejo de información. Es imperativo garantizar que los procesos sean claros, transparentes y acordes con los principios internacionales de derechos humanos y las obligaciones legales vigentes en el país.

Conforme al estándar de desempeño establecido, Claro no cumple con ninguno de los criterios establecidos al igual que en la edición anterior, por lo que no lleva ninguna estrella.



72 Ídem. pág. 21



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Autorización judicial		
	Sí	No
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.		•

Si bien la ISP establece un compromiso explícito de entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia únicamente cuando exista una orden judicial previa, este compromiso se encuentra expresado exclusivamente en la política de privacidad que regula los datos recabados y procesados a través de sus aplicaciones oficiales. Sin embargo, la política de privacidad divulgada por COPACO no menciona de manera específica los servicios de telecomunicaciones que también proporciona, como telefonía e Internet. Esto no implica necesariamente que la misma protección no se aplique al contenido de las comunicaciones a través de estos servicios, pero la falta de una referencia explícita en la política disponible en línea deja esta cuestión sin aclarar.

En cuanto al segundo criterio, en las condiciones evaluadas, la ISP no hace distinción entre el contenido de las comunicaciones y los metadatos, por lo que igualmente amerita una calificación negativa.

Los informes de 2017, 2020 y 2022 ya señalaban prácticas similares a las observadas en 2024, reflejando una falta de avances. Persiste la falta de claridad en la entrega de información bajo orden judicial, especialmente en el manejo de metadatos, los cuales se entregan únicamente a solicitud del Ministerio Público, sin supervisión judicial adecuada. Esto incumple el debido proceso constitucional y las sentencias de la Corte Interamericana de Derechos Humanos, que exigen transparencia y control judicial. Urge implementar protocolos claros y alineados con estándares internacionales para proteger los derechos fundamentales.

De acuerdo con el estándar de desempeño establecido, COPACO no cumple con ninguno de los criterios evaluados, lo que se traduce en una calificación sin estrella.



Personal

PERSONAL - NÚCLEO S.A.

Autorización judicial		
	Sí	No
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		●
Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.		●

La ISP informa que podrá compartir datos de una persona usuaria por orden escrita de autoridad judicial competente o cuando así sea permitido en cumplimiento con la ley. No obstante, menciona otras circunstancias que indican que la orden judicial no es un requisito excluyente para la divulgación de datos.

En relación con el segundo criterio, la empresa no realiza distinciones entre el contenido de las comunicaciones y los metadatos, es decir, no queda claro que tipo de datos o contenidos de las comunicaciones se comparte, lo que resulta en la inobservancia de ambos criterios.

Los informes de 2017, 2020 y 2022 ya advertían sobre las mismas prácticas identificadas en 2024, lo que evidencia una falta de progreso. La entrega de metadatos se realiza únicamente a pedido del Ministerio Público, sin la supervisión judicial requerida, incumpliendo el debido proceso constitucional y las sentencias vinculantes de la Corte Interamericana de Derechos Humanos. Es necesario adoptar medidas claras y transparentes que respeten los estándares internacionales y garanticen la protección de los derechos fundamentales.

Por otro lado, se identificó que en el informe del 2017, el Ministerio Público confirmó que una periodista del periódico ABC fue objeto de vigilancia y se encontraron evidencias de que la empresa Personal facilitó sus datos sin el debido proceso legal⁷³. Aunque este caso se relaciona específicamente con el servicio de telefonía y no con el servicio de Internet de la empresa, es fundamental destacar que la manipulación indebida de metadatos en servicios de telecomunicaciones vulnera nuestros derechos humanos y podría ser considerada inconstitucional. Ante la gravedad de este hecho, resulta indispensable que Personal emita públicamente un posicionamiento claro al respecto.

Conforme al estándar de desempeño establecido, Personal no cumple con ninguno de los criterios establecidos, por lo que no lleva estrella.



73 Abc Color (2016). Gobierno usó su sistema de inteligencia para espiar periodista. <https://www.abc.com.py/edicion-impresa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html>



TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Autorización judicial		
	Sí	No
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.		•

La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia bajo diversas circunstancias, no restringiéndose únicamente a una orden judicial. Esta disposición se refleja en el aviso de privacidad, donde Tigo refiere que puede compartir datos personales, presentando varias opciones de manera disyuntiva y sin que la orden judicial sea un requisito excluyente para la entrega de datos en respuesta a requerimientos estatales.

Sin embargo, Millicom International Cellular SA, la empresa matriz de Tigo Paraguay, destaca en su informe anual sobre divulgación a las autoridades judiciales (LED) que las subsidiarias, incluida Tigo Paraguay, solo entregan datos sobre el contenido de las comunicaciones bajo orden judicial en Paraguay⁷⁴. Cabe señalar como una dificultad el acceso a este documento, ya que no se encuentra disponible en el sitio web de Tigo Paraguay, sino únicamente en la página web de Millicom.

En la página 7 del informe LED arriba citado, Millicom señala que, en Paraguay, las autoridades exigen acceso directo a la red móvil. Los procedimientos establecidos permiten a la empresa verificar la orden judicial necesaria para iniciar la interceptación y estar al tanto de cuándo ocurre. Señala que, en caso de discrepancias legales, la empresa puede presentar una queja ante la Corte Suprema de Justicia. No obstante, según este informe, dependiendo del tipo de acceso directo, es posible que Tigo no sea notificada en todos los casos de interceptación de la comunicación del cliente. Asimismo, menciona que la solicitud escrita real recibida cuenta como una solicitud en las tablas de datos y una solicitud puede abarcar información sobre varias personas o dispositivos. Finalmente, la empresa afirma que evalúa la legalidad de estas solicitudes antes de proporcionar la información solicitada a las autoridades.

En dicho documento, se distinguen tres tipos de requerimientos por autoridad: interceptación a las comunicaciones, Mobile Financial Services (servicios financieros ofrecidos por la ISP, datos sobre transacciones y actividad de cuentas) y metadatos (direcciones IP, tráfico de mensajes, correo electrónico, navegación en internet, información de ubicación). Es valorable que la empresa matriz de Tigo Paraguay incluya en su informe información sobre la política de acceso a las comunicaciones y establezca que la entrega del contenido de las mismas se realiza exclusivamente mediante orden judicial. Sin embargo,

⁷⁴ Millicom International Cellular SA. 2023 Millicom Group Law Enforcement Disclosure (LED). Recuperado de: <https://www.millicom.com/media/5828/2023-led-report-20240402-2-2.pdf>

resulta imperativo que dicha información esté disponible en español y de forma accesible a través del sitio web oficial de la ISP en Paraguay, considerando que este es el principal canal de interacción con los usuarios en el territorio nacional.

La transparencia en este aspecto es fundamental, ya que involucra un derecho humano esencial: la protección frente al acceso indebido a las comunicaciones privadas por parte de las autoridades. Por esta razón, no es posible otorgar una evaluación positiva en este criterio mientras la política de privacidad de Tigo Paraguay no incluya una declaración explícita y accesible que garantice que el acceso al contenido de las comunicaciones únicamente se realiza bajo la debida autorización judicial. Este nivel de claridad y especificidad es indispensable para cumplir con los estándares internacionales en derechos humanos y garantizar la confianza de los usuarios en el manejo de sus datos por parte de la empresa.

En respuesta al segundo criterio, la información proporcionada por Millicom indica que en Paraguay existen procesos claros y requisitos específicos para la supervisión judicial sobre interceptación y solicitudes de metadatos de los clientes. Sin embargo, en el informe, no queda claro a quién se le otorga acceso a esta información, ya que, aunque se menciona quiénes pueden solicitar e impartir órdenes de interceptación, la distinción no es clara.

En lo que respecta al primer y segundo criterio, ya en las ediciones anteriores del 2017, 2020 y 2022, se observan las mismas prácticas identificadas en este periodo 2024. Persiste la falta de claridad en la entrega de información bajo orden judicial, particularmente en lo referente a metadatos, los cuales son proporcionados únicamente a solicitud del Ministerio Público. Esta práctica contraviene los estándares del debido proceso constitucional y las sentencias de la Corte Interamericana de Derechos Humanos, que son vinculantes para nuestra jurisdicción. Por otro lado, la empresa sostiene que la mayoría de las solicitudes se refieren a la categoría de metadatos del cliente, principalmente para confirmar la identidad detrás de números de teléfono específicos. No obstante, resulta ambiguo si dichas solicitudes refieren a requerimientos fiscales u órdenes judiciales.

En suma, según el estándar de desempeño establecido, Tigo no cumple con los criterios establecidos, por lo que no obtiene ninguna estrella.





VOX - HOLA PARAGUAY S.A.

Autorización judicial		
	Sí	No
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de una persona usuaria a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.		•

No se dispone de información accesible para determinar si la ISP entrega datos, ya sea mediante orden judicial u otro método. Bajo el estándar de desempeño establecido, Vox no satisface ninguno de los criterios, lo que resulta en una calificación sin estrella.

Como se puede observar, el resultado del cumplimiento de este criterio por parte de estas empresas es preocupante. Aunque el artículo 228 del Código Procesal Penal otorga al Ministerio Público la facultad de solicitar informes a entidades privadas, incluidas las ISP, es importante subrayar la primacía de las normativas específicas sobre las disposiciones generales en este análisis. En particular, los artículos 198, 199 y 200 del mismo código establecen la necesidad de una orden judicial para cualquier intervención en las comunicaciones. Asimismo, es esencial recordar la excepcionalidad de dichas intervenciones, conforme a las disposiciones constitucionales que buscan salvaguardar la intimidad de las personas. Además, la Ley de Telecomunicaciones y las sentencias de la Corte Interamericana de Derechos Humanos (CIDH), que son de aplicación obligatoria gracias al principio de Convencionalidad, garantizan la protección tanto del contenido como de la existencia de las comunicaciones, incluyendo los metadatos.

Se reitera la preocupación sobre este punto, expresada ya en ediciones anteriores. Las contradicciones y prácticas jurisdiccionales cuestionables en este ámbito necesitan mejoras y no deben ser excusa para que las ISP eviten un escrutinio riguroso respecto a las solicitudes de interceptaciones de las comunicaciones.





CRITERIO 3. Notificación a la persona usuaria

Para obtener una estrella en esta categoría, las empresas deben cumplir con al menos una de las siguientes acciones: Tener una política que garantice la notificación a las personas usuarias afectadas por medidas de vigilancia estatal tan pronto como la ley lo permita. Demostrar que han emprendido acciones legales para eliminar los impedimentos legales o regulatorios que dificultan dichas notificaciones. Probar que han promovido mecanismos de notificación ante el Congreso o ante otros entes regulatorios.

Criterio de evaluación

- I. La empresa se compromete a notificar a las personas usuarias 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.

Estándar de desempeño:

Estrella llena		La ISP cumple el criterio
Estrella vacía		La ISP no cumple con el criterio

REPORTE - NOTIFICACIÓN A LA PERSONA USUARIA



CLARO - AMX PARAGUAY S.A.

Notificación a la persona usuaria		
	Sí	No
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias 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.		•

En la política de privacidad de Claro no se observa que la empresa se comprometa a notificar a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión, excepto en el caso de una fusión, adquisición o venta de activos. Ante este último caso, la ISP sostiene que asegurará la confidencialidad y notificará a las personas usuarias afectadas antes de la transferencia de información o la aplicación de una nueva política de privacidad.

Como mencionamos en la edición anterior, el compromiso de notificar sobre la transferencia de información personal no es suficiente, ya que la política de privacidad permite transferencias a terceros, tanto nacionales como extranjeros, en diversas circunstancias que van más allá de las funciones esenciales de la empresa. Esto incluye transferencias con fines de procesamiento externo, promoción de productos o servicios, y cumplimiento legal, sin detallar mecanismos claros de notificación previa a las personas usuarias.

La falta de compromiso para notificar a las personas usuarias sobre el uso, solicitud o compartición de sus datos personales ha sido una constante en todas las ediciones anteriores de este informe. Esta omisión refleja una brecha en la transparencia y el respeto a los derechos de las personas usuarias, evidenciando la necesidad de implementar mecanismos claros de notificación que fortalezcan la confianza y cumplan con estándares internacionales.

Conforme al estándar de desempeño establecido, Claro no cumple con el criterio por lo que no obtiene estrellas.





COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A

Notificación a la persona usuaria		
	Sí	No
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias 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.		•

La ISP en cuestión no hace referencia a notificaciones a la persona usuaria y recordemos que las condiciones de privacidad disponible en su página web se refiere únicamente al uso de aplicaciones de la compañía.

Desde las primeras evaluaciones, se ha señalado que no existen políticas transparentes ni procedimientos establecidos para informar a sus usuarios cuando su información es solicitada, utilizada o compartida, ya sea por requerimientos legales o por otras razones.

De acuerdo con el estándar de desempeño establecido, COPACO tampoco cumple con el criterio y, por lo tanto, no obtiene estrella.



Personal

PERSONAL - NÚCLEO S.A.

Notificación a la persona usuaria		
	Sí	No
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias 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.		•

Personal no cumple con el criterio de notificar a la persona usuaria sobre la entrega a terceros de sus datos personales. Aunque han actualizado su política de privacidad con respecto a la edición anterior de esta investigación, aún no se observa que refiera la notificación a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión así como establece el estándar de desempeño.

En todas las ediciones anteriores de este informe se ha señalado la ausencia de un compromiso por parte de la empresa para informar a las personas usuarias cuando sus datos personales son solicitados, utilizados o compartidos. Esta carencia evidencia una falta de transparencia que afecta la confianza de las personas usuarias y subraya la necesidad de establecer mecanismos claros de notificación alineados con los estándares internacionales.

Conforme al estándar de desempeño establecido, esta ISP no obtiene estrella en este criterio.





TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Notificación a la persona usuaria		
	Sí	No
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias 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.		•

Al igual que lo observado en nuestra edición anterior, Tigo sigue sin abordar en su aviso de privacidad la cuestión de la notificación a la persona usuaria antes y/o después de la entrega de datos personales a terceros.

Todas las ediciones anteriores de este informe han destacado la ausencia de medidas claras para notificar a las personas usuarias sobre el manejo de sus datos personales. Esta falta de transparencia representa una oportunidad clave para la empresa, que podría fortalecer la confianza de las personas usuarias al implementar procesos de notificación alineados con buenas prácticas internacionales.

Conforme al estándar de desempeño establecido, Tigo no cumple con el criterio por lo que no obtiene estrella.





VOX - HOLA PARAGUAY S.A.

Notificación a la persona usuaria		
	Sí	No
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias 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.		•

Es importante subrayar nuevamente que esta ISP no dispone de políticas de privacidad de datos, al menos no de manera pública. Asimismo, no se identifica ninguna otra mención o referencia acerca de notificaciones a la persona usuaria 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.

En ediciones previas de este informe se ha resaltado la falta de compromiso de la empresa para notificar a las personas usuarias sobre el uso o la solicitud de sus datos personales. Esta omisión evidencia la necesidad de adoptar políticas más transparentes que refuercen la confianza de los usuarios y cumplan con estándares internacionales.

De acuerdo con el estándar de desempeño establecido, Vox no satisface el criterio, por lo que no obtiene ninguna estrella.



CRITERIO 4. Políticas de promoción y defensa de los derechos humanos

¿Ha iniciado la 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 este criterio se analiza si la empresa cuenta con una política institucional que reconozca su responsabilidad en la protección y respeto de los derechos humanos, incluyendo el derecho a la privacidad, y si participa en foros o mecanismos orientados a promover estos derechos en el ámbito de sus responsabilidades empresariales.





También se considera si la empresa ha intervenido, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante entidades reguladoras para defender el derecho a la privacidad, así como si ha tomado medidas legales para proteger la privacidad de sus usuarios y usuarias.

Asimismo, se evalúa si la empresa lleva a cabo actividades como campañas de sensibilización, jornadas informativas o acciones publicitarias destinadas a concientizar sobre la importancia de la privacidad y los derechos digitales. Este criterio busca medir el compromiso integral de la empresa con la privacidad desde distintas perspectivas.

Criterios de evaluación

- I. Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales;
- II. Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales;
- III. Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales;
- IV. 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, Telecommunications Industry Dialogue, Pacto Global).

Estándar de desempeño:

Estrella llena		La ISP cumple con tres o todos los criterios
Media estrella		La ISP cumple con dos criterios
Un cuarto de estrella		La ISP cumple con un criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS



CLARO - AMX PARAGUAY S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	No
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		•
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	•	
Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales.		•
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, Telecommunications Industry Dialogue, Pacto Global).	•	

Sobre el primer criterio a considerar, la ISP participó en la aprobación del reglamento de protección al usuario de telecomunicaciones con CONATEL aprobado en el 2016. Más allá de esta iniciativa, no se han identificado otras acciones políticas o legales públicas que busquen proteger la privacidad de las personas usuarias en el ámbito legislativo. Tampoco hay indicios de que la empresa haya impugnado judicialmente solicitudes de información que pudieran ser excesivas o no ajustarse a los requisitos legales.

Aunque la compañía ha participado en consultas y audiencias públicas relacionadas con datos personales, contenidos nocivos en internet y ciberseguridad, no se ha observado un posicionamiento público definido sobre su incidencia en la elaboración de estas normativas.

La ISP, en su página web, no presenta referencias a actividades o contenidos que aborden específicamente la protección de datos personales. Sin embargo, en el código de ética de América Móvil, al cual la empresa se adhiere como subsidiaria y pone disponible desde su página web⁷⁵, se compromete a proteger y respetar los derechos humanos, incluyendo campañas de concientización sobre estos principios.

Aunque no se identificaron menciones directas en la web de la empresa, el informe de sustentabilidad,⁷⁶ indica también que América Móvil proporciona certificaciones y capacitaciones a sus empleados en temas relacionados con el manejo de datos personales y seguridad digital. Adicionalmente, la subsidiaria en Paraguay ha lanzado una campaña de “Seguridad digital” en su perfil de Instagram⁷⁷, presentando una Guía de Seguridad Digital para usuarios, aunque la visibilidad de esta información puede ser limitada debido a su disposición en la red social. En ese sentido, consideraremos como cumplido el segundo criterio, aunque recomendaremos más adelante mejorar ciertos aspectos puntuales.

En cuanto al último criterio, la ISP colabora con otros miembros del sector por lo que puntúa positivamente. En el marco de iniciativas de la GSMA (Groupe Speciale Mobile Association), por ejemplo, insta a los participantes del sector de las telecomunicaciones a informar sobre emisiones y establecer objetivos ambiciosos de reducción. Además, como parte de su estrategia de sustentabilidad, la empresa trabaja con asociaciones y organizaciones para alcanzar metas alineadas con iniciativas globales como los Objetivos de Desarrollo Sostenible (ODS), los Diez Principios del Pacto Mundial y la campaña Ambición Empresarial de las Naciones Unidas para 1.5 °C. En Paraguay, colabora con diversas entidades, incluyendo la Cámara de Operadores Móviles del Paraguay (COMPY) y la Red Paraguaya de Empresas Inclusivas (RPEI).

Conforme a lo expresado, Claro cumple con dos de los cuatro criterios establecidos, por lo que califica con media estrella.



75 Claro. Código de Ética: <https://landing.claro.com.ar/p/pdf/claro-codigo-etica.pdf>

76 América Móvil. Informe de Sustentabilidad 2023. Recuperado de <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

77 Claro Paraguay. Recuperado de <https://www.instagram.com/claropy?igsh=MW0wchM5a3RydXA4Nw==>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	No
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		•
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	•	
Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales.		•
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, Telecommunications Industry Dialogue, Pacto Global).		•

COPACO cuenta con iniciativas promovidas sobre temas de seguridad digital en su página web y redes sociales bajo “Che mba’e: mis datos, mi seguridad”, proporcionando contenido educativo dirigido a sus usuarios y usuarias. En ese contexto, consideraremos cumplido el criterio 2.

Sin embargo, no se observa información que cumpla con los demás criterios considerados. En las ediciones de 2017 y 2020 se observó que COPACO participó activamente en los Foros de Gobernanza de Internet en su capítulo paraguayo. Sin embargo, esta participación cesó y no se identificaron otras acciones relacionadas con la gobernanza ni con la defensa de los derechos de las personas usuarias. En consecuencia, al contar con 1 de 4 criterios, se la califica con un cuarto de estrella.



Personal

PERSONAL - NÚCLEO S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	No
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		•
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	•	
Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales.		•
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, Telecommunications Industry Dialogue, Pacto Global).	•	

En la página web de la empresa no se observa que tome públicamente un compromiso con la promoción y protección de derechos humanos, compromiso que si se observa por ejemplo al revisar la página de su par internacional⁷⁸.

Por otro lado, la ISP también colaboró en el proceso de aprobación del reglamento de protección al usuario de telecomunicaciones con CONATEL en 2016. Más allá de dicha iniciativa, no se encontraron otras iniciativas políticas o legales públicas que busquen proteger la privacidad de las personas usuarias ante el Poder Legislativo. Tampoco se observa que la ISP refiera haber resistido vía judicial a solicitudes de información excesivas o que no cumplan con los requisitos legales. Aunque ha participado de consultas y audiencias públicas sobre normativas relacionados con datos personales, contenidos nocivos en internet y políticas de ciberseguridad, no se han encontrado posicionamientos públicos claros a favor o en contra de estas regulaciones. Esta falta de posicionamiento público podría interpretarse como una falta de compromiso activo en la defensa de la privacidad y los derechos digitales de sus usuarios.

Asimismo, se evidencian esfuerzos orientados a educar y capacitar a la sociedad en temas relacionados con la protección de datos personales y seguridad digital⁷⁹. Además, la empresa es miembro participante de la iniciativa GSMA⁸⁰. De esta manera, al igual que en la edición anterior, cumple con los criterios segundo y cuarto, por lo que puntúa con media estrella.



78 TELECOM Argentina. Recuperado de <https://institucional.telecom.com.ar/sustentabilidad>

79 Personal. Blog. Recuperado de <https://blog.personal.com.py>

80 GSMA. Memberships. Recuperado de <https://www.gsma.com/get-involved/gsma-membership/our-members/>



TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Políticas de promoción y defensa de los derechos humanos		
	Sí	No
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		•
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	•	
Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales.	•	
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, Telecommunications Industry Dialogue, Pacto Global).	•	

Se destaca que la empresa Tigo ha tenido participación pública en diversas iniciativas legislativas relacionadas con la tecnología. Según los informes de 2017 y 2020, Tigo formó parte de grupos de análisis legislativo enfocados en la ley de “Protección de niños y adolescentes contra contenido dañino en Internet”. Asimismo, la empresa colaboró en grupos de trabajo para la elaboración del Plan Nacional de Ciberseguridad. Además, Tigo figura como una de las ISP que participaron activamente en el proceso de aprobación del reglamento de protección al usuario de telecomunicaciones en conjunto con CONATEL en 2016. Asimismo, la ISP informa que, en el marco de sus compromisos sociales, colabora con CONATEL y el Gobierno Nacional para expandir la conectividad a todos los puntos del país⁸¹. No obstante, no se identificaron iniciativas políticas o legales dirigidas a proteger la privacidad de sus usuarios y usuarias ante el Poder Legislativo en lo que respecta al 2023 y 2024.

Si bien Millicom⁸² destacó su prioridad para el año 2024 de aumentar su involucramiento con las autoridades de los distintos países en los que opera para contribuir a la definición de, por ejemplo, leyes de vigilancia claras, transparentes y efectivas con garantías adecuadas, queda pendiente evaluar si esta prioridad se reflejó también en la subsidiaria Tigo Paraguay.

81 Tigo. Compromisos Sociales: <https://www.tigo.com.py/conocenos/compromisos-sociales>

82 Millicom. Reporte LED Millicom 2023. pág 15.

Con relación al segundo criterio, en el reporte anual 2023⁸³ Millicom alega que tanto el grupo como sus subsidiarias, siguiendo los principios de las Naciones Unidas y otros estándares internacionales, promueven activamente los derechos humanos, incluida la privacidad y la libertad de expresión. Esto también se evidencia en la página web de Tigo Paraguay, en el apartado de responsabilidad corporativa⁸⁴. Se observa también en los informes del 2020 y 2022 que participa del Pacto Global de la ONU, así como del Telecommunications Industry Dialogue. Además, tiene iniciativas específicas, como “Conectadas” y “Maestros conectados” dirigidas a capacitar a mujeres emprendedoras, a maestros y maestras del país en herramientas digitales.

Respecto al tercer criterio, cabe mencionar que en el ya citado informe de sustentabilidad 2023, Millicom informa que implementa medidas para evaluar la legalidad de las solicitudes de información antes de proporcionar a las autoridades y cuenta con mecanismos para presentar quejas ante la Corte Suprema de Justicia en caso de considerar que las órdenes o interceptaciones no cumplen con los requisitos legales.

En cuanto al cuarto criterio, la ISP está también involucrada en la GSMA⁸⁵, organización global que impulsa la innovación en el ecosistema móvil para favorecer entornos empresariales positivos y cambios sociales.

En el informe 2022, se destacó la presencia de Millicom como miembro de Global Network Initiative (GNI), sin embargo desde el 2023, esta empresa decidió retirarse y solo concentrarse en la GSMA.

En suma, se observa que ésta ISP cumple con tres de los cuatro criterios establecidos en el estándar de desempeño, por lo que amerita calificarla con una estrella.



83 Millicom. Annual Report 2023. Recuperado de: <https://www.millicom.com/media/5769/ar-2023-w-mic-sa.pdf>

84 Tigo. Responsabilidad Corporativa. Recuperado de <https://www.tigo.com.py/conocenos/responsabilidad-corporativa>

85 GSMA. Memberships. Recuperado de <https://www.gsma.com/get-involved/gsma-membership/our-members/>



VOX - HOLA PARAGUAY S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	No
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		•
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.		•
Si la empresa resiste a través de la vía judicial las solicitudes de información que sean excesivas y no cumplan con los requisitos legales.		•
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, Telecommunications Industry Dialogue, Pacto Global).	•	

Vox solo cumple con el último de los tres criterios observados dado que participa en la iniciativa GSMA⁸⁶, cumpliendo con un criterio de los cuatro establecidos. También se analizaron las ediciones anteriores de esta investigación y no se evidenció la participación ni la realización de acciones públicas en defensa de los derechos de las personas usuarias. En consecuencia, califica con un cuarto de estrella.



86 GSMA. Memberships. Recuperado de <https://www.gsma.com/get-involved/gsma-membership/our-members/>

CRITERIO 5. Transparencia




¿Publica la ISP informes de transparencia que contienen información sobre cuántas veces los gobiernos han solicitado datos de sus usuarios y usuarias y, la frecuencia con que la empresa proporcionó esos datos a los gobiernos?

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.

Criterios de evaluación

- I. La ISP publica informes de transparencia para que la persona usuaria pueda enterarse de la colaboración con las autoridades gubernamentales sobre los datos proveídos;
- II. La ISP publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando:
 - a. la cantidad de solicitudes y divulgaciones clasificadas 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.

Estándar de desempeño:

Estrella llena		La ISP cumple con ambos criterios
Media estrella		La ISP cumple con uno de los criterios
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - TRANSPARENCIA



CLARO - AMX PARAGUAY S.A.

Transparencia		
	Sí	No
La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales.	•	
La ISP 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.		•

Al igual que lo observado en la edición anterior, Claro Paraguay persiste en la falta de informes específicos sobre su colaboración con autoridades gubernamentales. Por otro lado, cabe señalar que se evidencia un convenio en 2018 con la Corte Suprema de Justicia⁸⁷, estableciendo mecanismos tecnológicos para el acceso a la información generada por AMX Paraguay, esta información no está en la página web de la ISP, y se carece de detalles sobre la vigencia del convenio.

La principal dificultad radica en que la información relevante solo puede obtenerse a través del Informe de Sustentabilidad disponible en el sitio web de América Móvil, lo que obliga a consultar la página de la empresa matriz, ya que no está accesible en la de la subsidiaria. A pesar de esta limitación, dicho informe constituye la única fuente de información disponible para evaluar a la ISP en este criterio, por lo que tomaremos en cuenta lo allí presentado.

87 Poder Judicial. Noticias. 12 de marzo de 2018. <https://www.pj.gov.py/notas/15105-convenio-entre-amx-paraguay-y-la-corte-suprema-de-justicia>

En su Informe de Transparencia en las Comunicaciones 2023⁸⁸, citado más arriba, América Móvil informa que su subsidiaria en Paraguay se encuentra obligada a colaborar con las autoridades de seguridad nacional y procuración de justicia en virtud de normas constitucionales y otras leyes y normas reglamentarias. Asimismo, a diferencia de años anteriores, la empresa matriz indicó que las subsidiarias recibieron 810.956 solicitudes en sus filiales, incluyendo un desglose de la información por países. En ese sentido, se considera cumplido el primer criterio.

Un avance significativo de esta empresa se evidencia al comparar las primeras ediciones de QDTD con las más recientes. En la primera y segunda edición no se incluía información relevante ni en la casa matriz. Sin embargo, a partir de los informes de 2022, América Móvil comenzó a publicar reportes de transparencia sobre sus subsidiarias en América Latina. Estas publicaciones se presentan en bloques regionales, y a partir del 2023, se discriminan también la cantidad de solicitudes por países.

Con relación al segundo criterio, la empresa tampoco satisface éste, ya que el único informe localizado no detalla la colaboración con el gobierno. Considerando este desempeño, corresponde calificar a esta ISP con media estrella, ya que cumple con uno de los criterios evaluados.



88 América Móvil. Informe de Transparencia en las Comunicaciones 2023. Recuperado de <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Transparencia		
	Sí	No
La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales.		•
La ISP 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.		•

La ISP no cumple con ninguno de los criterios establecidos. No publica informes de transparencia que detallen la colaboración con autoridades gubernamentales, la clasificación por tipo de datos, la autoridad solicitante y la motivación alegada.

COPACO facilita en su página web una lista de entes gubernamentales con las que celebró convenios hasta el 2022⁸⁹, entre los que se incluyen a la Corte Suprema de Justicia, el Poder Judicial y el Ministerio Público. Sin embargo, no es posible acceder a mayores detalles sobre el alcance de estos convenios, imposibilitando considerar esta información para evaluar el criterio número uno. Asimismo, en la sección de noticias de su sitio web y mediante búsquedas en Google se halla información reciente acerca de acuerdos con entidades gubernamentales como la Administración Nacional de Electricidad (ANDE)⁹⁰ y la Dirección Nacional de Migraciones⁹¹, pero estos parecen centrarse más en la mejora de la conectividad que en el intercambio de información o datos personales de sus usuarios y usuarias. Tampoco se observan en las ediciones anteriores de QDTD que esta empresa haya cumplido alguna vez con este criterio.

En conclusión, COPACO no cumple con ninguno de los criterios establecidos, por lo que no recibe ninguna estrella en cuanto al criterio de transparencia.



89 COPACO. Institucional. Transparencia. Ley 5282/14. Recuperado de <https://www.copaco.com.py/index.php/institucional/transparencia/ley-5282-14.html>

90 COPACO. Noticias. Recuperado de <https://www.copaco.com.py/index.php/cooperacion-interinstitucional.html>

91 Dirección Nacional de Migraciones. Noticias. Recuperado de <https://www.migraciones.gov.py/index.php/noticias/migraciones-y-copaco-dan-continuidad-al-acuerdo-para-provision-de-servicios-de-comunicacion-de-datos>

Personal

PERSONAL - NÚCLEO S.A.

Transparencia		
	Sí	No
La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales.	•	
La ISP 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.		•

Personal no cuenta con informes sobre su colaboración con el gobierno en su página web y tampoco se identifica ningún informe relevante en las herramientas de búsqueda en Internet. Esta ausencia de documentación se identificó en ediciones anteriores de QDTD correspondientes al 2017, 2020 y 2022, dificultando la evaluación de su desempeño en términos de protección de la privacidad y colaboración con autoridades gubernamentales, lo que justifica la conclusión de que la ISP no cumple con los criterios establecidos en el estándar de desempeño. A este respecto, Personal no califica en el criterio de transparencia.





TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Transparencia		
	Sí	No
La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales.	•	
La ISP 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.		•

En relación con el primer criterio, es relevante destacar que esta ISP nuevamente obtiene puntuación gracias a que su empresa matriz proporciona un informe sobre la colaboración con las autoridades gubernamentales en el Reporte LED Millicom 2023 ya mencionado más arriba.

El mentado informe indica que América del Sur, incluyendo a Bolivia, Colombia y Paraguay, recibió 414 órdenes de intervención en comunicaciones, 475 solicitudes de información sobre datos de servicios de pago móvil (MFS) y 45.277 solicitudes de informe sobre metadatos de usuarios y usuarias en 2023⁹². Si bien es destacable que la información sobre las solicitudes de interceptación de comunicaciones, acceso a metadatos y datos de MFS, el reto principal persiste en la falta de diferenciación por país. Por tanto, no es posible saber con certeza los números de solicitudes que corresponden a Paraguay.

Esta dificultad de acceso ya había sido identificada en informes anteriores, aunque con algunas variaciones. En 2017 el informe era publicado exclusivamente en inglés desde la matriz de la empresa Millicom y contenía información limitada omitiendo datos clave como volúmenes, origen, motivos y alcance de las solicitudes. En los informes de 2020 y 2022 se introdujeron algunos datos adicionales, sin embargo, estos no estaban desglosados por país sino únicamente por región. Esta práctica se ha mantenido presentando datos agrupados de manera general lo cual resulta en una persistente carencia de información específica y detallada por país. Esto limita la transparencia y dificulta una comprensión completa de las operaciones a nivel local. En relación con el segundo criterio, a pesar de la información proporcionada, no se puede considerar como cumplido, ya que no se presenta un desglose detallado que satisfaga los requisitos específicos de este criterio.

Entonces, Tigo cumple con uno de los dos criterios observados, por lo que califica con media estrella.



92 Millicom. Reporte LED Millicom 2023. pág 7.



VOX - HOLA PARAGUAY S.A.

Transparencia		
	Sí	No
La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales.		•
La ISP 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.		•

Al igual que en ediciones anteriores, se evidencia que Vox no presenta informes en su sitio web que aborden su colaboración con el gobierno. Tampoco existe información al respecto en los motores de búsqueda de Internet. Debido a la ausencia de documentación que cumpla con los criterios establecidos en el estándar de desempeño, la ISP no satisface ninguno de los criterios evaluados.



CRITERIO 6. Guías para la solicitud de información personal





Proporciona la ISP información clara y completa sobre los lineamientos, guías o protocolos orientados a las fuerzas de seguridad y otros organismos gubernamentales que expliquen cómo deben solicitar la información personal de sus clientes?, ¿cuáles son las condiciones para la entrega de dicha información personal?

Se evaluará si la ISP cuenta con los lineamientos, guías y protocolos que buscan determinar cómo cada empresa establece la forma en colaboración con el Estado. Ya sea por entregar información al sistema de persecución penal u otro tipo de investigación y, en su caso, qué especificaciones deben cumplir a dicho efecto. También se evalúa si la empresa, al momento de establecer sus propias reglas para las autoridades locales, tiene en cuenta el contexto nacional o si los lineamientos preestablecidos responden a procedimientos foráneos, y en tal caso corroborar si los mismos son más rigurosos a favor de la privacidad de sus usuarios y usuarias.

Criterios de evaluación

- I. Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes;
- II. Si los lineamientos, guías o protocolos se encuentran disponibles públicamente;
- III. Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.

Estándar de desempeño:

Estrella llena		La ISP cumple con todos los criterios
Media estrella		La ISP cumple con dos de los criterios
Un cuarto de estrella		La ISP cumple con uno de los criterios
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - GUÍAS PARA LA SOLICITUD DE INFORMACIÓN PERSONAL



CLARO - AMX PARAGUAY S.A.

Guías para la solicitud de información personal		
	Sí	No
Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes.	•	
Si los lineamientos, guías o protocolos se encuentran disponibles públicamente.	•	
Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.	•	

Similar a la circunstancia mencionada en nuestra edición anterior, Claro sigue sin facilitar información relevante para evaluar este criterio en su página web. Los protocolos para gestionar solicitudes de datos con los que cuenta se encuentran disponibles en la página de la empresa matriz, América Móvil.

Estos protocolos, detallados en el Informe de Transparencia en las Comunicaciones⁹³, abordan políticas legales y obligaciones aplicables en los países donde opera, incluido Paraguay. América Móvil, además, cuenta con una política de privacidad que establece los derechos de los titulares y proporciona pautas generales para los requerimientos gubernamentales. Se concluye que la ISP satisface los criterios relativos a protocolos de manejo de datos y su disponibilidad pública a través de su matriz. No obstante, sería deseable que esta información estuviera accesible directamente desde la página web de Claro.

En suma, Claro cumple con los tres criterios aquí considerados, por lo que califica con una estrella.



93 América Móvil. Informe de Transparencia en las Comunicaciones 2023. Recuperado de <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Guías para la solicitud de información personal		
	Sí	No
Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes.		•
Si los lineamientos, guías o protocolos se encuentran disponibles públicamente.		•
Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.		•

La ISP no proporciona lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de las personas. Aunque cuenta con un protocolo detallado para solicitar información pública conforme a la Ley Nº 5282/2014, de Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental, este no está orientado a guías específicas para fuerzas de seguridad u organismos gubernamentales. Dado que COPACO no satisface ninguno de los puntos aquí evaluados, no califica para el criterio de solicitud de información personal.



Personal

PERSONAL - NÚCLEO S.A.

Guías para la solicitud de información personal		
	Sí	No
Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes.		•
Si los lineamientos, guías o protocolos se encuentran disponibles públicamente.		•
Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.		•

La ISP no proporciona información clara y completa sobre los lineamientos, guías o protocolos dirigidos a las fuerzas de seguridad y otros organismos gubernamentales para solicitar información personal de los clientes.

Sin embargo, cabe mencionar que a través de una búsqueda en Google se encontró una noticia sobre un convenio entre la Corte Suprema de Justicia (CSJ) y Núcleo SA suscrito en el 2022 que tendrá una duración de cinco años⁹⁴. Según la información disponible, el convenio tiene como finalidad establecer mecanismos tecnológicos para que la CSJ acceda a datos generados por la ISP. El acuerdo destaca la utilización de oficios electrónicos en lugar de documentos escritos. Además, se establecen requisitos específicos para los oficios electrónicos enviados a la ISP, incluyendo la atención a plazos reglamentarios vigentes. También se subraya que la responsabilidad sobre la información entregada recae exclusivamente en el funcionario solicitante eximiendo a la ISP de cualquier responsabilidad legal por el manejo incorrecto de la información.

Dada la limitada información proporcionada y la falta de detalles específicos, especialmente la ausencia de la documentación del convenio y su no disponibilidad en la página de la ISP resulta difícil evaluar completamente los puntos establecidos para este criterio. Conforme con el estándar de desempeño la ISP califica sin puntuación alguna.



94 Poder Judicial. Notas. 19 de diciembre de 2022. Recuperado de <https://www.pj.gov.py/notas/23325-corte-suprema-y-nucleo-sa-suscribieron-convenio-a-fin-de-fortalecer-el-oficio-electronico>



TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Guías para la solicitud de información personal		
	Sí	No
Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes.	•	
Si los lineamientos, guías o protocolos se encuentran disponibles públicamente.	•	
Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.	•	

Según la información disponible en la página web de la ISP esta no presenta lineamientos específicos para el manejo de solicitudes de datos personales por parte de fuerzas de seguridad u organismos gubernamentales.

Sin embargo, podemos observar información relevante en el Reporte LED Millicom 2023. En el documento se detallan lineamientos y protocolos generales sobre cómo gestionan requerimientos de información por parte de autoridades, aunque dichos protocolos se encuentran únicamente disponibles en la versión en inglés⁹⁵. Si bien la barrera del idioma podría dificultar la comprensión completa de los documentos, adoptaremos una posición flexible al reconocer la existencia de este lo cual nos permite otorgar una calificación positiva respecto al segundo y tercer criterio de evaluación. Conforme al estándar de desempeño establecido Tigo cumple con los tres criterios evaluados por lo que califica con una estrella.



95 Millicom. Compliance and Business Ethics. Policies and Guiding Principles. Law Enforcement and Major Events Guidelines. Recuperado de <https://www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf>



VOX - HOLA PARAGUAY S.A.

Guías para la solicitud de información personal		
	Sí	No
Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes.		•
Si los lineamientos, guías o protocolos se encuentran disponibles públicamente.		•
Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.		•

Vox tampoco cumple con este criterio, ya que no proporciona información clara y completa sobre los lineamientos, guías o protocolos orientados a las fuerzas de seguridad y otros organismos gubernamentales, ni detalla las condiciones para la entrega de información personal de los clientes.

Considerando el estándar de puntuación, la ISP no recibe calificación alguna en este aspecto.



CRITERIO 7. Accesibilidad




¿Posee la ISP un sitio web con una interfaz con información perceptible y comprensible, navegación funcional y operable con relación a políticas de privacidad, términos y condiciones de sus productos y servicios?

Se evalúa si la ISP cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, si tiene una interfaz navegable y funcional, con información comprensible y compatible con herramientas de la persona usuaria en relación con el contenido sobre políticas de privacidad y términos y condiciones de sus productos y servicios.

Criterios de evaluación

- I. La ISP tiene una interfaz de sitio Web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función;
- II. La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado;
- III. La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible;
- IV. El contenido en el sitio Web de la ISP es compatible con las herramientas actuales de la persona usuaria (diferentes navegadores, tecnologías de apoyo y otros agentes de la persona usuaria).

Estándar de desempeño:

Estrella llena		La ISP cumple con tres o todos los criterios
Media estrella		La ISP cumple con dos de los criterios
Un cuarto de estrella		La ISP cumple con uno de los criterios
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - ACCESIBILIDAD



CLARO - AMX PARAGUAY S.A.

Accesibilidad		
	Sí	No
La compañía tiene un sitio web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función.	•	
La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado.		•
La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible.		•
El contenido en el sitio Web de la compañía está diseñado contemplando una diversidad de herramientas (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

En cuanto a la accesibilidad, la ISP no logró mejorar su estándar de cumplimiento desde la última evaluación. Es cierto que Claro proporciona documentos de “Términos y Condiciones de Uso” y “Políticas de Privacidad” para varios servicios, los cuales se encuentran disponibles a través de un enlace en la parte inferior de la página principal⁹⁶. Sin embargo, acceder a estos documentos requiere navegar a través de varias páginas o utilizar filtros lo que puede resultar complicado sobre todo para personas usuarias de lectores de pantalla. Al intentar acceder a los documentos se observa una tabulación muy extensa y la navegación con teclado resulta difícil.

Aunque al acceder a cada documento se observa buen contraste y redimensionamiento de texto, lo que se ajusta al primer criterio de accesibilidad, la navegación en general carece de previsibilidad y accesibilidad completa, lo que incumple los criterios dos y tres.

96 Claro. Legal y Regulatorio. Recuperado de <https://www.claro.com.py/personas/legal-y-regulatorio>

Aunque se destaca nuevamente la opción que ofrece Claro de facilitar facturas en braille a las personas usuarias que así lo requieran⁹⁷, la accesibilidad general del sitio es limitada y se debe paginar seis veces para acceder a la información que refiere el procedimiento de solicitud de este tipo de facturas. Igualmente, cabe recordar que mucha información relevante para esta investigación no está directamente disponible en la página de la ISP, habiendo tenido que recurrir a la página de la empresa matriz.

La evaluación de la página web utilizando herramientas como WAVE⁹⁸ y TAW⁹⁹ revelan varios otros problemas de accesibilidad. Por citar algunos, si bien la estructura de pestañas sigue un orden lógico, se identificaron preocupaciones como la falta de etiquetas en formularios que puede complicar la comprensión y navegación para usuarios de lectores de pantalla. La presencia de botones vacíos afecta la información proporcionada a aquellos que utilizan tecnologías de apoyo. En general, también se encuentran problemas de contraste que podrían afectar la legibilidad del texto, especialmente para usuarios con baja visión.

Se identificó también la presencia de texto subrayado que puede causar confusión, ya que comúnmente se asocia con enlaces. Además, se detectó texto redundante en ciertos atributos lo cual podría afectar la claridad y comprensión del contenido. La falta de atributos “aria-label” o “aria-labelledby” en ciertos elementos y problemas con la designación del idioma también se prestan a mejoras. Considerando ello, si bien se contemplan diferentes navegadores y diversidad de dispositivos el sitio no es adecuado para el uso de tecnologías de apoyo como lectores de pantalla, incumpliendo así con el cuarto criterio.

En resumen, la página web enfrenta desafíos de accesibilidad significativos que podrían perjudicar la experiencia de las personas usuarias, especialmente de aquellas con discapacidades. Por lo que, al cumplir solo con un criterio de los evaluados, Claro califica con un cuarto de estrella.



97 Claro. Legal y Regulatorio. Otro. Factura Braille. Recuperado de <https://www.claro.com.py/personas/legal-y-regulatorio/factura-braille>

98 Web Accessibility Tool. Recuperado de <https://wave.webaim.org>

99 TAW. Recuperado de <https://www.tawdis.net/resumen>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Accesibilidad		
	Sí	No
La compañía tiene un sitio web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función.	•	
La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado.		•
La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible.	•	
El contenido en el sitio Web de la compañía está diseñado contemplando una diversidad de herramientas (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

Primeramente, cabe señalar que COPACO no garantiza acceso a información fehaciente mediante la inclusión de términos y condiciones claros en su página web, así como un aviso de privacidad completo que cubra todos los servicios que ofrece.

En cuanto a la página web de la empresa y considerando el primer criterio evaluado, se debe señalar que aunque se encontraron sugerencias de mejora según las herramientas de accesibilidad utilizadas como WAVE¹⁰⁰ y TAW¹⁰¹, la información general del sitio web es perceptible y se pueden acceder a los diferentes componentes de la interfaz de usuario. Además, los colores de fondo y primer plano tienen una relación de contraste suficiente y cuenta con tamaño de textos normales. Por lo tanto, se considera, en términos generales, que este criterio está cumplido.

En relación con el segundo aspecto evaluado, la navegación mediante teclado es posible, sin embargo, se identifican deficiencias que afectan la funcionalidad como la falta de una jerarquía clara en los encabezados y la ausencia de etiquetas descriptivas que dificultan la navegación y comprensión del contenido. Igualmente, algunos enlaces no proporcionan información clara sobre su función o destino. Por lo mismo, este criterio no se cumple.

100 WAVE. Reporte: <https://wave.webaim.org/report#/https://www.copaco.com.py>

101 TAW. Resumen de consulta: <https://www.tawdis.net/resumen>

Sobre el tercer aspecto estudiado cabe referir que, aunque se encontraron algunas advertencias relacionadas con la falta de textos alternativos, la información en el sitio web es comprensible y opera de manera predecible para los usuarios. Aunque se encontraron algunas advertencias relacionadas con la falta de textos alternativos, el contenido es legible y el sitio funciona de manera coherente. Por lo tanto, este criterio se considera cumplido.

Ahora bien, se identificaron problemas significativos en cuanto a la navegabilidad del sitio web, especialmente relacionados con enlaces que carecen de texto que identifique claramente su propósito y la falta de textos alternativos en imágenes. Estos problemas indican que el diseño del sitio web no contempla adecuadamente la diversidad de herramientas y agentes de usuario, lo que puede afectar negativamente a personas que dependen de tecnologías de asistencia. Por lo tanto, este criterio no se considera cumplido.

Considerando lo anterior, COPACO cumple con dos de los cuatro criterios analizados, por lo que califica con media estrella.



PERSONAL - NÚCLEO S.A.

Accesibilidad		
	Sí	No
La compañía tiene un sitio web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función.	•	
La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado.		•
La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible.	•	
El contenido en el sitio Web de la compañía está diseñado contemplando una diversidad de herramientas (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

Tomando en consideración los informes de las herramientas de accesibilidad WAVE¹⁰² y TAW¹⁰³, así como la verificación manual de la página web de la ISP, se considera que este criterio se cumple ya que el sitio web presenta una interfaz escalable con tamaños de textos adecuados y una correcta identificación del idioma facilitando la percepción de la información. Sin embargo, no podemos dejar de mencionar que se encontraron varios problemas que requieren atención, como la ausencia de textos alternativos en imágenes y otros contenidos no textuales, que impide que personas usuarias de tecnologías asistivas accedan plenamente al contenido.

Respecto del segundo criterio evaluado, aunque el sitio permite la navegación mediante teclado, se identificaron obstáculos que afectan la funcionalidad, como la ausencia de una estructura clara de encabezados y etiquetas que dificulta la navegación secuencial y la comprensión del contenido. Asimismo, algunos enlaces carecen de descripciones contextuales claras, lo que puede confundir a los usuarios sobre su función o destino. Dadas estas deficiencias, este criterio no se considera cumplido.

El tercer criterio aquí evaluado también se considera cumplido, ya que el contenido aparece de predecible, con texto legible y comprensible, y el idioma principal identificado como español. No obstante, sugerimos atención a esta área debido a que se observaron algunas dificultades relacionadas con la falta de asistencias específicas para los usuarios, como instrucciones claras o ayudas contextuales, que puede afectar la experiencia de usuarios con discapacidades cognitivas o aquellos no familiarizados con la interfaz.

102 WAVE: <https://wave.webaim.org/report#/https://www.personal.com.py/index.html>

103 Taw: <https://www.tawdis.net/resumen>

Por último, se detectaron problemas que afectan la compatibilidad con tecnologías de asistencia. En este contexto, se identificó una jerarquía inadecuada de encabezados que dificulta la navegación mediante lectores de pantalla, así como múltiples alertas de bajo contraste, lo que puede impedir la lectura del texto a personas con dificultades visuales. Estos problemas indican que el sitio no está completamente diseñado considerando la diversidad de herramientas de apoyo y navegadores, lo que se sugiere como un área relevante de mejora.

La ISP cumple con dos de los cuatros criterios evaluados por lo que califica con media estrella.





TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Accesibilidad		
	Sí	No
La compañía tiene un sitio web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función.	•	
La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado.	•	
La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible.	•	
El contenido en el sitio Web de la compañía está diseñado contemplando una diversidad de herramientas (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).	•	

La compañía cumple con el primer criterio de accesibilidad ya que su sitio web cuenta con un fácil acceso a documentos desde la página, como: términos y condiciones, aviso de privacidad e incluso el contrato de suscripción de servicios de telecomunicaciones. Los primeros dos documentos mencionados tienen textos que pueden ser redimensionados y adaptados, garantizando una buena percepción de la información y cumpliendo con el principio de equivalencia de contenido.

En relación con el segundo criterio se determina que la ISP cumple con la accesibilidad para navegación con teclado. La portada del sitio web funciona correctamente y permite desplazamientos y acercamientos con el teclado sin inconvenientes. Aunque se identifican algunas áreas de mejora en la estructuración de encabezados y el orden de tabulación, el carrusel también es navegable por teclado, lo que garantiza una experiencia funcional para usuarios con necesidades de accesibilidad.

La ISP también cumple con el tercer criterio ya que el texto del sitio web es legible y comprensible y el contenido aparece y opera de forma predecible. Esto garantiza una buena experiencia de usuario y facilita la comprensión de la información presentada en el sitio.

En cuanto al cuarto criterio se determina que la compañía lo cumple ya que su sitio web está diseñado considerando una diversidad de herramientas y agentes de usuario. Se realizaron pruebas con lector de pantalla y se encontraron alternativas textuales en la mayoría de los contenidos multimedia. Aunque las

herramientas de accesibilidad utilizadas, como WAVE¹⁰⁴ y TAW¹⁰⁵, para evaluar la página web de la ISP identificaron algunos errores relacionados con el contraste y la definición de textos alternativos en ciertos íconos, estos errores no superan más de cuatro, cumpliendo el sitio web con los estándares de accesibilidad.

Tigo cumple con los cuatro criterios de accesibilidad, garantizando una experiencia positiva para todas las personas usuarias, incluyendo aquellas con necesidades especiales de acceso a la información. Por ello, califica con una estrella.



104 WAVE: <https://wave.webaim.org/report#/https://www.tigo.com.py>

105 TAW. Resumen: <https://www.tawdis.net/resumen>



VOX - HOLA PARAGUAY S.A.

Accesibilidad		
	Sí	No
La compañía tiene un sitio web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función.		•
La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado.		•
La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible.		•
El contenido en el sitio Web de la compañía está diseñado contemplando una diversidad de herramientas (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

La compañía no cumple con el primer criterio de accesibilidad ya que su sitio web presenta problemas significativos relacionados con la perceptibilidad de la información y los componentes de la interfaz de usuario. Por otro lado, la página web no tiene disponible información relevante sobre los términos y condiciones o la política de privacidad, puntos que ya fueron advertidos en la edición anterior de esta investigación.

La ISP tampoco cumple con el segundo criterio. Si bien cuenta con soporte de teclado, la página web presenta varios problemas de navegación que afectan la funcionalidad y la usabilidad para usuarios que dependen del teclado o herramientas de asistencia como la falta de varios encabezados y etiquetas. Aunque la interfaz es funcional en general, los problemas identificados impactan negativamente en la experiencia del usuario.

En cuanto al tercer criterio, en esta ocasión se ha mejorado la identificación del idioma de la página según se valida con el reporte de TAW¹⁰⁶ aunque aún persisten problemas como la falta de definiciones para palabras poco comunes o del idioma guaraní utilizadas. Además, no se ofrece asistencia a los usuarios para algunos elementos desplegable no estándar, ni para prevenir y corregir errores. Se observa que algunas páginas aún no están finalizadas a pesar de estar vinculadas en el menú principal del sitio,

106 TAW. Resumen: <https://www.tawdis.net/resumen>

un problema que persiste desde la edición anterior de esta investigación¹⁰⁷. Aunque el contenido del sitio web es legible y comprensible en términos generales, los problemas de navegabilidad e incluso la ausencia de numerosos textos alternativos¹⁰⁸ dificultan la operación predecible del sitio, pudiendo generar confusión en la experiencia del usuario al interactuar con el contenido.

Finalmente, la ISP tampoco cumple con el cuarto criterio ya que los problemas de navegabilidad, adaptabilidad y contraste afectan la accesibilidad del sitio en diferentes navegadores, tecnologías de apoyo y agentes de usuario. La diversidad de herramientas no está contemplada adecuadamente en el diseño del sitio afectando negativamente la experiencia del usuario.

En suma, Vox no cumple con ninguno de los criterios establecidos, por lo que no recibe ninguna estrella.



107 Igual que lo reportado en el 2022, al intentar ingresar a la página de “TELEFONOS” (sic) que está en el menú principal lleva a una página “en construcción”. Recuperado de <https://www.vox.com.py/telefonos>

108 WAVE. Recuperado de <https://wave.webaim.org/report#/https://www.vox.com.py>

CONCLUSIÓN

Desde las primeras ediciones se ha observado una diferencia sustancial entre las empresas proveedoras de Internet nacionales y aquellas que operan como subsidiarias de empresas extranjeras. Empresas como Claro, Personal y Tigo han mantenido mejores puntajes desde el inicio de la evaluación en 2017. Aunque han mostrado mejoras en algunos aspectos y criterios hasta 2024, su progreso sigue siendo lento y enfrenta grandes desafíos. En contraste, las empresas proveedoras nacionales como COPACO y VOX han mostrado un avance mínimo desde 2017, lo cual resulta preocupante debido a su impacto en la calidad del servicio y la competitividad del mercado local. Esta falta de progreso limita la protección de los derechos de sus usuarios y usuarias.

Políticas de privacidad y datos personales

Con respecto al análisis de las prácticas de privacidad de datos entre las ISP se revela un panorama heterogéneo, con algunas proveedoras demostrando pasos positivos mientras que otras se quedan muy rezagadas. Aunque empresas como Claro, Personal y Tigo han facilitado el acceso a sus políticas de privacidad y ofrecen información relativamente detallada sobre las prácticas de recopilación y procesamiento de datos, sigue habiendo dudas sobre la exhaustividad y claridad de la información que proporcionan. A modo de ejemplo, ninguna de las tres empresas describe claramente los periodos de conservación de datos, un aspecto crucial de la protección de datos. Esta falta de transparencia podría suscitar preocupación por la posibilidad de que los datos se almacenen indefinidamente, contradiciendo los principios de minimización de datos y limitación de su finalidad.

Copaco, a pesar de tener una política de privacidad, limita su alcance a los datos recogidos a través de sus aplicaciones, olvidándose de abordar las prácticas de tratamiento de datos para otros servicios como Internet y telefonía. Este alcance limitado crea una preocupante laguna de transparencia en relación con el enfoque general de la empresa sobre la privacidad de los datos. Tigo, a pesar de tener una política de privacidad aparentemente exhaustiva, muestra incoherencias entre la política y su contrato de suscripción de servicios, en particular en lo que respecta a la necesidad del consentimiento de la persona usuaria para compartir datos con terceros. Estas discrepancias podrían causar confusión a sus usuarios y usuarias.

El caso más preocupante es el de Vox, que carece por completo de una política de privacidad a disposición del público. Esta ausencia demuestra el poco interés que tienen por la transparencia y los derechos de las personas usuarias, lo que subraya la necesidad de tomar medidas inmediatas para subsanar esta deficiencia crítica.

Autorización judicial

En relación con la autorización judicial, los resultados de esta edición no difieren significativamente de los obtenidos en análisis previos de QDTD. Todas las proveedoras de servicios de internet exigen un orden judicial antes de entregar información de sus usuarios y usuarias. Sin embargo, este debido proceso no incluye los metadatos de las comunicaciones, a pesar de que los estándares internacionales de derechos humanos aplicables a la vigilancia, como lo establecido en las sentencias de la Corte Interamericana de Derechos Humanos en los casos *Escher vs. Brasil* (2009) y *CAJAR vs. Colombia* (2023), señalan que estos también deben estar protegidos. Estas sentencias son vinculantes para la jurisprudencia paraguaya y refuerzan la necesidad de un marco legal estricto en esta materia.

El análisis de este criterio subraya la importancia de la normativa específica por sobre la legislación general, particularmente en el contexto de la vigilancia de las comunicaciones. Los artículos 198, 199 y 200 del Código Procesal Penal de Paraguay establecen de manera clara y explícita que cualquier intervención en las comunicaciones requiere de una orden judicial. Este principio refuerza el carácter excepcional de estas medidas, buscando equilibrar las necesidades de las investigaciones penales con la protección de los derechos fundamentales. Además, las disposiciones constitucionales y la Ley de Telecomunicaciones complementan este marco al proteger no solo el contenido de las comunicaciones, sino también su existencia, incluyendo los metadatos. Este enfoque integral busca garantizar que cualquier intervención comunicacional se realice bajo estricta legalidad y con pleno respeto a las garantías fundamentales. Un punto crítico identificado en este criterio es la falta de claridad y uniformidad en las políticas de las empresas respecto a la privacidad y el debido proceso. Por ejemplo, Claro menciona en su política que comparte datos por “razones legales”, pero no aclara si esto está condicionado a una orden judicial. Según el Informe de Sustentabilidad 2023 de América Móvil, su empresa matriz, se comprometen a evitar intervenciones ilegales y a respetar la privacidad de los usuarios. Sin embargo, el informe también menciona al Ministerio Público como una autoridad competente para solicitar datos, incluidas la geolocalización y la interceptación de comunicaciones, a pesar de que no tiene facultades para emitir órdenes judiciales. Esto plantea serias preocupaciones sobre posibles violaciones del debido proceso y del derecho a la privacidad.

Por otro lado, Personal afirma que comparte datos de usuarios solo con una orden escrita de una autoridad judicial competente, pero también señala que esta no es un requisito exclusivo. Asimismo, al igual que COPACO, no establece una distinción clara entre contenidos y metadatos, lo que debilita aún más la protección de la privacidad de las personas usuarias. En el caso de Tigo, su aviso de privacidad indica que puede compartir datos en diversas circunstancias sin especificar que una orden judicial sea un requisito previo. No obstante, su empresa matriz, Millicom, asegura en su Informe de Divulgación a las Autoridades 2023 que las subsidiarias, incluida Tigo Paraguay, solo entregan contenido de comunicaciones con una orden judicial. Esta discrepancia entre la política local de Tigo y las afirmaciones de su matriz genera dudas sobre las prácticas reales de la empresa.

Finalmente, Vox no proporciona información pública sobre si divulga datos de usuarios ni bajo qué circunstancias lo hace. Esta falta de transparencia imposibilita evaluar su compromiso con la autorización judicial para la divulgación de datos, lo que representa un vacío crítico en términos de protección de la privacidad.

Aunque las empresas muestran un cumplimiento general en cuanto a la exigencia de órdenes judiciales para el acceso a contenido de las comunicaciones, persisten serias preocupaciones respecto a la protección de los metadatos, la claridad en las políticas de privacidad y la transparencia en los procesos. Estos aspectos son esenciales para garantizar el respeto al derecho a la privacidad y el debido proceso en Paraguay.

Notificación a la persona usuaria

Sobre el tercer criterio, el análisis revela que ninguno de las cinco ISP cuenta con una política de notificación a los usuarios cuando sus datos son solicitados por las autoridades. Esta falta de transparencia ya identificada en todas las ediciones anteriores de QDTD, plantea preocupaciones significativas sobre los derechos de los usuarios y las protecciones del debido proceso en Paraguay.

Políticas para la promoción y defensa de los derechos humanos

En cuanto a este criterio las ISP analizadas en su mayoría no demuestran un compromiso público sólido con los derechos humanos, especialmente en lo que respecta a la búsqueda de regulaciones sobre la privacidad y protección de datos personales. Sin embargo, las empresas subsidiarias como CLARO y TIGO realizan acciones positivas porque provienen principalmente de las políticas de las empresas matriz, en lugar del compromiso directo de las locales. Se destaca que las empresas CLARO, Personal, Tigo y VOX participan de la GMSA, una organización global que promueve un entorno empresarial positivo y el cambio social en el ecosistema móvil. Así también Tigo y Claro son las empresas que cuentan con más campañas de seguridad para sus personas usuarias, identificadas a lo largo de las ediciones de QDTD.

Transparencia

Respecto a este criterio solo Claro y Tigo, proporcionan algún nivel de transparencia, y estos informes sólo se encuentran accesibles en las páginas web de las empresas matrices. Estos informes de transparencia regionales no siempre ofrecen desgloses detallados a nivel de país, lo que dificulta evaluar las prácticas específicas y las tasas de cumplimiento de sus subsidiarias nacionales. Además estos informes de transparencia disponibles se centran principalmente en órdenes de interceptación y solicitudes de metadatos, ofreciendo información limitada sobre otras formas de intercambio de datos de usuarios con entidades gubernamentales. Por ejemplo, sería relevante incluir detalles sobre solicitudes de datos como nombres, direcciones o información de facturación, que podrían ser requeridos por las autoridades para identificar a personas en el marco de investigaciones, así como aclarar si estas empresas participan en programas de monitoreo continuo u otras prácticas de vigilancia sistemática.

Accesibilidad

Y con relación al último criterio relacionado a accesibilidad, el análisis revela una marcada disparidad en la accesibilidad de los sitios web de las ISP. A lo largo de las 4 ediciones de QDTD, se observaron interesantes avances en este criterios. Por ejemplo, Tigo se destaca como el líder indiscutible, demostrando un fuerte compromiso con la inclusión al cumplir con los cuatro criterios de accesibilidad evaluados. En contraste, Claro, Copaco, Personal y Vox presentan deficiencias en distintos grados, siendo Vox el que muestra las barreras más significativas en términos de accesibilidad.

RECOMENDACIONES

El análisis de la presente investigación subraya la necesidad de mejoras en todos los ámbitos. Todas las ISP de Paraguay deberían priorizar el desarrollo de políticas de privacidad claras, completas y fácilmente accesibles que cubran todos sus servicios. Deberían abordar explícitamente los periodos de retención de datos, incluir referencias legales específicas y garantizar la coherencia entre los distintos documentos relacionados con las prácticas de tratamiento de datos.

La falta de notificación a las personas usuarias por parte de las ISP es un problema crítico que requiere atención inmediata. Al no notificar a las personas usuarias sobre las solicitudes de datos, estas empresas impiden que las personas ejerzan su derecho a impugnar posibles vigilancias ilegales y proteger su privacidad. Abordar esta deficiencia es crucial para fomentar un entorno de protección de datos que respete los derechos de los usuarios y promueva una mayor transparencia y rendición de cuentas.

Si bien las empresas matrices de Claro y Tigo han dado pasos iniciales hacia una mayor divulgación, la falta de informes independientes a nivel local y el alcance limitado de la información proporcionada dificultan una rendición de cuentas significativa. Las cinco ISP deben priorizar la transparencia publicando informes completos y detallados que permitan a los usuarios comprender y escrutar cómo se manejan sus datos en respuesta a las solicitudes gubernamentales. Esta mayor transparencia es esencial para construir confianza y garantizar la protección de la privacidad de los usuarios y los derechos de debido proceso paraguayo.

Además, es esencial adoptar medidas proactivas que vayan más allá de las declaraciones políticas básicas. Las ISP deben participar en iniciativas del sector que promuevan la privacidad de los datos y los derechos humanos, invertir en programas de educación y concienciación de las personas usuarias y participar de forma proactiva en recursos legales contra solicitudes de datos excesivas o ilegales. Tomando estas medidas, las ISP pueden fomentar una mayor confianza con sus usuarios y usuarias y contribuir a un entorno de protección de datos más sólido en Paraguay.



“¿Quién defiende tus datos?”

qdtd.tedic.org

2024

Esta obra está bajo una
Licencia Creative Commons
Atribución-CompartirIgual 4.0
Internacional.

