¿Quién defiende tus datos?

Paraguay - Abril, 2020

ELECTRONIC FRONTIER FOUNDATION

TEDIC
TECNOLOGÍA & COMUNIDAD

"¿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.

Quiénes somos

TEDIC es una organización sin fines de lucro que defiende y promueve los derechos humanos en Internet. Busca fomentar la producción de conocimiento y cultura libre en Internet sobre derecho, tecnología y género.

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 los usuarios y la innovación.

Consulta esta investigación en:
https://qdtd.tedic.org

Investigación principal
Maricarmen Sequera
Luis Alonzo Fulchi
Belén Giménez – Parte accesibilidad

Colaboración
Veridiana Alimonti de EFF

Diseño y diagramación
Horacio Oteiza

Tabla de contenidos

Introducción 5
Contexto nacional 6
Criterios de evaluación 9
1. Políticas de privacidad y protección de datos personales 9
2. Autorización judicial 12
3. Notificación al usuario 13
4. Políticas de promoción y defensa de los derechos humanos 15
5. Transparencia 16
6. Guías para requerimiento de información personal 17
7. Accesibilidad 17

Metodología 19
Criterio 1: Política de privacidad y protección de datos personales 19
Criterio 2: Autorización judicial 20
Criterio 3: Notificación al usuario 21
Criterio 4: Políticas de promoción y defensa de los derechos humanos 21
Criterio 5: Transparencia 22
Criterio 6: Guías para la solicitud de información personal 23
Criterio 7: Accesibilidad 24

Reporte de evaluación 26
Cuadro general comparativo 26
Reporte de evaluación por ISP 27
Claro - AMX Paraguay S.A 27
1. Política de privacidad y datos personales 27
2. Autorización judicial 28
3. Notificación al usuario 29
4. Políticas de promoción y defensa de los derechos humanos 29
5. Transparencia 31
6. Guías para requerimiento de información personal 31
7. Accesibilidad 32

COPACO - COPACO S.A. 34
1. Política de privacidad y datos personales 34
2. Autorización judicial 35
3. Notificación al usuario 36
4. Políticas de promoción y defensa de los derechos humanos 36
5. Transparencia 37
6. Guías para requerimiento de información personal 38
7. Accesibilidad 38

40

Personal - Nucleo S.A 40
1. Política de privacidad y datos personales 40
2. Autorización judicial 41
3. Notificación al usuario 42
4. Políticas de promoción y defensa de los derechos humanos 42
5. Transparencia 43
6. Guías para requerimiento de información personal 44
7. Accesibilidad 45
Tigo - Telefónica Celular del Paraguay S.A. (Telecel S.A.) 47
1. Política de privacidad y datos personales 47
2. Autorización judicial 48
3. Notificación al usuario 49
4. Políticas de promoción y defensa de los derechos humanos 49
5. Transparencia 51
6. Guías para requerimiento de información personal 52
7. Accesibilidad 53
VOX - Hola Paraguay S.A. 55
1. Política de privacidad y datos personales 55
2. Autorización judicial 56
3. Notificación al usuario 56
4. Políticas de promoción y defensa de los derechos humanos 57
5. Transparencia 58
6. Guías para requerimiento de información personal 59
7. Accesibilidad 59
Conclusiones 61
1. Políticas de Privacidad 61
2. Autorización judicial 61
3. Notificación 62
4. Políticas de promoción y defensa de los derechos humanos 62
5. Transparencia 62
6. Guías para requerimiento de información personal 63
7. Accesibilidad 63
Recomendaciones 64
Políticas de Privacidad 64
Autorización Judicial 64
Notificaciones 64
Políticas de promoción y defensa de los derechos humanos 64
Transparencia 65
Guías para requerimiento de información personal 65
Accesibilidad 65

Introducción

El proyecto "Quién defiende tus datos" está inspirado en "Who has your back" de EFF, aunque la metodología difiere de la aplicada en EEUU, ya que la realidad legal de Paraguay es bien diferente a la estadounidense.

En su segunda edición, el proyecto evaluó a las mismas empresas de telefonía y servicios de Internet que se habían evaluado en 2017: COPACO[1], VOX[2], PERSONAL[3], TIGO[4] y CLARO[5]. Se ha excluido a ChacoNet[6] ya que se tomó el criterio de analizar solamente las empresas que tienen un mercado superior a 15 000 clientes a nivel nacional.

Se ha habilitado una tabla de resultados para poder comparar el rendimiento de las empresas en las categorías y criterios de evaluación, basados en: su compromiso público con el cumplimiento de la ley; sus adopciones de buenas prácticas favorables a las personas usuarias de servicio de Internet; su transparencia sobre las prácticas y políticas; la accesibilidad en sus plataformas Webs, entre otros.

Cada empresa fue evaluada con base en las 7 categorías señaladas y justificadas a continuación, cuya elaboración tuvo en cuenta los requisitos de la ley 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 sostenibilidad y otros documentos que estuvieron disponibles en los sitios Web de las empresas hasta el 30 de enero de 2020. 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 enero 2020. Finalmente, estos comentarios y opiniones de las empresas fueron ajustados en la conclusión y en los puntajes correspondientes.

1 https://www.copaco.com.py
2 https://www.vox.com.py
3 https://www.personal.com.py
4 https://www.tigo.com.py
5 https://www.claro.com.py
6 https://www.chaconet.com.py

Contexto nacional

Según los informes anuales de la Comisión Nacional de Telecomunicaciones de Paraguay (CONATEL)[7] —ente regulador de las telecomunicaciones— y concretamente el último resumen de conexiones por usuarios del año 2018[8], se observa que la cantidad de conexiones a Internet es de 433.415 y si se desglosa por tipo de tecnología se tiene que: 230.356 son por cable módem, 62.991 por ADSL, 31.535 por fibra óptica, 68.959 por 3G (sólo por módem USB), 24.156 por 4G (sólo por módem USB), 10.777 por WIMAX y 4.641 utilizando otras tecnologías.

En términos de uso de Internet en el año 2018, el porcentaje de penetración[9] en banda ancha móvil[10] es 53,70 % y la penetración de Internet de banda ancha fija es 4,8 %[11]. Cabe recordar que Paraguay puede denominarse un país pequeño en tanto su población ronda los 7 millones de personas[12] y su territorio unos 400.000 km².

Según el informe 2017 de CEPAL[13], la penetración de Internet se incrementó en todos los países y quintiles entre el 2011 y el 2015. Sin embargo, Paraguay ha mostrado que el *acceso* a Internet sigue *sumamente desigual* entre los hogares más ricos y los más pobres. La diferencia es de *20 veces superior* del quintil más rico con relación al quintil más pobre. La *brecha de conexión* entre zona urbana y rural es de 20 puntos porcentuales.

La asequidad en el servicio de banda ancha fija que se mide por el precio promedio ofrecido de 1 Mbps como porcentaje del PBI per cápita, el país ocupa el cuarto lugar de los países de América Latina menos asequible con un porcentaje de 2,2 % aproximadamente, es decir que el costo de acceso a Internet es alto con relación a los ingresos de las personas usuarias. Además, en las tarifas mínimas para bolsas de datos prepagos de banda ancha móvil, también es uno de los países menos asequibles con 1,5 %[14].

Asimismo, cuando se habla sobre porcentajes de conexión de alta velocidad en América Latina, Paraguay y Venezuela aparecen en los últimos lugares con alrededor de 0,2 % de conexiones de más de 10 Mbps y alrededor de 0,1 % de conexiones por encima de 15 Mbps. Como referencia, a nivel mundial, los 10 países más avanzados en esta materia superan el 50 % de sus conexiones por encima de 15 Mbps.

---

7 https://www.conatel.gov.py/

8 Cobertura movil 2018 – CONATEL www.conatel.gov.py/conatel/wp-content/uploads/2020/01/cobertura-movil-2018.xlsx

9 Por porcentaje de penetración, entendemos a la *cantidad de personas que pueden acceder dentro de un país*.

10 Suscripciones activas a banda ancha móvil / población x 100

11 Suscripciones activas a banda ancha fija / población x 100

12 Población paraguaya http://countrymeters.info/es/Paraguay

13 CEPAL informe 2017 https://repositorio.cepal.org/bitstream/handle/11362/43365/S1800083_es.pdf?sequence=1&isAllowed=y

14 CEPAL informe 2017 - Idem

Un estudio desarrollado en 2018 por OpenSignal[15], posiciona a Paraguay en el puesto número 13, de 14 países relevados a nivel regional, con una velocidad promedio de 11,5 Mbps de descarga en internet móvil.

La cobertura de telefonía móvil e Internet móvil por región geográfica correspondiente al año 2018, según CONATEL se configura de la siguiente manera:

Cobertura de telefonía móvil e internet móvil por región geográfica. Año 2018					
Región	**Zona**	**Cantidad de localidades**		**Cantidad de hogares**	
Oriental	Urbana	2.183		996.850	
	Rural	5.471		545.629	
Occidental	Urbana	96		24.259	
	Rural	484		23.656	
Región	**Zona**	**2G**			
		Localidades cubiertas		**Población cubierta**	
Oriental	Urbana	2.177	99,73 %	996.081	99,92 %
	Rural	5.179	94,66 %	524.707	96,17 %
Occidental	Urbana	90	93,75 %	24.086	99,29 %
	Rural	324	66,94 %	17.991	76,05 %
Región	**Zona**	**3G**			
		Localidades cubiertas		**Población cubierta**	
Oriental	Urbana	2.161	98,99 %	994.568	99,77 %
	Rural	4.954	90,55 %	495.707	90,85 %
Occidental	Urbana	88	91,67 %	23.619	97,36 %
	Rural	265	54,75 %	12.453	52,64 %
Región	**Zona**	**4G**			
		Localidades cubiertas		**Población cubierta**	
Oriental	Urbana	1.931	88,46 %	835.365	83,80 %
	Rural	2.309	42,20 %	74.404	13,64 %
Occidental	Urbana	64	66,67 %	11.958	49,29 %
	Rural	148	30,58 %	2.109	8,92 %

Entonces, se puede observar que hay una fuerte concentración del sector de servicios de Internet y de telefonía móvil en Paraguay.

15 As 4G reach in Latin America improves, so does the consumer experience. March. 2018. Disponible en: https://www.opensignal.com/2018/03/05/as-4g-reach-in-latin-america-improves-so-does-the-consumer-experience

Para el estudio del proyecto se han seleccionado a las principales empresas Proveedoras de Servicios de Internet (ISP, por su sigla en inglés) de Paraguay, con base en la información encontrada en los documentos del Registro Nacional de Servicios de Telecomunicaciones (RNST), dependiente de CONATEL. Según dicho registro existen 105 operadores[16] con servicios de acceso a Internet y transmisión de datos. De estos, los que tienen alcance nacional son:

1. Telefónica Celular del Paraguay S.A. (Telecel S.A.) (Tigo)
2. Lexa Ingenieria S.R.L.
3. COPACO S.A.
4. AMX Paraguay S.A. (Claro)
5. Hola Paraguay S.A. (Vox)
6. Nucleo S.A. (Personal)
7. Tesam Paraguay S.A.

Para el presente estudio se seleccionaron las que superan los 15.000 suscripciones de servicio de Internet, que son las siguientes ISP: Tigo, COPACO, Claro, Vox y Personal.

Se destaca que este mercado de operaciones de servicio de Internet durante el año 2018 generó ingresos brutos por un total de 4.600.772.074.248 Gs[17] (9 millones de USD aproximadamente). Está compuesta por los ingresos de telefonía fija: 256.812.963.011 Gs, telefonía móvil (incluye Internet móvil 3G): 2.754.994.606.581 Gs, Internet móvil 4G/LTE: 687.064.194.866 Gs e Internet fija: 901.900.309.790 Gs.

16 Según consulta pública respondida en febrero de 2019 https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/19799

17 Ídem punto 8.

Criterios de evaluación

Se utilizaron **7 indicadores** para evaluar las *prácticas y políticas de privacidad* de cada ISP, basados en los siguientes puntos de vista:

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

A continuación, se desarrollan cada uno de los criterios:

1. Políticas de privacidad y protección de datos personales

> *La 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 los usuarios 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 en el caso que haya una investigación criminal bajo solicitud del juez competente.*

Al respecto, tanto la *Constitución de la República* en su artículo 33 —Sobre la Intimidad de las Personas— como los *Tratados Internacionales* protegen el derecho a la intimidad como uno de los pilares de las democracias modernas. Asimismo, organismos internacionales de protección de *derechos humanos* han señalado que las empresas deben establecer e implementar condiciones de servicio que sean transparentes, claras, accesibles, así como apegarse a las normas y principios internacionales de derechos humanos; incluyendo las condiciones en las que pueden generarse interferencias con el derecho a la privacidad de los usuarios[18]. Es indispensable que la ISP cuente con políticas que cumplan estos protocolos a la hora de entregar información personal 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 sus usuarios por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico 4868/2013. En este escenario, es imprescindible que las ISP describan y den a conocer qué información personal está siendo retenida, así como

18 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.

las medidas para salvaguardar dichos datos ante posibles ataques o riesgos que puedan afectar dicha información.

El artículo 10 de la ley 4858/2013 dice:

> *"Los Proveedores de Servicios de Intermediación y los Proveedores de Servicios de Alojamiento de Datos deberán almacenar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio, por un período mínimo de 6 (seis) meses, en los términos establecidos en este artículo. Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.*
> *Los Proveedores de Servicios de Alojamiento de Datos deberán almacenar sólo aquellos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.*
> *No podrán utilizar los datos almacenados para fines distintos a los que estén permitidos por la ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos".*

En un caso contencioso[19] reciente en el que se condenó al Brasil por el uso ilegal de escuchas telefónicas en un proceso penal, la Corte Interamericana señaló que el derecho a la privacidad protege tanto al *contenido* de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación, como ser los *metadatos* o *datos de tráfico*. Esta jurisprudencia vinculante a la jurisdicción nacional paraguaya, sitúa a estos datos en una instancia de protección constitucional y de derechos humanos.

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

> *Artículo 9 de la ley 4868/2013: "Obligación de los Proveedores de Servicios de Intermediación. Los Proveedores de Servicios de Intermediación consistentes en la prestación de servicios de acceso a Internet, estarán obligados, sin perjuicio de las disposiciones vigentes sobre los Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente, a: a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia; Esta obligación de información se tendrá por cumplida si*

19 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.

el correspondiente Proveedor incluye la información exigida en su página o sitio principal de Internet. a) suspender el acceso a un contenido o servicio cuando un órgano competente, en ejercicio de las competencias que legalmente tenga atribuidas, requiera que se interrumpa la prestación de un servicio o que se retire algún contenido que vulnere lo dispuesto en el Artículo 6º".

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

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

Por último se encuentra la Ley 2340/2016 Qué amplia la ley N.º 1334 del 27 de octubre de 1998 "De Defensa del Consumidor y del Usuario".

El artículo 55.- De la Identificación del Comprador. En la venta de un servicio de telecomunicaciones, el responsable de la comercialización del mismo, ya sea dependiente del propio operador o no, recabará los datos del comprador (nombre, apellido, fecha de nacimiento y número de Cédula de Identidad), y los remitirá al operador para su registro, dentro de los siguientes treinta días de verificado dicho acto. El operador del servicio de telecomunicaciones se limitará a registrar los datos suministrados por el responsable de la comercialización y no asumirá responsabilidad alguna por la veracidad de los mismos. ***El operador deberá conservar los datos registrados por un plazo mínimo de un año posterior a la cancelación del servicio***[20].

Esta normativa obliga a las ISP retener datos de la persona usuaria durante 1 año. Sin embargo, según consulta a las ISP, sólo se resguardan la información de perfil de la persona usuaria y contratos, no los contenidos y metadatos de las comunicaciones.

20 La negrita es de los autores.

2. Autorización judicial

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

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

El debido proceso para una interceptación de información.

3. Notificación al usuario

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

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

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

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

> *"Es imposible que una persona impugne efectivamente la interferencia de un gobierno en su vida privada si no sabe si ha sido víctima. En líneas generales, la falta de transparencia respecto a la aplicación de las leyes que rigen la vigilancia encubierta puede impedir el control democrático significativo de esas leyes"*[21].

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"*[22].

---

21 "Necesario y proporcionado". Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. Versión Mayo 2014. Página 36.

22 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

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

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

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

Con esto en mente, creemos que es importante fomentar la práctica de la notificación al usuario a través del proyecto *"¿Quién defiende tus datos?"* (WHYB). En los casos en que las solicitudes de datos no van acompañadas de la obligación de confidencialidad, la notificación es permitida por la ley paraguaya (dada la ausencia de prescripción legal en contrario). La posibilidad de notificación de usuario puede ser necesaria, no sólo en los casos de solicitudes de datos en procesos civiles, sino también en relación con las solicitudes hechas por otras agencias gubernamentales, tales como el Ministerio de Hacienda o CONATEL. Se fortalece la posibilidad de desafío legal a la presentación de pruebas irrelevantes a los hechos del caso.

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

4. Políticas de promoción y defensa de los derechos humanos

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

En este parámetro se analiza si la ISP tiene un posicionamiento institucional público en el que haya reconocido sus responsabilidades de *respeto y protección de derechos humanos*, incluyendo el *derecho a la privacidad*. Para este efecto, se analiza si existe algún posicionamiento que cumpla con las características señaladas por el Principio 16 de los Principios Rectores sobre las Empresas y los derechos humanos aprobados por el Consejo de derechos humanos de la Organización de las Naciones Unidas[23] 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."*

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, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad, así como si ha defendido la privacidad de sus usuarios por la vía judicial.

También se evalúa, si participa en algún mecanismo sectorial o multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales (Ejemplos: *Global Network Initiative*[24] o *Telecommunications Industry Dialogue*[25]).

---

23 Principios Rectores sobre empresas y derechos humanos https://www.business-humanrights.org/es/node/86208/principios-rectores-sobre-empresas-y-derechos-humanos

24 *Global Network Initiative* *https://globalnetworkinitiative.org/*

25 *Telecommunications Industry Dialogue* www.telecomindustrydialogue.org

Por otro lado, es esencial 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)[26] son espacios de debate público propiciados por Naciones Unidas, donde se discutan de forma abierta los principios compartidos, normas, reglas, procesos de toma de decisión y programas, que modelan la evolución y el uso de Internet.

5. Transparencia

El Principio 21 de los Principios Rectores sobre las Empresas y los derechos humanos de Naciones Unidas[27], exige buenas prácticas a las empresas sobre transparencia desde la perspectiva de los derechos humanos.

Los *informes de transparencia* del sector TIC en relación al impacto de la privacidad de los usuarios han sido más frecuentes en los últimos años[28]. La publicación de un informe de transparencia sobre las *solicitudes de acceso a datos* por parte de autoridades de seguridad y justicia debe proveer suficiente información para evaluar el contenido y el alcance de las medidas de vigilancia por parte de las autoridades.

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

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

---

26 Foro de Gobernanza de Internet – Global: https://www.intgovforum.org/multilingual/ y Foro de Gobernanza de Internet en Paraguay: https://www.intgovforum.org/multilingual/

27 Principios Rectores sobre empresas y derechos humanos https://www.business-humanrights.org/es/node/86208/principios-rectores-sobre-empresas-y-derechos-humanos

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

6. Guías para 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 diferencia de la publicación de informes de transparencia ya que los informes de transparencia apelan a datos estadísticos de solicitudes recibidas y cumplidas mientras que en los lineamientos analizados buscan determinar cómo cada empresa establece la forma en la que las fuerzas policiales o de investigación deben solicitarle información y, en su caso, qué especificaciones deben cumplir a dicho efecto.

Además, se analiza 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.

Algunos buenos ejemplos son el de Telefónica[29], Entel[30], VTR[31] y Comcast[32] que cuenta con una lista de requerimientos y procedimientos internos globales antes solicitudes de las autoridades locales.

7. Accesibilidad

La accesibilidad de la información encontrada en la Web, no importe la discapacidad o diversidad funcional de las personas usuarias, es fundamental para la ampliación del compromiso con la transparencia y el respeto de los derechos humanos. La Convención Internacional sobre los Derechos de las Personas con Discapacidad[33], a través de su artículo 9, reconoce al acceso a las tecnologías de la información y comunicación, incluyendo a la Web, como un derecho humano básico.

La accesibilidad de la Web consiste en disponibilizar el contenido a través de un diseño e infraestructura que funcione para todos los usuarios, 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 usuarios.

---

29 Telefónica: El cual *"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, Respuesta Diligente y Seguridad". Pág 4, 2016* https://www.telefonica.com/documents/153952/67280426/requerimientos-principios-es.pdf/6f5a0668-15b9-9b5c-3f69-65d866c5b53b

30 Entel. Disponible en : http://www.entel.cl/legales/pdf/Guia-judiciales.pdf

31 VTR. Disponible en https://vtr.com/img/documents/Protocolo-de-Entrega-de-información-a-la-Autoridad.pdf

32 Comcast de EEUU. Disponible en https://www.xfinity.com/~/media/403eeed5ae6f46118ddbc5f8bc436030

33 La convención de los derechos de personas con discapacidad https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-9-accessibility.html

Que las proveedoras de Internet 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.

Para este criterio, se evalúan los sitios Web oficiales de las proveedoras de Internet utilizando la guía de principios de Accesibilidad[34] de la Web Accessibility Initiative (WAI), parte del W3C (World Wide Web Consortium).

34 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

Metodología

Para esta investigación se analizó documentación sobre cada empresa de telefonía y proveedora de Internet, luego se intentó establecer contacto con cada una de ellas. Se logró socializar los resultados preliminares de evaluación con las empresas Tigo[35], Personal[36], Vox[37], Claro[38] y COPACO[39]. En estas reuniones se presentó la metodología de evaluación que sería implementada para el año 2020, así como se recibió retroalimentación por parte de las propias ISP.

Criterio 1: Política de privacidad y protección de datos personales

Lo que precisamos saber es: ¿La ISP proporciona información clara y completa sobre la recopilación, uso, almacenamiento, procesamiento y protección de datos personales del usuario?
En esta categoría, se evalúan las *políticas y avisos de protección de datos y privacidad* de la ISP, disponible públicamente, sobre el tratamiento de los datos personales que obtiene al prestar el servicio de telecomunicaciones, y no únicamente sobre datos que otorga la persona al contratar el servicio o utilizar el sitio Web de la ISP. ¿Se establece de manera precisa qué información de usuario y de sus comunicaciones son obtenidas, almacenadas, así como la temporalidad con la que dichos datos son almacenados?

¿Cuáles son los criterios de evaluación?

I. La ISP proporciona información y claras referencias legales sobre la recopilación de datos personales, incluyendo los datos personales que se recogen y en qué situaciones se produce la recogida;
II. La ISP proporciona información y claras referencias legales sobre el uso y/o procesamiento de datos personales, incluyendo los fines para los que se utilizan y cómo se produce este;
III. La ISP proporciona información y claras referencias legales en el almacenamiento de datos personales, incluyendo cuánto tiempo se almacenan los datos así como donde se almacenan y cuando se eliminan, si es que se eliminan;
IV. La ISP proporciona información y claras referencias legales sobre protección de datos personales, incluyendo las prácticas de seguridad que se observan en los procedimientos de retención de datos, si existe política de anonimización de datos y quién/es tendría/n acceso a las bases de datos;
V. La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo;
VI. Es fácil acceder a esta información en el sitio Web de la ISP.

35 http://www.tigo.com.py
36 https://personal.com.py
37 https://www.vox.com.py
38 https://www.claro.com.py
39 https://www.copaco.com.py

Estándares de desempeño:
Política de privacidad

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

Criterio 2: Autorización judicial

Precisamos saber: ¿La ISP se comprometen a divulgar información del cliente, metadatos y contenidos de las comunicaciones únicamente en presencia de una orden judicial?
En esta categoría se evalúa si la 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 ISP, en su contrato o cualquier documento oficial a disposición del público deja claro a los usuarios las circunstancias en que las autoridades judiciales o administrativas pueden tener acceso a sus datos.

¿Cuáles son los criterios de evaluación?

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

Estándares de desempeño:
Autorización judiciales

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 con ninguno de los criterios

Criterio 3: Notificación al usuario

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

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

¿Cuáles son los criterios de evaluación?

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

Estándares de desempeño:
Notificación al usuario

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

Criterio 4: Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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 esta categoría se evalúa si posee una *política institucional* en la que reconoce sus responsabilidad de respeto y protección de los derechos humanos, incluyendo el derecho a la privacidad; y si participa en algún foro o mecanismo para el respeto de derechos humanos en el ámbito de sus responsabilidades empresariales.

También se evalúa si la empresa ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad, así como si ha defendido la privacidad de sus usuarios por la vía judicial.

Asimismo, se evalúa si realizan algún tipo de actividad publicitaria, campaña de concientización, realización de jornadas.

¿Cuáles son los criterios de evaluación?

I. Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios 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 publica 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 multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).

Estándares de desempeño:
Política de promoción y defensa de los derechos humanos

Estrella llena		La ISP cumple con 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

Criterio 5: Transparencia

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

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

¿Cuáles son los criterios de evaluación?

I. La ISP publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales;
II. 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.

Estándares de desempeño:
Transparencia

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

Criterio 6: Guías para la solicitud de información personal

Precisamos saber: ¿La ISP proporciona 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 los 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 para entregar información al sistema de persecusión penal u otro tipo de investigación y, en su caso, qué especificaciones deben cumplir a dicho efecto.

También se evalúa si la ISP, 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.

¿Cuáles son los 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.

Estándares de desempeño
Guías para requerimiento de información personal

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

Criterio 7: Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

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

¿Cuáles son los 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 de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).

Estándares de desempeño:
Accesibilidad

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 de evaluación

Cuadro general comparativo

Cuadro general comparativo 2020								
ISP	Criterios							Porcentaje de cumplimiento*
	Políticas de privacidad	Autorización judicial	Notificación al usuario	Políticas de promoción y defensa de los derechos humanos	Transparencia	Guías para requerimiento de información personal	Accesibilidad	
Claro	★	☆	☆	★	☆	☆	★	36,4 %
COPACO S.A.	☆	☆	☆	☆	☆	☆	☆	0 %
Personal	☆	☆	☆	★	☆	☆	★	18,2 %
tigo	★	★	☆	★	★	☆	★	54,5 %
VOX COPACO	☆	☆	☆	★	☆	☆	☆	4,5 %

* El cálculo de porcentajes se realizó considerando el número total de criterios cumplidos por cada ISP en relación al número total de criterios existentes (22 criterios en total).

Claro - AMX Paraguay S.A

1. Política de privacidad y datos personales

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

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 del usuario y sus comunicaciones es obtenida y almacenada.		•
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades.	•	
La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo.	•	
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la ISP.	•	

La ISP tiene una política de privacidad que es accesible desde su Web, a "dos clics de distancia", luego de acceder a "Legal y Regulatorio"[40] en el pie de su página principal. Después se debe hacer clic en "Políticas de privacidad" y allí se accede a la mencionada política.

En la misma puede leerse que recopilarán datos de identificación, contacto, etc., pero no dicen cuáles de manera precisa. Por esta razón creemos que no corresponde el segundo criterio.

40 https://www.claro.com.py/personas/legal-y-regulatorio/

Sí se establecen las causas y procedimientos de posibles transmisión de datos, así como la necesaria autorización expresa del cliente en caso de que la transmisión se realice a terceros.
No se encontraron referencias a la temporalidad del almacenamiento. Sin embargo, en la reunión informativa la ISP confirmó que aplica el artículo 55 de la ley 2034/2016 – Amplia la ley de derecho al consumidor, que les obliga a almacenar un mínimo de 1 año posterior a la cancelación del servicio. Sin embargo, esta información no se encuentra en las políticas de privacidad publicada en su página Web.

La ISP cumple 3 a 4 criterios.

2. Autorización judicial

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

Autorización judicial		
	Sí	**No**
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
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.		•

Cuando la empresa habla de entrega de datos con fines legales se hace de la siguiente forma:

> *"[...]Compartiremos información personal con empresas, organizaciones e individuos fuera de CLARO si creemos de buena fe que el acceso, el uso, la conservación o la divulgación de la información es razonablemente necesaria para:*
>
> *Cumplir con las leyes, las reglamentaciones, los procesos legales o las exigencias gubernamentales aplicables. [...]"*

De acuerdo a las observaciones que nos facilitó la ISP, se entrega la información al sistema de persecución penal de dos formas: orden judicial y pedido de informe de la Fiscalía.
En busca a colaborar con las autoridades del sistema penal no han podido mediar de manera suficiente para que todos los pedidos sólo sean por orden judicial. En los últimos años, han logrado obligar que los pedidos de informes sean firmados por el fiscal de la causa y no por cualquier funcionario.

Sin embargo se remarca que la investigación evalúa los compromisos públicos y la necesidad de orden judicial para acceder al contenido que esta IPS no lo expresa claramente en la política de la empresa. Es importante reconocer que la ISP ha contestado y dialogado con TEDIC durante la investigación, pero no se puede brindar puntos por una información que la empresa no comparte públicamente.

La ISP no cumple el criterio.

3. Notificación al usuario

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

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

No se encontraron referencias sobre la notificación a partir de situaciones legales de entrega de información personal.

La ISP no cumple el criterio.

4. Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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?

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

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

Se encontró evidencias sobre publicaciones de sensibilización sobre la privacidad realizado en el año 2019. La publicación[41] se llamó "Tu seguridad es importante para nosotros" publicado en sus redes oficiales. Según el Informe global de sustentabilidad de AMX[42] han realizado en Paraguay desde el año 2018 capacitaciones sobre seguridad y privacidad enfocados en datos personales. Pero no se encontraron casos en los que la ISP se resistió judicialmente a solicitudes de información ilegales o excesivas.

Sobre el último punto, se observa que la ISP forma parte de Global Compact International[43] espacio internacional de dialogo sobre los derechos humanos y de los mecanismos para afrontar responsabilidad en materia de derechos humanos, aunque no participa ni en el Pacto Global[44] capítulo Paraguay (Global Compact). También forma parte del grupo GSMA y de los Objetivos de Desarrollo Sostenible de Naciones Unidas, así también cuenta con políticas de derechos humanos[45].

La ISP cumple con dos criterios.

41 Publicaciones de Claro el 7/08/2019. Disponible en https://www.facebook.com/claropy/photos/a.204663149551786/3408194305865305/?type=3&theater

42 Sustainability Report 2018 – América Móvil. Capítulo: Training sessions on information security and privacy carried out . Pag 55. Disponible en https://s22.q4cdn.com/604986553/files/doc_downloads/sustainability/AMX-SR-2018-ENG.PDF

43 Web portal América Móvil: https://www.americamovil.com/English/sustainability/global-engagement/default.aspx

44 Web del Pacto Global Paraguay: http://pactoglobal.org.py/

45 Políticas de derechos humanos de América Móvil https://s22.q4cdn.com/604986553/files/doc_downloads/human_rights/Pol%C3%ADtica_Der_hum.pdf y Informe de sustentabilidad. Año 2018. Pág 32 https://s22.q4cdn.com/604986553/files/doc_downloads/sustainability/AMX-SR-2018-ENG.PDF

5. Transparencia

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

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.		•

No se encontró evidencia de informes de transparencia por parte de Claro, ni detalles sobre la colaboración con autoridades gubernamentales, más allá de las mencionadas anteriormente.

La ISP no cumple ninguno de los criterios.

6. Guías para requerimiento de información personal

Precisamos saber: ¿La ISP proporciona 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 los clientes, cuáles son las condiciones para la entrega de dicha información personal?

Guías para requerimiento 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.		•

No se encontró evidencia sobre protocolos o guías sobre solicitud de información de sus clientes por parte de Claro de acceso público.

La ISP no cumple ninguno de los criterios.

7. Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

Accesibilidad		
	Sí	**No**
La ISP tiene una interfaz de 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 ISP es compatible con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).	•	

Claro, en su sitio tiene, diferentes páginas "Términos y condiciones de uso" correspondientes a cada servicio que brinda (Cabledistribución IPTV[46], Factura Braille[47], Prepago[48] y Telefonía móvil[49]), así como también un sitio de Políticas de Privacidad, como ya se mencionó en apartado anterior. El contenido de dichas páginas aparece con buen contraste de colores, y tamaño de texto adecuado, por lo que se puede afirmar que presenta información perceptible y adaptable, cumpliendo con el primer criterio. También cabe mencionar que Claro es la única ISP que disponibiliza el servicio de Factura Braille a través de su sitio Web.

Dentro de estas páginas se puede hacer scrolling sin dificultad con las teclas de dirección, además de zoom in y out con el teclado. Los usuarios también tienen tiempo suficiente para leer y utilizar el contenido, y estos no cuentan con elementos parpadeantes que puedan causar convul-

46 Términos y condiciones Claro Cabledistribución IPTV. Disponible en: https://www.claro.com.py/portal/py/legal-regulatorio/lightbox/descripcion-ED-8.html

47 Términos y condiciones Claro Factura Braille. Disponible en: https://www.claro.com.py/portal/py/legal-regulatorio/lightbox/descripcion-ED-3.html

48 Términos y condiciones Claro Prepago. Disponible en: https://www.claro.com.py/portal/py/legal-regulatorio/lightbox/descripcion-ED-7.html

49 Términos y condiciones Claro Telefonía móvil. Disponible en: https://www.claro.com.py/portal/py/legal-regulatorio/lightbox/descripcion-ED-6.html

siones o reacciones físicas. Sin embargo en líneas generales los sitios no poseen una estructura que sea predecible o enteramente accesible: esto se debe a que los enlaces no tienen nombres adecuados y esto dificulta la identificación utilizando lectores de pantalla, a la vez que vuelve difícil encontrar la información. Esto último se debe a que no están denominadas las secciones de "Términos y Condiciones", o "Política de Privacidad". Por lo tanto no cumple el segundo criterio. Además, si bien el texto es legible y comprensible, se identifica al español como idioma primario, desde el principio, y se utilizan explicaciones para hacer que el lenguaje sea sencillo de entender, debido a que los enlaces no son predecibles, no se encuentran mecanismos de navegación funcional y etiquetas accesibles que hagan más fácil encontrar la información, por ende este tercer criterio tampoco se cumple.

A pesar de lo mencionado en cuanto a la falta de accesibilidad y predictibilidad de los enlaces del sitio de Claro, los contenidos son comprensibles y compatibles con las herramientas de usuario actuales, como lectores de pantalla y plataformas, que analizan el nivel de accesibilidad, por lo que cumple el cuarto criterio.

La ISP cumple con dos criterios.

COPACO S.A.

COPACO - COPACO S.A.

1. Política de privacidad y datos personales

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

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 del usuario y sus comunicaciones es obtenida y almacenada.		•
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades.		•
La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo.		•
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la ISP.		•

COPACO afirma tener una política de privacidad[50] sin embargo no fue posible encontrarla en su sitio Web, incluso utilizando las herramientas avanzadas de búsqueda de Google.

Justamente utilizando esa herramienta en la Web de COPACO, se pudo encontrar un "Reglamento de protección al usuario" que pertenece a CONATEL, pero que presenta algunos problemas: 1. Se encuentra en un formato "rasterizado" de texto: imposibilidad de indexar su contenido. 2. No hace referencia alguna a COPACO y desde que COPACO no lo enlaza en su Web, no podemos decir que haya una vinculación formal entre dicho documento y la ISP.

50 De acuerdo a lo que indica en el apartado "Datos de carácter personal" en https://www.copaco.com.py/index.php/condiciones.html

Además se encontró un PDF, también en formato no indexable, denominado “Disposiciones generales”[51] pero que no hace referencia alguna a datos de carácter personal ni privacidad.

La ISP no cumple ninguno de los criterios.

2. Autorización judicial

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

Autorización judicial		
	Sí	**No**
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
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.		•

Se confirma que la ISP entrega el contenido de las comunicaciones sólo a través del orden judicial. Sin embargo, sobre los metadatos entregan a las autoridades con orden judicial y con pedido de informe del Ministerio Público. No existen casos en los que la ISP se resistió judicialmente a ello.

La investigación evalúa los compromisos públicos y la necesidad de orden judicial para acceder al contenido no está clara en la política de la empresa. También se remarca que la ISP no ha accedido a dialogar con TEDIC durante la investigación, por tanto no se puede brindar puntos por una información que la ISP no comparte públicamente.

La ISP no cumple ninguno de los criterios.

51 Accesible desde https://www.copaco.com.py/index.php/info-generales.html

3. Notificación al usuario

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

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

No se encontró evidencia del compromiso de COPACO a la notificación del usuario.

La ISP no cumple el criterio.

4. Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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?

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

No se encontraron referencias a la protección de los derechos humanos en Internet, ni sobre vigilancia estatal y control de las comunicaciones, no se encontraron iniciativas políticas, ni legales así como tampoco jornadas o publicaciones al respecto. Sin embargo, se ha encontrado una participación activa durante los últimos 3 años en las mesas de múltiples partes interesadas del Foro de Gobernanza de Internet en Paraguay. No se encontraron tampoco casos en los que la ISP se resistió judicialmente a solicitudes de información ilegales o excesivas.

Sobre el último punto, no se observa que ISP forme parte de mecanismos para afrontar responsabilidad en materia de derechos humanos, pues no participa ni en el *Pacto Global*[52] capítulo Paraguay (*Global Compact*) ni en otros espacios internacional en que se discuten estos temas.

La ISP no cumple ninguno de los criterios.

5. Transparencia

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

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 el área de transparencia de su página Web, COPACO solamente hace referencia al marco legal vigente, enlazando a las leyes 5189/14 y 5282/14 así como al portal estatal de denuncias de corrupción.

La ISP no cumple ninguno de los criterios.

52 Sitio Web de Pacto Global Paraguay: http://www.pactoglobal.org.py/

6. Guías para requerimiento de información personal

Precisamos saber: ¿La ISP proporciona 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 los clientes, cuáles son las condiciones para la entrega de dicha información personal?

Guías para requerimiento 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.		•

No se encontró evidencia de la existencia de ninguno de los 3 criterios para COPACO.

La ISP no cumple ninguno de los criterios.

7. Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

Accesibilidad		
	Sí	**No**
La ISP tiene una interfaz de 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 ISP es compatible con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

COPACO tiene un sitio Web que cuenta con contenido cuyo tamaño de texto puede ser redimensionado y adaptado para no perder de vista información, además de un buen contraste. Sin embargo existen elementos que no aparecen enteramente perceptibles y no tienen alternativas descriptivas equivalente. Si bien las imágenes cuentan con texto alternativo indicando que son los logos, dentro del sitio hay botones o entradas de formulario que no tienen texto o equivalente descriptivo que ayude a identificar el elemento con un lector de pantalla. Como resultado, no cumple el primer criterio.

Si bien dentro de estos sitios se puede hacer scrolling sin dificultad con las teclas de dirección, y *zoom in* y *out* con el teclado, los usuarios tienen tiempo suficiente para leer y utilizar el contenido, y los mismos no cuentan con contenido parpadeante que pueda causar convulsiones o reacciones físicas, los sitios no poseen una estructura que sea predecible o enteramente accesible. Esto es debido a que la herramienta de análisis de accesibilidad Web identificó la presencia de enlaces sin texto descriptivo que hace difícil que se puedan identificar estructuralmente, lo que dificulta la identificación con lectores de pantalla, así como no permite encontrar fácilmente la información. Por ende no cumple el segundo criterio.

En su página de "Políticas de Privacidad y Datos Personales", COPACO afirma tener una política de privacidad[53] dentro del mismo sitio de condiciones de uso de sus servicios, sin embargo no fue posible encontrarla, incluso utilizando las herramientas avanzadas de búsqueda de Google. A pesar de haber encontrado un "Reglamento de protección al usuario" que pertenece a CONATEL, la imposibilidad de indexar su contenido, la falta de referencia alguna a COPACO y también la falta de una vinculación formal a través de un enlace de este contenido a la Web de COPACO hacen que no se cumplan con aspectos de accesibilidad como la predictibilidad y operabilidad y compatibilidad con herramientas de usuario actuales, como lectores de pantalla y plataformas que analizan el nivel de accesibilidad de los mismos. Por ende, no se cumple con el tercer ni cuarto criterio.

La ISP no cumple ninguno de los criterios.

53 De acuerdo a lo que indica en el apartado "Datos de carácter personal" en el sitio Web mencionado: https://www.copaco.com.py/index.php/condiciones.html

Personal - Nucleo S.A

1. Política de privacidad y datos personales

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

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 del usuario y sus comunicaciones es obtenida y almacenada.		•
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades.		•
La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo.	•	
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la ISP.		•

Personal cuenta con una política de privacidad, pero no está fácilmente accesible desde su página Web. Al menos, se debió utilizar las herramientas avanzadas de búsqueda de Google para poder encontrarla[54].

En dicha política se establece que se almacenará "cierta" información personal pero no se establece claramente cuál. Por otro lado no se establece temporalidad, pero sí afirma que podrá ser suprimida por el titular del dato.

En lo referente a la transferencia a terceros, Personal no establece causas y procedimientos pero sí indica que la misma será transferida con el consentimiento expreso del usuario, salvo que la ley o la autoridad competentes indiquen lo contrario.

54 Disponible en: https://www.personal.com.py/public/docs/politica-club.html

Para terminar este indicador, cabe decir que si bien el lenguaje es sencillo y comprensible, la misma no está disponible desde la página principal ni desde alguna otra.

La ISP cumple 1 a dos criterios.

2. Autorización judicial

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

Autorización judicial		
	Sí	**No**
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
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.		•

Personal establece que la revelación de datos personales se realizará por "requerimiento de ley" o ante "autoridad competente" pero nada afirma sobre orden judicial previa. Según conversación con las ISP se confirma que el contenido de las comunicaciones sólo se entrega con una orden judicial. Sin embargo, sobre los metadatos entregan indistintamente a las autoridades, sea con orden judicial o con pedido de informe del Ministerio Público.

La investigación evalúa los compromisos públicos y la necesidad de orden judicial para acceder al contenido no está clara en la política de la empresa. También se remarca que la ISP no ha accedido a dialogar con TEDIC durante la investigación, por tanto no se puede brindar puntos por una información que la ISP no comparte públicamente.

La ISP no cumple los criterios.

3. Notificación al usuario

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

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

La Política de Privacidad de Personal es muy sintética y no menciona nada referente a la notificación al usuario.

La ISP no cumple el criterio.

4. Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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?

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

Sobre el último criterio, se observa que la ISP forma parte del grupo GSMA[55]. No se observa que la empresa forma parte de Global Compact International espacio internacional de diálogo sobre los derechos humanos y de los mecanismos para afrontar responsabilidad en materia de derechos humanos, ni en el Pacto Global[56] capítulo Paraguay (Global Compact).

No se ha encontrado evidencia en los demás puntos del criterio de Políticas de promoción y protección de los derechos humanos.

La ISP cumple con un criterio.

5. Transparencia

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

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.		•

No se encontraron informes de transparencia.

La ISP no cumple ninguno de los criterios.

55 Lista de miembros de GSMA capítulo Paraguay: https://www.gsma.com/membership/membership-types/operator-membership/

56 Web del Pacto Global Paraguay: http://pactoglobal.org.py/

6. Guías para requerimiento de información personal

Precisamos saber: ¿La ISP proporciona 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 los clientes, cuáles son las condiciones para la entrega de dicha información personal?

Guía para requerimiento 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.		•

No se encontró evidencia de protocolos de actuación para la recepción de solicitud de información por parte de los clientes.

La ISP no cumple ninguno de los criterios.

7. Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

Accesibilidad		
	Sí	**No**
La ISP tiene una interfaz de 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 ISP es compatible con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).	•	

A pesar de que Personal posee una página Web de "Términos y Condiciones de uso"[57] que cuenta con contenido cuyo tamaño de texto puede ser re-dimensionado y adaptado para no perder de vista información, y que cuenta con buen contraste, existen elementos que no tienen información enteramente perceptible y alternativas descriptivas equivalentes. Si bien las imágenes tienen texto alternativo indicando su propósito, dentro de la página se identificaron botones que se encuentran sin texto o equivalente descriptivo que ayude a identificar el elemento con un lector de pantalla. Como resultado, no cumple el primer criterio.

En relación al segundo criterio, dentro de la página se puede hacer scrolling sin dificultad con las teclas de dirección, y zoom in y out con el teclado. Además los usuarios tienen tiempo suficiente para leer y utilizar el contenido, y el mismo no cuenta con contenido parpadeante que pueda causar convulsiones o reacciones físicas. Por otro lado, la página no posee una estructura que sea predecible o enteramente accesible y esto se debe a que la estructura de la página, le falta la identificación apropiada de un encabezado y título. Esto dificulta el uso de lectores de pantalla. Además, cabe mencionar dentro de este criterio que Personal cuenta con una página que habla sobre su política de privacidad[58] cuyo contenido es perceptible, tiene buen contraste y es adaptable en cuanto a tamaño, sin embargo no está fácilmente accesible desde su sitio Web. La misma fue encontrada utilizando las herramientas avanzadas de búsqueda de Google, lo que representa una falta de navegación funcional, y por tanto no cumple el segundo criterio.

57 Términos y condiciones de uso de Personal. Disponible en: https://www.personal.com.py/#!/public/institucional/terminos/
58 Política de privacidad de Personal. Disponible en: https://www.personal.com.py/public/docs/politica-club.html

Dentro del tercer criterio, se observa que el texto de ambas páginas es legible y comprensible, con el español como idioma primario y en donde se utilizan explicaciones para hacer que el lenguaje sea sencillo de entender. Sin embargo no existe una navegación predecible en su totalidad, no se encuentran mecanismos de navegación funcional y etiquetas accesibles que hagan más fácil encontrar la información en cuanto a políticas de privacidad, por lo que el tercer criterio tampoco se cumple.

A pesar de lo mencionado en cuanto a la falta de accesibilidad y predictibilidad de los enlaces de dichas páginas, los contenidos de ambas son comprensibles y compatibles con las herramientas de usuario actuales, como lectores de pantalla y plataformas que analizan el nivel de accesibilidad de los mismos, por ende cumplen con el cuarto criterio.

La ISP cumple con un criterio.

Tigo - Telefónica Celular del Paraguay S.A. (Telecel S.A.)

1. Política de privacidad y datos personales

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

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 del usuario y sus comunicaciones es obtenida y almacenada.	•	
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades.	•	
La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo.	•	
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la ISP.	•	

La política de privacidad es accesible desde la portada de la Web de Tigo, en el pie de página[59] y a un solo clic.

De los 6 criterios evaluados, el que falla es el de la **temporalidad**, ya que si bien la nombra, hace un juego de palabras para no establecerla, diciendo *"Tigo guarda sus datos personales únicamente 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"*.

La ISP cumple con 5 de los 6 criterios.

59 Disponible en: https://www.tigo.com.py/aviso-privacidad

2. Autorización judicial

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

Autorización judicial		
	Sí	**No**
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.	•	
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 declara que podrá entregar datos ante *"un requerimiento de una entidad gubernamental o administrativa en el ejercicio de sus funciones o por orden de autoridad judicial competente"*. Esto quiere decir que lo hará en cualquiera de los 3 casos, no es requerimiento excluyente la orden judicial.

Se destaca que en el informe anual de Millicom, la ISP informa que solo entregan contenido bajo orden judicial en Paraguay[60]. Esta es una información pública y accesible por las personas usuarias. La dificulta que se ha encontrado para acceder a este documento es que no se encuentra la ruta desde la web de Tigo Paraguay y sólo existe en la versión en inglés.

Si bien están enumerados los diferentes "datos personales" que recopila la empresa, no se encontró diferenciación de entrega a la autoridad entre datos y metadatos.

Según conversación con la ISP, se asegura que los contenidos sólo se entregan con orden judicial y los metadatos indistintamente: orden judicial o pedido de informe de la Fiscalía.

La ISP cumple con uno de los criterios.

60 Reporte anual de Millicom. Disponible en: (p.11): https://www.millicom.com/media/3960/led-report-2019.pdf. Un cambio en relación al reporte de 2018 - https://www.millicom.com/our-responsibility/cr-news-reports/.

3. Notificación al usuario

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

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

No se encontró evidencia de mecanismos de notificación a los usuarios.

No cumple con el criterio.

4. Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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?

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

No se encontraron iniciativas políticas ni legales por parte de Tigo en lo referente a protección de la privacidad de sus usuarios ante el Poder Legislativo o Ejecutivo. Tampoco se evidenciaron resistencias a través de la vía judicial, en caso de abusos de la autoridad competente o no cumplan con los requisitos legales.

En su página de responsabilidad social[61], la empresa desarrolla su área de trabajo en la inclusión en 3 ejes: social, educativa y digital. Se trabajan en temas de salud y educativas pero no se menciona que hayan actividades ni publicidad en lo referente a la protección de datos personales.

Han realizado algunas actividades referentes a la seguridad digital pero sin perspectiva de protección de datos personales como un derecho humano. En su página de "Inclusión digital"[62] se hace referencia a las "Directrices de protección de la niñez" pero el enlace está roto. Por otro lado, la empresa ha desarrollado en conjunto con Unicef Paraguay, un "Manual de Internet segura" como guía para padres, docentes, niños y jóvenes. En su página 6 desarrollan brevemente el concepto de privacidad y aplicado solamente a la protección en redes sociales. También se encuentra información en su sitio Web sobre control parental para los dispositivos móviles[63] y seguridad de identidad digital para billeteras digitales[64].Por lo tanto no desarrollan el concepto de privacidad y datos personales como derechos humanos.

Sobre el último criterio, se observa que la ISP forma parte de Global Compact International[65] espacio internacional de diálogo sobre los derechos humanos y de los mecanismos para afrontar responsabilidad en materia de derechos humanos, también se destaca la participación en el Pacto Global capítulo Paraguay[66] (Global Compact) así como también que forma parte del grupo GSMA[67].

La ISP cumple con dos criterios.

61 Disponible en: https://www.tigo.com.py/responsabilidad-corporativa/comprometidos-con-la-inclusion
62 Disponible en: https://www.tigo.com.py/responsabilidad-corporativa/comprometidos-con-la-inclusion
63 Disponible en https://ayuda.tigo.com.py/hc/es/articles/360015801754-Control-Parental-Ten%C3%A9s-el-poder-sobre-lo-que-decid%C3%ADs-compartir
64 Disponible en https://ayuda.tigo.com.py/hc/es/articles/360040097313--C%C3%B3mo-realizar-el-registro-digital-de-mi-c%C3%A9dula- y https://ayuda.tigo.com.py/hc/es/articles/360009905873-7-Tips-de-seguridad-para-utilizar-tu-billetera-Tigo-Money
65 Lista de membresía de UNGlobal: https://www.unglobalcompact.org/what-is-gc/participants/92701-Millicom
66 Lista de organizaciones adheridas al Pacto Global capítulo Paraguay: http://pactoglobal.org.py/participantes/
67 Lista de miembros de GSMA capítulo Paraguay: https://www.gsma.com/membership/membership-types/operator-membership/

5. Transparencia

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

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.		•

No se encontró evidencia de informes de transparencia, en el recorrido de la página institucional de la empresa, ni en su buscador, así como tampoco utilizando las herramientas avanzadas de búsqueda de Google. Sólo se encontró de manera genérica en la página Web oficial de Millicom[68]. El informe que describe en idioma inglés la información detallada de las solicitudes de interceptación de las comunicaciones, acceso a metadatos y a datos de servicios de pago por móvil (MFS). Sin embargo, la empresa no revela los datos relativos a Paraguay de manera separada. Las informaciones presentadas agregan datos de las solicitudes recibidas en Paraguay, Bolivia y Colombia, entre algunos datos se destaca que han clasificado según: interceptación, MFS, metadato por autoridades y por clientes.

La ISP cumple con un criterio.

68 Informe anual de Millicom. Año 2019. Capítulo: Privacy and freedom of expressión. Pág 201. Disponible en: https://www.millicom.com/media/3960/led-report-2019.pdf

6. Guías para requerimiento de información personal

Precisamos saber: ¿La ISP proporciona 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 los clientes, cuáles son las condiciones para la entrega de dicha información personal?

Guías para requerimiento 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 simplemente afirma que una de las razones del tratamiento de datos personales es legal que podría ser *"[…] el requerimiento de una entidad gubernamental o administrativa en el ejercicio de sus funciones o por orden de autoridad judicial competente [...]"*. Es la única referencia que se encontró en su página Web.

Luego de la entrevista con la ISP, los responsables del área legal confirmaron que cuentan con los lineamientos y protocolos en sus propios sistemas de atención al cliente, cuando el cliente solicita información personal. Sin embargo, no se encuentran disponibles para conocimiento de sus clientes de manera previa. Se destaca que cuentan también con lineamientos internos para aceptar o no los requerimientos solicitados por la autoridad competente. Cuentan con personal capacitado en analizar cada caso de solicitud fiscal y judicial basándose en su guías internas.

El documento no es accesible al público desde la web. Sin embargo se brindará una ¼ de estrella por hacer público en los lineamientos generales de Millicom[69], que siguen las guías aplicadas en cada país que la empresa actúa.

La ISP cumple con 1,5 de los criterios.

69 Law enforcement and major events guidelines – Millicom. Disponible en: https://www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf

7. Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

Accesibilidad		
	Sí	**No**
La ISP tiene una interfaz de 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 ISP es compatible con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).	•	

TIGO posee una página Web de "Términos y Condiciones de Uso" de sus servicios[70] y una página Web de "Aviso de privacidad"[71] que cuentan con texto de cuyos tamaño re-dimensionable y adaptados para no perder de vista información. Sin embargo, se identificaron elementos que presentan información enteramente perceptible y alternativas descriptivas equivalentes. Si bien las imágenes cuentan con texto alternativo que permite identificar su función, dentro de ambas páginas hay botones que se encuentran sin texto o equivalente descriptivo que ayuden a identificar los elementos con un lector de pantalla. Además, se identificaron errores de contraste en relación al formato en el cual se disponibilizan los enlaces, tanto en los contenidos como en el menú y en el pie de página. Ya que esto impide el ágil acceso con lectores de pantalla, no cumple el primer criterio.

En relación al segundo criterio, se observa que se puede hacer *scrolling* sin dificultad con las teclas de dirección, y *zoom in* y *out* con el teclado y los usuarios tienen tiempo suficiente para leer y utilizar el contenido, y los mismos no cuentan con contenido parpadeante que pueda causar convulsiones o reacciones físicas. Sin embargo las páginas en cuestión no presentan una estructura que sea predecible o enteramente accesible. Esto es debido a que la herramienta de análisis de accesibilidad Web identificó la presencia de enlaces sin texto descriptivo que hace difícil que se puedan identificar estructuralmente, y esto dificulta el uso eficiente de los lectores de pantalla, así como encontrar fácilmente la información. Por ende no cumple el segundo criterio.

70 Términos y condiciones de uso de Tigo. Disponible en: https://www.tigo.com.py/terminos-y-condiciones
71 Aviso de privacidad de Tigo. Disponible en: https://www.tigo.com.py/aviso-privacidad

Tanto la página de “Términos y Condiciones”, como “Aviso de Privacidad” son accesibles desde la portada de Tigo, ya que se encuentran en el pie de página y a un solo clic, lo que hace que la navegación sea bastante funcional y accesible. El texto en ambas páginas también es legible y comprensible, identificando el idioma primario como español desde el principio, y utilizando explicaciones para hacer que el idioma sea sencillo de entender. Por lo tanto, cumple con el tercer criterio.

Los contenidos de ambas páginas son comprensibles y compatibles con las herramientas de usuario actuales, como lectores de pantalla y plataformas que analizan el nivel de accesibilidad de los mismos, por ende cumple con el cuarto criterio.

La ISP cumple con dos criterios.

VOX - Hola Paraguay S.A.

1. Política de privacidad y datos personales

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

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 del usuario y sus comunicaciones es obtenida y almacenada.		•
La política de privacidad establece la temporalidad con la que los datos del usuario son almacenados.		•
La política de privacidad establece las causas y procedimientos a través de los cuales los datos de los usuarios son transmitidos a terceros y a autoridades.		•
La ISP proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo.		•
La política de privacidad utiliza un lenguaje sencillo, libre de tecnicismos y comprensible para el usuario y la política se encuentra disponible en la página de Internet de la ISP.		•

No se encontró Política de Privacidad ni Términos y Condiciones en la página Web de Vox. Se realizó una inspección manual y se utilizaron las herramientas de búsqueda avanzada de Google.

La ISP no cumple ninguno de los criterios.

2. Autorización judicial

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

Autorización judicial		
	Sí	**No**
La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa.		•
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 encontraron referencias sobre la entrega de datos sobre comunicaciones por parte de Vox, ni indicios sobre resistencia a solicitudes excesivas.

Sin embargo, se siguen las tendencias que las demás ISP utilizan como estándar. Los contenidos sólo se entregan por orden judicial, y los metadatos indistintamente: orden judicial y pedido de informe del Ministerio Público.

La investigación evalúa los compromisos públicos y la necesidad de orden judicial para acceder al contenido no está clara en la política de la empresa. También se remarca que la ISP no ha accedido a dialogar con TEDIC durante la investigación, por tanto no se puede brindar puntos por una información que la ISP no comparte públicamente.

La ISP no cumple ninguno de los criterios.

3. Notificación al usuario

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

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

No se encontró evidencias sobre notificaciones al usuario.

La ISP no cumple el criterio.

4. Políticas de promoción y defensa de los derechos humanos

Precisamos saber: ¿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?

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

No se encontraron iniciativas políticas ni legales por parte de Vox en lo referente a protección de la privacidad de sus usuarios. Tampoco se evidenciaron campañas, jornadas o publicaciones para generar conciencia sobre el derecho a la privacidad. No se ha encontrado casos en los que la ISP se resistió judicialmente a solicitudes de información ilegales o excesivas.

Sobre el último criterio, se observa que la ISP forma parte del grupo GSMA[72]. No se observa que la empresa forma parte de Global Compact International espacio internacional de dialogo sobre los derechos humanos y de los mecanismos para afrontar responsabilidad en materia de derechos humanos, ni en el Pacto Global[73] capítulo Paraguay (Global Compact).

La ISP cumple con un criterio.

72 Lista de miembros de GSMA capítulo Paraguay: https://www.gsma.com/membership/membership-types/operator-membership/

73 Web del Pacto Global Paraguay: http://pactoglobal.org.py/

5. Transparencia

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

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.		•

No se encontraron informes de transparencia sobre colaboración con autoridades gubernamentales. Cabe destacar que Vox es una empresa estatal, adquirida por COPACO en 2010, por lo que la probabilidad de colaboración con las autoridades es mucho mayor y por lo tanto, la necesidad de transparencia, también lo es. También se destaca que la fusión entre Vox y COPACO se realizará este año 2020[74].

La ISP no cumple ninguno de los criterios.

74 La COPACO se fusionará con Vox en febrero, anuncia Empresas Públicas Abc Color. Enero 2020. https://www.abc.com.py/edicion-impresa/economia/2020/01/04/la-copaco-se-fusionara-con-vox-en-febrero-anuncia-empresas-publicas

6. Guías para requerimiento de información personal

Precisamos saber: ¿La ISP proporciona 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 los clientes, cuáles son las condiciones para la entrega de dicha información personal?

Guía para requerimiento 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.		•

No se encontró evidencias de lineamientos o protocolos en este sentido.

La ISP no cumple ninguno de los criterios.

7. Accesibilidad

Precisamos saber: ¿la ISP posee un sitio Web con una interfaz de usuario con información perceptible y comprensible, navegación funcional y operable en relación a políticas de privacidad y términos y condiciones de sus productos y servicios?

Accesibilidad		
	Sí	**No**
La ISP tiene una interfaz de 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 ISP es compatible con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).		•

Como fue mencionado también en la categoría de “Política de Privacidad y Datos Personales”, no se encontraron páginas con información sobre “Política de Privacidad” ni “Términos y Condiciones” en el sitio Web de Vox. Se realizó una inspección manual y se utilizaron las herramientas de búsqueda avanzada de Google, lo cual permitió encontrar un documento sobre Términos y condiciones de uso del sitio en formato PDF[75]. No obstante, cabe mencionar que dicho formato de documento no es enteramente accesible, ya que impide el uso de herramientas de usuario que facilitan la lectura y acceso a la información a través de lectores de pantalla. Por ende, Vox no cumple con ningún criterio.

La ISP no cumple ninguno de los criterios.

75 Términos y condiciones de uso del sitio de Vox. Disponible en: https://web.vox.com.py/solicitudes/Condiciones/Terminos-Condiciones.pdf

Conclusiones

Existe una importante diferencia entre las proveedoras de Internet nacionales y aquellas que son subsidiarias de casas matrices extranjeras. Los resultados de los criterios son cumplidos mayormente por las ISP de capital extranjera debido a la existencia de estándares y prácticas promovidas por las empresas internacionales de telecomunicaciones y sus accionistas en bolsas de valores internacionales. Sin embargo, muchas de sus prácticas no son difundidas en sus portales Webs a nivel nacional.

Asimismo, hay un significativo avance de las ISP Claro y Tigo en los cumplimientos de las buenas prácticas basados en derechos humanos en la presente edición de "Quien defiende tus datos", en comparación a la investigación de la edición 2017. De acuerdo a los resultados de la investigación se describen las siguientes conclusiones:

1. Políticas de Privacidad

Se destaca una diferencia en los resultados de la publicación "Quién defiende tus datos" edición 2017. Para la actual investigación, se tuvo en cuenta los mismos criterios. Las ISP Tigo y Claro son las empresas que han mejorado sus políticas o aviso de privacidad disponibles en su página principal.

Personal, cuenta con cierta información pero insuficiente para la protección del derecho a la intimidad de los que contratan el servicio de telefonía e Internet. Tampoco se encuentra accesible en su página Web.

COPACO, y Vox *no tienen una política o aviso de privacidad* disponible en su página principal de Internet, por lo que ninguna ISP con capital del Estado paraguayo cumple con este criterio.
La ISP Tigo es la única que cumple con este criterio, sólo ha fallado en informar el tiempo de conservación. Las demás ISP tendrán que hacer el esfuerzo de indicar de manera clara qué información se recaba sobre el usuario y sus comunicaciones, y por cuánto tiempo se conservan los datos personales.

2. Autorización judicial

La Constitución de la República es clara al exigir que las autoridades designadas por las leyes deben obtener una *autorización judicial* antes de obtener acceso al contenido de las comunicaciones. Todas las ISP entrevistadas informaron cumplir este requisito siempre que se refiera a contenidos de las comunicaciones, pero no afirman ese compromiso claramente en sus políticas locales. Eso debe cambiar para que firmen un compromiso público en favor de la privacidad de sus usuarios. Tigo lo hace de manera pública en el informe global de Millicom sobre solicitudes de datos por autoridades de investigación, pero solamente en inglés y en la página Web de la empresa global.

Sin embargo, es importante destacar a lo que se refiere a metadatos, todas las ISP informaron que muchas veces entregan esta información sin orden judicial, sólo con el requerimiento fiscal denominado por el código procesal penal "pedido de información". Este mecanismo fue aceptado por la Corte Suprema sin tener en cuenta las sentencias internacionales vinculantes a nuestra jurisdicción nacional que indican la autoridad judicial como único mecanismo posible.

3. Notificación

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

4. Políticas de promoción y defensa de los derechos humanos

Únicamente la empresa Claro - América Móvil, fue detectada con el compromiso público de reconocimiento de sus responsabilidades empresariales en materia de derechos humanos y han realizado difusiones en temas de seguridad y privacidad enfocados en datos personales.

Asimismo, las ISP Claro y Tigo cuentan con una alta representación en instancias Internacionales sobre políticas de derechos humanos como *US Global Compact y su participación en el* capítulo Paraguay. Se resalta la participación de Tigo – a través de Millicom en *Telecommunications Industry Dialogue*. Y se destaca que las ISP Claro, Personal y Tigo forma parte del grupo GSMA[76].

No encontramos evidencia de que cualquier de las ISP investigadas haya defendido la privacidad de sus usuarios en los tribunales, resistiendo a solicitudes ilegales o excesivas. En lo que respecta a la participación en el Foro de Gobernanza de Internet, solo Vox ha cumplido con este criterio.

5. Transparencia

Únicamente Tigo a través del informe anual de Millicom en su capítulo sobre *"Law enforcement requests in 2019 - South America"* publica un informe de solicitudes de datos y metadatos de los usuarios solicitados por las autoridades judiciales. No obstante, este informe sólo se encuentra disponible en inglés y no ofrece suficiente información que permita saber el volumen, origen, motivos y alcance de solicitudes por país, sino sólo de manera general. Tampoco el número e identidad de las autoridades que solicitan a acceder a dichos datos por lo que no se cumple el segundo punto del mismo criterio para completar la estrella.

76 Lista de miembros de GSMA capítulo Paraguay: https://www.gsma.com/membership/membership-types/operator-membership/

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

6. Guías para requerimiento de información personal

Tigo es la única ISP que informa contar con procedimiento 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 de acuerdo con el marco legal paraguayo. Sin embargo, la empresa los mantiene fuera del conocimiento de sus usuarios y del público en general.

Las ISP tampoco identifican personas específicas como responsables a los cuales se puede contactar. O simplemente registran datos genéricos, en particular emails institucionales.

7. Accesibilidad

De las 5 IPS analizadas, las ISP Claro, Personal y Tigo cuentan con contenidos en sus sitio Web de la ISP compatibles con las herramientas de usuario actuales (diferentes navegadores, tecnologías de apoyo y otros agentes de usuario).

Unicamente la ISP Claro cuenta con una interfaz de sitio Web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función. Y la ISP Tigo es la única que califica en el criterio sobre si el sitio Web con información comprensible, que aparece y opera de forma predecible.

Recomendaciones

Políticas de Privacidad

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

Estos *avisos de privacidad y tratamiento de datos* forman parte de los estándares de economía digital que promueven los reportes de la OECD –desde este 2017, Paraguay es miembro oficial de esta organización. La adecuaciones mínimas a estas normas de buenas prácticas visibilizaría a nivel regional y mundial la responsabilidad y compromiso de las empresas locales en la calidad de la conectividad de los habitantes del territorio paraguayo.

Autorización Judicial

Establecer explícitamente este requisito en el *aviso de privacidad y tratamiento de datos personales* para la colaboración con autoridades de seguridad y justicia que implique la intervención del contenido de comunicaciones privadas o la entrega de metadatos (datos que identifiquen al usuario y detalles de su comunicación, como los registros de conexión).

Asimismo, es deseable que todas las ISP incluyan en sus avisos detalles del tratamiento que realizan sobre los metadatos almacenados. Se ha demostrado —por jurisprudencias internacionales vinculantes a nuestro sistema judicial— que los metadatos pueden revelar aspectos sensibles de la vida privada de las personas.

Notificaciones

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

Políticas de promoción y defensa de los derechos humanos

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

Se recomienda que las ISP realicen de manera proactiva actividades, jornadas, publicaciones, campañas sobre la importancia de seguridad digital, derechos a la privacidad y protección de datos personales de sus usuarios y usuarias.

Se sugiere a las ISP a realizar litigios estratégicos en el Poder Judicial para fortalecer y mejorar las interpretaciones legales que se dan en artículos de normativas vigentes ambiguas o confusas que tienen que ver con los derechos humanos en Internet.

Transparencia

El *informe de transparencia* es un elemento positivo para el resguardo de los derechos humanos. Conocer el número global de solicitudes realizadas por las autoridades de persecución penal, estadísticas respecto a las solicitudes realizas por otras autoridades, identificación de las instituciones solicitantes, tipos de solicitudes y razones que fueron otorgadas para hacer la solicitud, son claves para hacer un seguimiento de la vigilancia estatal de las comunicaciones. Un ejemplo a seguir es TELIA Company[77] de Suecia y Finlandia, que además de clasificar y divulgar los datos de interceptación legal de datos de sus usuarios, también publica informes de sostenibilidad donde expone todos los casos en que ellos defendieron la privacidad y otros derechos humanos de sus usuarios.

Es importante recalcar que empresas intermediarias como Facebook, Google, Twitter divulgan en sus páginas web informes de transparencia donde se especifican las solicitudes de los gobiernos.

Guías para requerimiento de información personal

Será necesario que cada ISP elabore políticas públicamente disponible que establezca protocolos o guías sobre la actitud respecto a solicitudes de información de organismos gubernamentales o fuerzas de seguridad.

Accesibilidad

Se sugiere utilizar la guía de principios de la iniciativa Accesibilidad de la Web (WAI), parte del W3C (World Wide Web Consortium) para disponibilizar el contenido a través de un diseño e infraestructura que funcione para todos los usuarios, sin importar el hardware, software, idioma, ubicación, habilidad cognitiva o sensorial.

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

TEDIC
TECNOLOGÍA & COMUNIDAD

EFF

“¿Quién defiende tus datos?”
qdtd.tedic.org/
2020

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