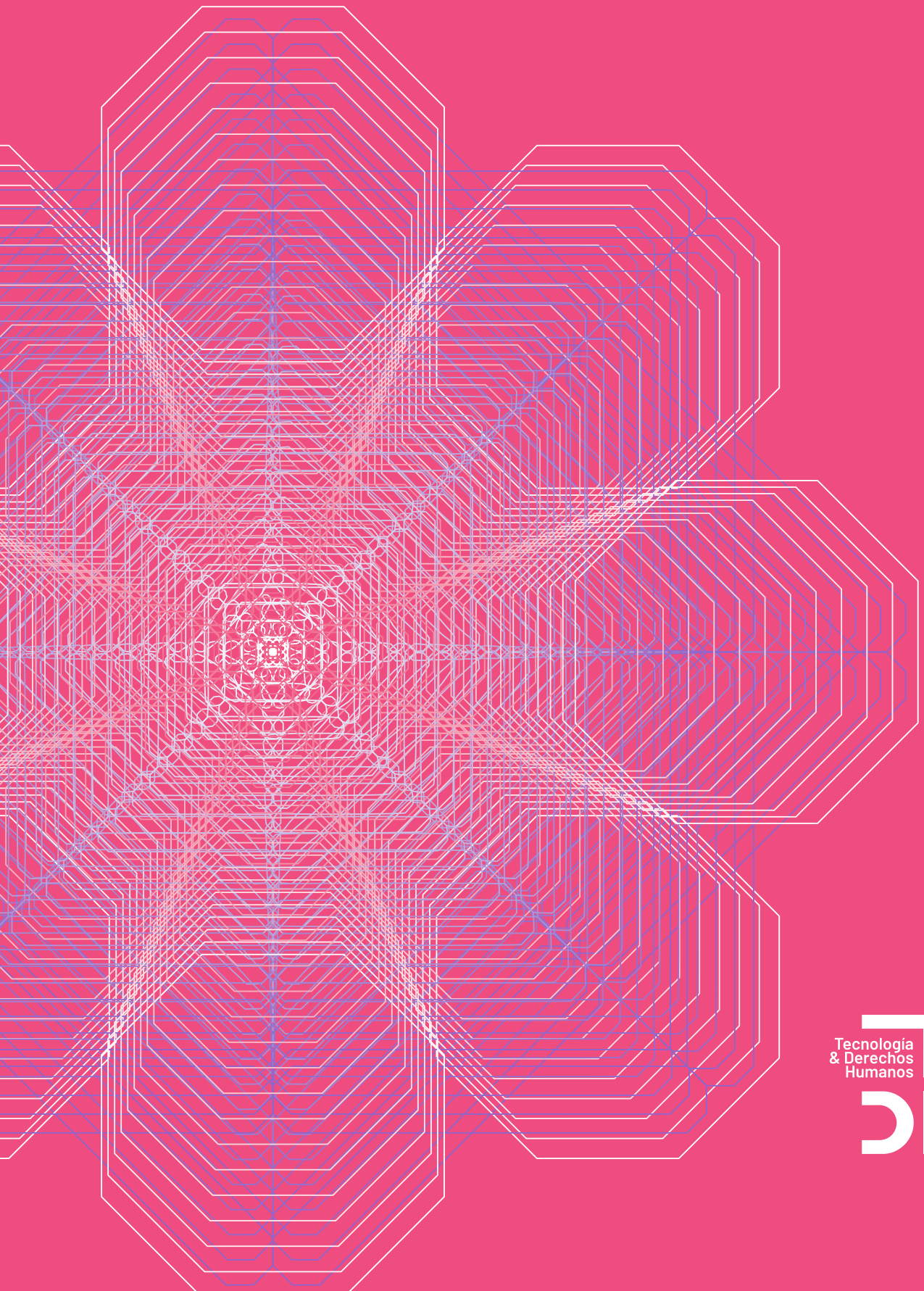
¿QUIÉN DEFIENDE TUS DATOS?

Paraguay 2026



Tecnología & Derechos Humanos

TEDIC

¿QUIÉN DEFIENDE TUS DATOS?

Paraguay 2026

Tecnología & Derechos Humanos

“¿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.

Tecnología & Derechos Humanos

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

¿QUIÉN DEFIENDE TUS DATOS?

Paraguay 2026

ABRIL 2026

COORDINACIÓN Y CO-EDICIÓN
Maricarmen Sequera

CO-EDICIÓN Y REVISIÓN
Veridiana Alimonti

AUTORA
Marlene Samaniego

ASISTENCIA DEL PROYECTO
Maricel Achucarro

COMUNICACIÓN
Camila Rolón

DISEÑO Y DIAGRAMACIÓN
Horacio Oteiza

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

ISBN 978-99989-999-4-7

TABLA DE CONTENIDO

INTRODUCCIÓN 6

CUADRO GENERAL COMPARATIVO 8

METODOLOGÍA 9

CONTEXTO NACIONAL 10

CRITERIOS DE EVALUACIÓN 18

REPORTE POR CADA ISP 29

REPORTE POR EMPRESA SOBRE LA POLÍTICA DE PRIVACIDAD Y DATOS PERSONALES 32

- STARLINK 32
- CLARO – AMX PARAGUAY S.A 36
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 40
- PERSONAL - NÚCLEO S.A. 44

REPORTE - AUTORIZACIÓN JUDICIAL 49

- STARLINK 49
- CLARO - AMX PARAGUAY S.A. 51
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 53
- PERSONAL - NÚCLEO S.A. 55

REPORTE - NOTIFICACIÓN A LA PERSONA USUARIA 58

- STARLINK 58
- CLARO - AMX PARAGUAY S.A. 59
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 61
- PERSONAL - NÚCLEO S.A. 62

REPORTE - POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS 65

- STARLINK 65
- CLARO - AMX PARAGUAY S.A. 68
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 70
- PERSONAL - NÚCLEO S.A. 73

REPORTE - TRANSPARENCIA 76

- STARLINK 76
- CLARO - AMX PARAGUAY S.A. 78
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 80
- PERSONAL - NÚCLEO S.A. 82

REPORTE - GUÍAS PARA LA SOLICITUD DE INFORMACIÓN PERSONAL 84

- STARLINK 84
- CLARO - AMX PARAGUAY S.A. 86
- TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 88
- PERSONAL - NÚCLEO S.A. 90

REPORTE - ACCESIBILIDAD 92

STARLINK 92
CLARO - AMX PARAGUAY S.A. 94
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 96
PERSONAL - NÚCLEO S.A. 98

REPORTE - PROTOCOLO DE ENTREGA DE DATOS PARA INVESTIGACIONES PENALES 102

STARLINK 102
CLARO - AMX PARAGUAY S.A. 104
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.) 107
PERSONAL - NÚCLEO S.A. 109

CONCLUSIÓN 111

RECOMENDACIONES 114

BIBLIOGRAFÍA 115

INTRODUCCIÓN

El proyecto ¿Quién defiende tus datos? se inspira en la iniciativa Who has your back? de la Electronic Frontier Foundation (EFF). Sin embargo, la metodología aplicada en este estudio es distinta, debido a que la realidad legal y regulatoria de Paraguay presenta particularidades que demandan un enfoque diferente.

El objetivo central de la investigación es fomentar la transparencia, así como la adopción de mejores prácticas en privacidad y protección de datos personales por parte de las empresas proveedoras de servicios de Internet (ISP) en Paraguay. Esta investigación intenta responder, entre otras, las siguientes interrogantes: ¿Cómo y hasta qué punto las ISP protegen la privacidad de los usuarios? ¿Las ISP realizan acciones que protejan los datos personales de los usuarios? ¿Existen protocolos en las ISP que regulen la actuación frente a solicitudes de los estados? ¿Las ISP realizan defensas activas en la protección de los derechos digitales en los espacios de la comunicación pública?

Las Naciones Unidas han declarado, en diversos informes y resoluciones, el acceso a Internet como fundamental para el ejercicio de los derechos humanos, incluyendo la libertad de expresión, acceso a la información y la participación en el ejercicio de la democracia (Consejo de Derechos Humanos, 2016) (Asamblea General, 2016). De manera similar, los Principios Rectores de la ONU sobre Empresas y Derechos Humanos establecen que las empresas deben respetar los derechos humanos y evitar impactos adversos de sus actividades (Naciones Unidas, 2011).

La principal novedad de esta edición, respecto a las anteriores (TEDIC, 2017, 2020, 2022, 2024), es la promulgación de la Ley № 7593/2025 “De Protección de Datos Personales en la República del Paraguay” (Presidencia de la República del Paraguay, 2025a), que establece por primera vez un régimen integral y general de protección de datos personales en el país. Esta ley constituye “un logro colectivo basado en evidencia y participación plural” (TEDIC, 2025), resultado de un proceso multisectorial impulsado por la Coalición de Datos Personales, con participación activa de organizaciones de la sociedad civil, academia y personas expertas en derechos digitales

La Ley № 7593/2025 tiene por objeto la protección integral de los datos personales de las personas físicas, con el fin de garantizar el ejercicio pleno de sus derechos y el libre flujo de información conforme a la Constitución y a los tratados internacionales ratificados por Paraguay. Su ámbito de aplicación comprende el tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado cuando los datos formen parte de un archivo, realizado por personas físicas o jurídicas, públicas o privadas.

La ley también establece criterios para su aplicación extraterritorial en el caso de tratamientos vinculados a la oferta de bienes o servicios a personas que se encuentren en Paraguay o en el caso del seguimiento de conducta de personas dentro del territorio nacional. Esta previsión resulta relevante para prestadores de servicios que, por su infraestructura o por el tratamiento de datos que realicen, tengan involucrados flujos de datos de carácter internacional.

La publicación de esta ley cambia de manera sustancial el panorama para esta investigación. En versiones anteriores, muchos de los criterios estaban enfocados en lo que se consideraban mejores prácticas a nivel internacional por la ausencia de una ley marco. En esta edición, el análisis se rige por la incorporación de disposiciones de carácter legal que se encuentran estatuidas en los pilares que se deben considerar en la regulación: principios de tratamiento, bases legitimadoras, derechos de los titulares, seguridad, notificación de brechas, internacionalidad de la regulación, y la creación de un organismo competente.

Por lo tanto, en este contexto, la evaluación del desempeño empresarial ya no se limita a examinar compromisos voluntarios, sino que analiza el grado de adecuación a un marco normativo vinculante que eleva los estándares exigibles en materia de privacidad y protección de datos personales. Además, es necesario realizar una revisión de carácter recurrente en la evaluación de desempeño de las ISP, para luego sistematizarla, resguardando la protección de los datos personales en el ámbito digital de Paraguay.

CUADRO GENERAL COMPARATIVO

Cuadro general comparativo									
ISP	Criterios								Porcentaje de cumplimiento*
	Políticas de privacidad	Autorización judicial	Notificación a la persona usuaria	Políticas de promoción y defensa de los derechos humanos	Transparencia	Guías de requerimiento de información personal	Accesibilidad	Protocolo de entrega de datos para investigaciones penales	
STARLINK	☆	☆	☆	☆	☆	☆	★	☆	24%
Claro	☆	☆	☆	★	★	★	☆	★	45%
tigo	☆	☆	☆	★	★	★	★	★	48%
personal	★	☆	☆	★	☆	☆	☆	☆	14%

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

METODOLOGÍA

La presente investigación se enfocó en la evaluación de las principales empresas que proveen servicios de Internet en Paraguay y que, en consecuencia, poseen una presencia importante en la esfera nacional. Para esta edición se eligieron empresas que, en función de la cobertura y de la operación, superan el umbral de relevancia, tomando como eje los indicadores de mercado publicados por la Comisión Nacional de Telecomunicaciones (CONATEL, 2025).

A diferencia de las ediciones anteriores, en esta investigación se excluyen Vox y Copaco del universo evaluado y se incorpora a Starlink como nuevo actor relevante. La incorporación de Starlink (Sequera, 2024) se justifica en virtud de su operación efectiva en el país, así como de la importancia de evaluar su desempeño en materia de privacidad, en atención a los aspectos técnicos y normativos que rigen la prestación de servicios por vía satelital.

Los proveedores de servicios de Internet recopilan información sobre sus usuarios y usuarias tanto para comercializarla como para cumplir con obligaciones legales. En este sentido, esta investigación se centró en el análisis cualitativo de políticas de privacidad, contratos de adhesión, informes de sostenibilidad, protocolos públicos y otros documentos que pueden ser consultados de forma directa en el sitio web de cada empresa, hasta el cierre de la fecha de campo estipulada para esta investigación.

El análisis se realizó dentro del marco de los criterios definidos en esta investigación, los cuales toman en consideración tanto el marco normativo vigente en Paraguay, incluyendo la recientemente promulgada Ley № 7593/2025 de Protección de Datos Personales, como las buenas prácticas internacionales en materia de protección de la privacidad y tratamiento de datos personales.

CONTEXTO NACIONAL

1. ACCESO Y CONECTIVIDAD

El acceso a Internet en Paraguay ha experimentado un crecimiento sostenido en los últimos años. El acceso a las tecnologías de la información y la comunicación, además de ser un derecho, posibilita distintas formas de participar en la sociedad, la economía y la política. Sin embargo, las brechas en el acceso y los usos de Internet se mantienen, algo que se evidencian en áreas rurales y en grupos poblacionales en situación de vulnerabilidad.

Según el Instituto Nacional de Estadísticas (INE) en el 2024, el 81,6% de la población utiliza Internet, de ese conjunto, el 81,0 correspondía a hombres y 82,1% a mujeres. Por su parte, según área de residencia, 86,2% (2.690.170) de la población urbana accedió a Internet en contraposición a 73,7% (1.327.659) de población rural (INE, 2024).

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

El PNT 21-25 (CONATEL, 2021) también señala que las tecnologías de acceso predominantes en banda ancha fija por cable son actualmente las conexiones HFC, seguidas por las conexiones FTTX y finalmente las conexiones ADSL. Análisis que permite una comprensión más completa de la capacidad y eficiencia de la red en el país y podría contribuir a la formulación de estrategias y políticas para mejorar la conectividad y garantizar un acceso equitativo y eficiente a los servicios de telecomunicaciones en el ámbito nacional.

La expansión de la conectividad también implica un aumento en el volumen y la sensibilidad de los datos personales que las empresas proveedoras tratan. Cuanto más se profundiza en el uso de los servicios, más exigencias se plantean a las ISP en la adopción de políticas más sólidas de protección de datos, así como en el cumplimiento de los principios de transparencia y debido proceso.

La inclusión de servicios satelitales como Starlink agrega nuevos desafíos regulatorios, especialmente respecto de la transferencia internacional de datos, la jurisdicción y la supervisión por parte de autoridades nacionales.

En una primera etapa, se realizó una evaluación preliminar con el objetivo de obtener un puntaje inicial por cada empresa. Esta evaluación, además, permitió el reconocimiento de fortalezas, debilidades y de áreas que podrían ser mejoradas, en cada uno de los criterios que se analizaron.

Luego, TEDIC se comunicó con las empresas que fueron evaluadas, a través de un correo electrónico, con el fin de presentar algunos resultados preliminares, y solicitar algunas aclaraciones y brindar la posibilidad de completar información que no está de manera pública. Este procedimiento metodológico es clave, no solo para la rigurosidad del estudio, también, para el fomento del diálogo y que la información que se publique realmente se ajuste a la información disponible en el momento de la publicación.

Finalmente, se realizó un análisis de los comentarios recibidos y, en los casos que se justificaba, se consideraron para los resultados finales y la asignación de puntuaciones.

2. CONTEXTO NORMATIVO

Este estudio requiere un análisis breve pero sustancial de las leyes de privacidad y protección de datos personales de las personas usuarias de servicios de Internet, así como las regulaciones específicas sobre telecomunicaciones, otras leyes y regulaciones que impacten directamente la gestión y el tratamiento de datos personales. Estas leyes y regulaciones establecen a los proveedores de servicios sus obligaciones y a las personas usuarias, sus derechos, marco que contextualiza la presente investigación.

2.1. Marco legal internacional

En el marco legal internacional vigente aprobado y ratificado por el Paraguay, instrumentos como la Declaración Universal de los Derechos Humanos (Naciones Unidas, 1948) y la Convención Americana de Derechos Humano (Presidencia de la Republica del Paraguay, 1989), protegen el derecho a la privacidad y la inviolabilidad de las comunicaciones. La jurisprudencia de la Corte Interamericana de Derechos Humanos (CIDH) ha reforzado estas protecciones, estableciendo precedentes relevantes para los Estados parte, incluido Paraguay, en relación con la protección de la privacidad y la vigilancia estatal, como los citados a continuación:

Caso Escher vs Brasil (2009)

Este caso resuelto por la Corte Interamericana de los Derechos Humanos (CIDH, 2009), examinó las violaciones de derechos humanos cometidas durante interceptaciones telefónicas realizadas a miembros de las organizaciones Coana y Adecon en Paraná entre mayo y junio de 1999. Aunque las grabaciones fueron autorizadas judicialmente, carecían de fundamentos adecuados, se extendieron más allá del plazo permitido y fueron filtradas a medios de comunicación.

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

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

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

Caso Restrepo (CAJAR) vs Colombia (2023)

La Corte emitió una sentencia histórica contra Colombia, declarando al Estado responsable de una campaña de vigilancia, acoso y persecución de miembros del Colectivo de Abogados "José Alvear Restrepo" (CAJAR) durante más de dos décadas (CIDH, 2023a, 2023b). Estas acciones, que incluyeron amenazas y hostigamiento, violaron derechos fundamentales como la vida, la integridad personal, la privacidad, la libertad de expresión y de asociación, afectando especialmente a las defensoras y a quienes se vieron obligados a exiliarse.

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

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

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

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

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

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

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

El tribunal concluyó que Colombia violó este derecho al restringir arbitrariamente el acceso y control de los miembros del CAJAR sobre sus datos personales en los archivos de inteligencia. Rechazó que la pertenencia de documentos a organismos de inteligencia sea suficiente para clasificarlos como reservados, exigiendo que las restricciones se basen en su contenido específico (EFF, 2024).

Ambas sentencias subrayan la importancia de proteger los derechos humanos, asegurar la protección de la privacidad y limitar la vigilancia estatal para prevenir abusos. Paraguay[1], al igual que muchas legislaciones de la región de América Latina protegen menos los metadatos que el contenido. Sin embargo, con estos casos, y bajo el principio de convencionalidad, el Estado paraguayo debe implementar medidas para evitar la vigilancia masiva y desproporcionada, garantizar la protección de datos personales, ofrecer garantías judiciales para que las personas, en especial los defensores de derechos humanos puedan desempeñar su labor sin temor a represalias o interferencias arbitrarias.

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

2.2. Marco legal nacional

La Constitución Nacional otorga reconocimiento al derecho a la intimidad (artículo 33), la protección del patrimonio documental y la información personal (artículo 36) y la protección del hábeas data (artículo 135), que otorga a las personas el derecho de acceder, modificar o suprimir información que les concierne y que se encuentra inscripta en bases de datos de carácter público o privado.

La promulgación de la Ley N.º 7593/2025 marca una nueva etapa en el ordenamiento jurídico paraguayo al establecer un régimen integral de protección de datos personales. La ley define conceptos fundamentales como datos personales, datos sensibles, tratamiento, responsable y encargado del tratamiento, consentimiento y anonimización.

La norma estructura el tratamiento de datos personales sobre un conjunto de principios generales que deben orientar todas las operaciones, su registro, organización, acceso, conservación, comunicación, transferencia o supresión de datos. Entre ellos, se establecen principios como: exactitud, exigiendo que los datos sean veraces y actualizados; confidencialidad, imponiendo reserva para evitar divulgaciones indebidas; finalidad, que limita el tratamiento a fines determinados, explícitos y legítimos; minimización o proporcionalidad, que exige tratar únicamente los datos pertinentes y no excesivos; limitación del plazo de conservación, estableciendo que los datos no deben conservarse más tiempo del necesario; lealtad y transparencia, que obliga a tratar datos de manera lícita y a entregar información clara a la persona titular; seguridad, que impone la adopción de medidas técnicas y organizativas para garantizar integridad y confidencialidad; y responsabilidad demostrada, que exige que el responsable adopte y pueda demostrar medidas de cumplimiento. Estos principios son especialmente relevantes al evaluar las políticas de privacidad de los ISP, dado que se traducen en obligaciones de información, limitación de usos, protección técnica y gobernanza interna.

La ley también establece bases legales para el tratamiento, incluyendo el consentimiento libre, informado e inequívoco del titular, el cumplimiento de obligaciones legales, la ejecución de contratos y el ejercicio de competencias públicas.

Esta misma ley, consolida un catálogo de derechos de los titulares de datos que debe ser operativizado por responsables y encargados para evaluar la efectividad real de las políticas empresariales. Entre estos derechos, la norma regula: el derecho a la información sobre el tratamiento, el derecho de acceso, el derecho de rectificación, el derecho de oposición, el derecho de supresión, el derecho a la portabilidad y garantías vinculadas a decisiones individuales automatizadas, incluyendo el derecho a solicitar revisión. La ley dispone exigencias de información mínima al momento de obtención de datos como por ejemplo las categorías de datos, identidad y contacto del responsable, finalidades, base legal, transferencias, canales para ejercer derechos, criterios de conservación, y además prevé reglas procedimentales sobre cómo deben atenderse las solicitudes, incluyendo obligaciones de respuesta y registros de pedidos y denegaciones. Este marco legal obliga a que las ISP tengan que tener canales claros y efectivos, plazos y respuestas que sean razonables y verificables, y constituye un fundamento directo para el componente práctico de esta investigación, que incluye solicitudes de ejercicio de derechos.

La norma establece en el ámbito de seguridad la adopción de medidas adecuadas y la comunicación de los incidentes de seguridad a la autoridad de control y, en su caso, a los titulares. También prevé la designación de un oficial de protección de datos y la realización de evaluaciones de impacto en caso de que el tratamiento de datos reúna ciertos riesgos significativos.

En cuanto a la transferencia internacional de datos personales, establece la regulación correspondiente para garantizar niveles adecuados de protección y el cumplimiento de determinadas condiciones y, por último, establece la creación de la Agencia Nacional de Protección de Datos Personales, como autoridad de control, y le asigna funciones de supervisión, reglamentación y control del ejercicio de la potestad sancionadora.

La existencia de este marco regulatorio integral redefine los requisitos mínimos estándar para las empresas proveedoras de servicios de Internet en Paraguay y es el eje central en torno al cual se estructura la evaluación de esta edición.

Ley N° 6.534/2020 de Protección de Datos Personales Crediticios (Presidencia de la República del Paraguay, 2020). Esta ley, que deroga la anterior Ley N°1.682/2001 y sus modificaciones[2], establece un nuevo marco para la protección de datos e información personal en Paraguay, poniendo más énfasis en tratar los aspectos vinculados a la información crediticia de toda persona, cualquiera sea su nacionalidad, residencia o domicilio, en entidades bancarias, financieras, burós de créditos. Si bien esta ley es sectorial, prevé definiciones relevantes en la materia como la de datos personales y datos personales sensibles, y complementa otras leyes y disposiciones dentro del marco normativo nacional.

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

Asimismo, en concordancia con las disposiciones constitucionales mencionadas, cabe citar a la Ley 642/95 “De telecomunicaciones” (Presidencia de la República del Paraguay, 1995), la cual también garantiza la inviolabilidad del secreto de la correspondencia y del patrimonio documental, salvo por orden judicial (Artículo 89). Esta disposición es aplicable tanto al personal de telecomunicaciones como a cualquier persona o usuario que tenga conocimiento de la existencia o contenido de dichas comunicaciones. Además, la normativa precisa que la inviolabilidad implica la prohibición de abrir, sustraer, interferir, cambiar texto, desviar curso, publicar, usar, tratar de conocer o facilitar a una persona ajena al destinatario tener conocimiento de la existencia o contenido de las comunicaciones confiadas a prestadores de servicios, así como dar ocasión para cometer tales actos (Artículo 90).

En igual sentido, debemos considerar la Ley N° 4.868/2.013 de Comercio Electrónico (Presidencia de la República del Paraguay, 2013); y sus disposiciones complementarias, al igual que la Ley N° 6.822/2.021 De los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos (Presidencia de la República del Paraguay, 2021b) y sus disposiciones complementarias. Según la Ley N.º 6.738/2021 que regula el teletrabajo en relación de dependencia (Presidencia de la República del Paraguay, 2021a), estas normativas tienen un alcance limitado y no abordan de manera integral la protección de datos en el país.

2 Esta ley derogó a la Ley N.º 1682/2001 y sus modificaciones (Ley N.º 1969/2002 y Ley N.º 5543/2015) por el cual se ofrecía una regulación parcial sobre la información privada, aunque con limitaciones. Actualmente esta derogación ha dejando un vacío en la normativa actual.

La Ley de Comercio Electrónico, en su artículo 9, establece que las ISP deben cumplir ciertas obligaciones adicionales, además de las normas vigentes sobre Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente. Estas obligaciones incluyen informar de manera permanente, fácil, directa y gratuita a sus clientes sobre diferentes herramientas técnicas que mejoren la seguridad de la información, como protección contra virus informáticos y programas espía, y la restricción de correos electrónicos no solicitados. También deben informar sobre las herramientas disponibles para filtrar y restringir el acceso a contenidos y servicios no deseados en Internet o perjudiciales para la niñez y la adolescencia. La ISP puede cumplir con esta obligación de información si incluye la información requerida en su página principal de Internet.

Y en su artículo 10, la misma ley establece el deber de retención de datos de tráfico a cargo de los Proveedores de Servicios de Intermediación (acceso a internet) y los Proveedores de Servicios de Alojamiento de Datos, quienes deben almacenar los datos de conexión y tráfico generados durante la prestación de sus servicios por un período mínimo de seis meses. Esta obligación tiene como única finalidad permitir la localización del equipo terminal utilizado por el usuario para transmitir la información, mientras que los proveedores de alojamiento solo deben conservar los datos imprescindibles para identificar el origen de lo alojado y el momento en que comenzó el servicio. La norma prohíbe expresamente utilizar estos datos para fines distintos a los legalmente permitidos y exige adoptar medidas de seguridad adecuadas para evitar su pérdida, alteración o acceso no autorizado. Su incumplimiento se considera una infracción muy grave (Art. 36), sancionable con multas de hasta 1.000 jornales mínimos y, en casos de reincidencia, con el bloqueo del acceso a los servicios del infractor por hasta dos años.

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

Por otro lado, existe normas fragmentadas de protección proactiva de datos personales, por ejemplo se encuentra la Resolución MITIC N.º 733/2019 establece un modelo de gobernanza de seguridad de la información para mejorar la ciberseguridad y la gestión de riesgos en el sector público.

Adicionalmente, normativas como el Decreto N.º 8709/2018, que regula el Sistema de Intercambio de Información (SII), incluyen principios clave como la limitación de la finalidad, la minimización de datos y los derechos ARCO (acceso, restricción, cancelación y oposición). Este sistema maneja tanto datos públicos como privados, diferenciándose de los datos abiertos, que solo abarcan información pública gubernamental.

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

En relación con el marco normativo penal, el Código Procesal Penal establece en su artículo 200 que la intervención de comunicaciones requiere una resolución fundada del juez, cualquiera sea el medio técnico utilizado para conocerlas. El resultado de la intervención debe ser entregada únicamente al Juez que la ordenó, quien podrá requerir la versión escrita de la grabación y ordenar la destrucción de

toda la grabación o de aquellas partes que no guarden relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. El mismo cuerpo normativo, en su artículo 228, otorga al juez y al Ministerio Público la facultad de requerir informes a personas o entidades públicas o privadas. Estos informes pueden solicitarse de forma verbal o escrita, detallando el procedimiento, el nombre del imputado, el lugar de entrega del informe, el plazo para su presentación y las consecuencias por incumplimiento.

Estas normas subrayan la excepcionalidad de la intervención de comunicaciones y la protección de éstas contra la divulgación de su contenido, en consonancia con las disposiciones internacionales y constitucionales que garantizan un enfoque garantista en la legislación penal. Por su parte, aunque no es vinculante, la jurisprudencia reciente también destaca la importancia de la orden judicial como requisito para la legalidad de la intervención, asegurando la salvaguarda de la garantía constitucional de la inviolabilidad de la comunicación privada[3].

Igualmente, cabe mencionar que los contratos para la adquisición de servicios de Internet se encuentran en la categoría de contratos de consumo, por lo que están amparados por la Ley N° 1.334/1998 De Defensa del Consumidor y Del Usuario, y sus modificaciones. Esta legislación protege a los consumidores frente a cláusulas establecidas unilateralmente por el proveedor, sin posibilidad de modificación por parte del consumidor. En este contexto, la misma resulta relevante al evaluar cómo las ISP protegen los derechos de los usuarios y considerar aspectos como la transparencia en las prácticas comerciales, la resolución de reclamos o disputas y los derechos de acceso a la información.

En relación a las conservaciones de datos de tráfico, la ley N° 7.549/2025, titulada “Que dispone la obligatoriedad de la conservación de datos de tráfico para combatir la pornografía relativa a niños y adolescentes y otros hechos punibles”, fue promulgada en el 2025. La ley establece la obligatoriedad de conservar datos de tráfico de servicios de Internet e identificar a las personas usuarias, como herramienta para las investigaciones judiciales de hechos punibles vinculados a la pornografía infantil y adolescente y otros delitos conexos. El núcleo de la ley se encuentra en el Artículo 6°, que obliga a los proveedores de servicios de Internet a conservar los datos de tráfico y conexión de los usuarios por un plazo de doce meses, incluyendo la dirección IP, la identificación del titular del servicio, la fecha y hora de conexión y desconexión, y la etiqueta de localización, aclarando expresamente que estos registros no incluyen el contenido de las comunicaciones sino solo los datos técnicos necesarios para individualizar a los usuarios. El Artículo 10° refuerza que en ningún caso autoriza la vigilancia masiva ni el acceso al contenido de los mensajes de las personas usuarias.

Por su parte se encuentra la Resolución de CONATEL N.º 2583/2024 (CONATEL, 2024) que establece también la obligatoriedad para todos los licenciatarios del servicio de acceso a Internet y transmisión de datos de conservar los registros de conexión. Esta resolución busca registrar los tráficos de datos tales como la dirección de IP (fecha y hora de asignación y liberación de la dirección), en caso de NAT (Network Address Translation) la correspondiente entre las direcciones privadas y pública, así como su almacenamiento obligatorio de hasta 6 meses como periodo mínimo, y habrá sanciones graves aplicadas en el caso que la ISP no colabore. Sin embargo, la resolución no especifica qué autoridades están facultadas para solicitar y tratar estos datos, ni los procedimientos legales necesarios, como la obtención de una orden judicial, para garantizar el respeto al principio del debido proceso. Este vacío regulatorio plantea preocupaciones sobre posibles vulneraciones a los derechos de privacidad y la protección de los datos personales.

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

La comprensión de este contexto resulta fundamental para una adecuada evaluación del desempeño de las empresas de telecomunicaciones en Paraguay y para el diseño de estrategias en el fortalecimiento de la protección de los derechos de las personas usuarias, considerando la interacción entre la legislación, la participación social y las regulaciones específicas que rigen el tratamiento de la privacidad y la protección de datos por parte de estas empresas.

CRITERIOS DE EVALUACIÓN

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

Para esta evaluación se revisaron los contratos de prestación de servicios, informes de sustentabilidad y otros documentos que estaban disponibles en los sitios web de las empresas hasta el 30 de marzo de 2026. También se buscó noticias que circularon en la prensa y los medios especializados y se revisaron los informes de Quién Defiende Tus Datos de años anteriores (TEDIC, 2017, 2020, 2022, 2024) para verificar actualizaciones y avances cualitativos y realizar una comparación final.

En una primera etapa se llevó a cabo una evaluación preliminar con el fin de obtener un primer puntaje para cada una de las empresas analizadas en este estudio y, así, comprender en qué parámetros de cada criterio podrían mejorar para alcanzar una mayor puntuación. Este proceso duró 3 meses y abarcó hasta el 30 de abril del 2026.

Luego de la evaluación preliminar TEDIC se puso en contacto con las empresas para solicitarles una reunión con el propósito de explicar en qué consiste el estudio y presentar los resultados preliminares obtenidos del análisis del 2025 y su comparativo en el tiempo con las ediciones anteriores. En esta reunión se buscó que las empresas pudieran brindar información precisa sobre su trabajo por el resguardo de la privacidad de las personas usuarias, así como también complementar la información que se encuentra disponible públicamente o, incluso, aclarar cualquier ambigüedad que pudiera surgir a partir de la misma.

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

A continuación, se desarrollan cada uno de los ocho criterios de evaluación de las empresas.

1. POLÍTICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

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

Al respecto, tanto la Constitución de la República en su artículo 33 —sobre la intimidad de las personas— como los tratados internacionales protegen el derecho a la intimidad como uno de los pilares de las democracias modernas. Asimismo, organismos internacionales de protección de Derechos Humanos han señalado que las empresas deben establecer e implementar condiciones de servicio que sean transparentes, claras, accesibles, así como 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 las personas usuarias (CIDH, 2013). Es indispensable que la ISP cuente con políticas que cumplan estos protocolos a la hora de entregar información y datos personales a las autoridades.

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

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

Las empresas deben almacenar los metadatos de las personas usuarias por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico Nº 4868/2013 y la Resolución de CONATEL Nº 83/2024. En este escenario, es imprescindible que los ISP describan y den a conocer qué información personal está siendo retenida, así como las medidas para salvaguardar dichos datos ante posibles ataques o riesgos que puedan afectar dicha información.

En un caso contencioso (CIDH, 2009) 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.

En el caso CAJAR contra Colombia (CIDH, 2023b), la sentencia concluyó que Colombia había violado los derechos fundamentales del colectivo de abogados como la privacidad, libertad de expresión y el derecho a defender los derechos humanos. También reconoció la autodeterminación informativa como derecho humano autónomo, enfatizando que las personas tienen control sobre quién accede y usa sus datos personales. También subrayó que la vigilancia invasiva y el acceso a metadatos sensibles, como ubicación, direcciones IP y comunicaciones privadas, requieren estricta autorización judicial para prevenir abusos y garantizar la proporcionalidad de estas medidas. El tribunal condenó las técnicas de espionaje

expansivo utilizadas por Colombia, que incluyen la recopilación indiscriminada de información personal y el acceso a bases de datos no públicas. Además, destacó la importancia de estándares claros en la recolección y tratamiento de metadatos, estableciendo que estos contienen información sensible que puede revelar hábitos, relaciones y movimientos de las personas. Al igual que el caso Escher, esta jurisprudencia nacional sitúa a estos datos en una instancia de protección constitucional y de derechos humanos.

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

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

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

Por último, en esta edición, en el marco de este criterio, también se considera si las compañías cumplen con las disposiciones establecidas en cuanto a la notificación de riesgo o fugas de datos personales (La Política Online, 2024). Se evaluará si tienen acciones de mitigación implementadas y protocolos de notificación a las autoridades en caso de fallas de seguridad que comprometan la información personal de los usuarios de servicios.

2. AUTORIZACIÓN JUDICIAL

La vigilancia sin consentimiento del afectado conlleva riesgos de abusos por las autoridades, por ello resulta imprescindible la autorización de un juez competente. Para solicitar información personal debe haber una autorización del juez competente tal como lo expresan las normas penales y la Constitución de la República del Paraguay. La interceptación de la comunicación privada de las personas tiene carácter excepcional con pena de nulidad en el juicio. Este criterio implica verificar si la ISP cuenta con políticas que cumplan los protocolos para entregar la información a la autoridad judicial. Es decir, detalles del expediente penal, número de causa, datos de la persona, el tipo base penal que incurre el investigado, argumentación legal y firma del juez de la causa.

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

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

La vigilancia sin consentimiento conlleva riesgos de abusos por las autoridades, por ello resulta imprescindible la autorización de un juez competente. Para solicitar información personal debe haber una autorización del juez competente tal como lo expresan las normas penales y la Constitución de la República del Paraguay. En el siguiente cuadro se explica cual el procedimiento para el acceso cumpliendo con los estándares del principio del debido proceso, así como las aplicaciones del código procesal penal paraguayo:

3. NOTIFICACIÓN A LA PERSONA USUARIA

La ISP deberá contar con una política de notificación a las personas usuarias afectadas por medidas de vigilancia estatal, en el primer momento permitido por la ley. Deberá demostrar que han litigado los impedimentos legales o regulatorios para llevar a cabo la notificación y publicar de forma accesible que ha promovido mecanismos de notificación a la persona usuaria al congreso o a otros entes regulatorios. Cuando se notifica a las personas usuarias que sus datos personales o registros de conexión a Internet han sido solicitados por las autoridades administrativas o judiciales se proporcionan condiciones de amplia defensa contra los abusos e irregularidades.

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

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

Sin notificación, la persona usuaria depende de que las propias empresas impugnen contra las solicitudes que consideran abusivas. Si son notificadas por las empresas, las personas usuarias tienen la posibilidad de defenderse de posibles violaciones de su intimidad. Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido por especialistas en Derechos Humanos en Internet y fue plasmado en los Principios Necesarios y Proporcionados que dicen 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 (Necesarios y proporcionados. Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones, 2014)

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 (Naciones Unidas, 2013).

Según la Relatoría Especial para la Libertad de Expresión de la CIDH (CIDH, 2025), cuando no existen sistemas de notificación para las operaciones de vigilancia, el derecho a un recurso efectivo se torna ilusorio. Esto se debe a que las personas no pueden impugnar acciones de las que no tienen conocimiento. En vista de ello, sostiene que los Estados deben establecer sistemas para informar a las personas afectadas cuando dicha notificación ya no contravenga el fin legítimo de la medida de vigilancia, y ha recomendado más específicamente la creación de sistemas de notificación sobre la vigilancia de las personas.

La Relatoría Especial sobre Derechos Humanos de la ONU ha enfatizado que la notificación podría no llevarse a cabo de inmediato en tanto se podría frustrar el éxito de una investigación, pero debería al menos efectuarse cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento no genere un riesgo inminente de peligro a la vida o integridad de alguna persona. No obstante, en Paraguay, la ya referida normativa vigente establece que, ante la noticia de un hecho presuntamente delictivo y en casos excepcionales, se podrá solicitar autorización judicial para intervenir las comunicaciones (Presidencia de la Republica del Paraguay, 1998a); empero, no hay obligación de notificar a la persona investigada durante esta etapa inicial, salvo cuando se formaliza una imputación y se identifica a la presunta persona responsable.

Atendiendo a las recomendaciones internacionales en materia de derechos humanos, las ISP tienen la responsabilidad de actuar con buena fe para salvaguardar la privacidad de las personas usuarias. Esto incluye notificarles sobre eventuales intervenciones en sus comunicaciones, en la medida en que dicha notificación no comprometa los objetivos de la investigación penal. Esta práctica, además, facilita que las personas puedan ejercer su derecho a buscar reparación en caso de que sus derechos hayan sido indebidamente afectados. En casos adversos a la implementación de la política de notificación de la empresa, la ISP deberá combatir judicialmente los impedimentos legales para notificar a las personas usuarias afectadas, cuando ya no frustre el objeto de la medida de vigilancia. Otra medida, sería llevar a cabo acciones de incidencia legislativa o regulatoria para la implementación de mecanismos legales de notificación.

En el contexto de las solicitudes de datos personales, las proveedoras de Internet adquieren un papel esencial en la protección de las garantías procesales de las personas usuarias afectadas. Es decir, la notificación por la empresa permite a la persona usuaria desafiar las solicitudes ilegales: tanto órdenes judiciales sin fundamento, como solicitudes de las autoridades administrativas sin competencia ni justificación. En la situación actual, la persona usuaria depende de los retos realizados por las propias empresas contra las peticiones que consideran abusivas. Si la persona usuaria es notificada, obtiene a la mayor brevedad, la capacidad de defenderse de posibles violaciones de su privacidad. Asimismo, la garantía de notificación está en línea con el derecho a la información a los titulares de datos personales establecido en el art. 27 de la Ley Nº 7593/2025.

Con esto en mente, es importante fomentar la práctica de la notificación a la persona usuaria a través del proyecto “¿Quién defiende tus datos?” (QDTD). En los casos en que las solicitudes de datos no van acompañadas de la obligación de confidencialidad, la notificación es permitida por la ley paraguaya (dada la ausencia de prescripción legal en contrario). La posibilidad de notificación de la persona usuaria puede ser necesaria, no sólo en los casos de solicitudes de datos en procesos civiles, sino también en relación con las solicitudes hechas por otras agencias gubernamentales, tales como el Ministerio de Hacienda o CONATEL. La notificación a la persona usuaria fortalece su capacidad de impugnar legalmente la inclusión de pruebas que sean irrelevantes o no estén relacionadas con los hechos del caso.

En esta edición, se vuelve a poner a esta categoría como una "prima", porque la notificación no es ni una obligación legal impuesta a las empresas ni una práctica generalizada en Paraguay. Es una medida vista como innovadora y en cierta medida costosa, debido a que requiere personal dedicado a las notificaciones. Por estas razones, su adopción revelaría un compromiso especial con el avance de la protección de los derechos de las personas usuarias. La notificación a la persona usuaria a la primera oportunidad legalmente posible, y preferiblemente antes de la divulgación de los datos, colabora con los principios de defensa legal y fomenta una cultura de protección de la privacidad.

4. POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS

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

En este parámetro se analiza si la ISP tiene un posicionamiento institucional público en el que hayan reconocido sus responsabilidades de respeto y protección de derechos humanos, incluyendo el derecho a la privacidad. Para este efecto, se analiza si existe algún posicionamiento que cumpla con las características señaladas por el Principio 16 de los Principios Rectores sobre las Empresas y los Derechos Humanos (Naciones Unidas, 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;
>
> Quede reflejada en las políticas y los procedimientos operacionales necesarios para inculcar el compromiso asumido a nivel de toda la empresa.

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

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

También se evalúa si la misma participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales como pueden ser la Global Network Initiative[4] o Telecommunications Industry Dialogue[5].

Por otro lado, también se considera que la ISP cuente con políticas de participación en las discusiones locales e Internacionales sobre el ecosistema de Internet; los Foros de Gobernanza de Internet (IGF), donde se discuten de forma abierta los principios compartidos, normas, reglas, procesos de toma de decisión y programas, que modelan la evolución y el uso de Internet.

5. TRANSPARENCIA

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

Los informes de transparencia del sector de las TIC en relación con el impacto en la privacidad de las personas usuarias han sido más frecuentes en los últimos años[6]. La publicación de un informe de transparencia sobre las solicitudes de acceso a datos por parte de autoridades de seguridad y justicia debe proveer suficiente información para evaluar el contenido y el alcance de las medidas de vigilancia por parte de las autoridades.

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

Este criterio evalúa la publicación de estadísticas respecto a cuántas solicitudes de información han sido recibidas y cumplidas, así como la inclusión de detalles sobre el tipo de solicitudes, instituciones solicitantes y la motivación y fundamentación de las autoridades.

4 Global Network Initiative https://globalnetworkinitiative.org

5 Telecommunications Industry Dialogue www.telecomindustrydialogue.org

6 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 DE REQUERIMIENTO DE INFORMACIÓN PERSONAL

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

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

Varios análisis regionales, como el proyecto brasileño "Quem Defende Seus Dados?" (InternetLab, 2025), demuestran que las prácticas más avanzadas relacionadas con las solicitudes de datos por parte de las autoridades están concentradas en un pequeño número de empresas que han creado políticas públicas exhaustivas junto con una revisión legal sólida. Entre estas se encuentran empresas globales, como Google y Meta, que tienen políticas sobre las autoridades, criterios de cumplimiento legal y mecanismos adecuados para cuestionar solicitudes excesivas.

En cuanto a las empresas de telecomunicaciones, por ejemplo, Telefónica ha desarrollado documentos de políticas globales basados en una revisión de legalidad, proporcionalidad y revisión de las solicitudes. Sin embargo, el informe ha revelado que en América Latina, la mayoría de los Proveedores de Servicios de Internet tienen un nivel bajo de cumplimiento, caracterizado por la falta de políticas que estén disponibles públicamente con un nivel suficiente de sofisticación, lo que demuestra una brecha considerable en comparación con los estándares globales.

7. ACCESIBILIDAD

La accesibilidad de la información disponible en la web, independientemente de la discapacidad o diversidad funcional de las personas usuarias, es esencial para fortalecer el compromiso con la transparencia y garantizar el respeto a los derechos humanos. La Convención de los Derechos de Personas con Discapacidad (Naciones Unidas, 2006), a través de su artículo 9, reconoce al acceso a las tecnologías de la información y comunicación, incluyendo la web, como un derecho humano básico.

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

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

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

8. CRITERIO SOBRE PROTOCOLO DE ENTREGA DE DATOS PARA INVESTIGACIONES PENALES

¿Se compromete la empresa a seguir la interpretación más protectora de la ley en materia de derecho a la privacidad ante la solicitud de datos personales por parte de agentes del Estado, y cuenta con políticas específicas para estos casos?

La provisión de datos personales en el contexto de las investigaciones penales es uno de los puntos de mayor fricción entre la investigación y la defensa del derecho al resguardo de la intimidad. Este criterio es de especial importancia en la presente edición por la reciente entrada en vigor de la Ley Nº 7593/2025 de Protección de Datos Personales (Presidencia de la República del Paraguay, 2025a), cuya ley establece los principios de legalidad, finalidad, proporcionalidad, minimización y responsabilidad demostrada, los cuales son aplicables a todo tratamiento y comunicación de datos personales.

La nueva ley establece que los requisitos de legalidad y los principios del tratamiento de datos deben ser respetados al comunicar datos a terceros, incluidas autoridades públicas. Por lo tanto, las empresas proveedoras de servicios de Internet deben, además de comprobar la competencia formal de la autoridad solicitante, valorar si la entrega de los datos es compatible con los derechos fundamentales.

Dentro del marco legal de Paraguay, existe una tensión significativa. El artículo 36 de la Constitución Nacional protege el derecho a las comunicaciones, estableciendo que solo pueden ser examinadas o interceptadas por orden de un juez, y sólo en las circunstancias prescritas por la ley. En el mismo sentido, el artículo 200 del Código Procesal Penal establece que para que las comunicaciones sean intervenidas debe haber una resolución judicial y que esto es excepcional (Presidencia de la República del Paraguay, 1998a).

Por otro lado, el artículo 228 del mismo ordenamiento legal habilita al juez y al Ministerio Público a ordenar la presentación de informes de entidades públicas o privadas en el contexto de un procedimiento penal, lo que ha sido utilizado para solicitar datos de registros o registros de conexión sin una orden judicial específica y ha generado un debate legal sobre el alcance de tales facultades cuando se trata de información sujeta al derecho a la privacidad.

Además, la Resolución de Directorio CONATEL № 2583/2024 impone a los prestadores de servicios de telecomunicaciones, obligaciones de conservación y disponibilidad técnica de ciertos datos. Sin embargo, la conservación de datos no significa que se tenga la facultad de entregarlos sin ningún tipo de restricciones ante cualquier solicitud del Estado. La conservación y el acceso son dos planos jurídicos diferentes, que deben ser analizados en el marco de las garantías constitucionales y la ley de protección de datos personales (CONATEL, 2024).

De forma similar, el Decreto № 1.165/14 (Presidencia de la República del Paraguay, 2014), establece que los proveedores deben informar sobre la finalidad del tratamiento de datos, comunicar el destinatario, y emplear medios seguros para el resguardo de dichos datos. Estas obligaciones refuerzan el deber de la empresa de realizar un uso responsable respecto a la información y su comunicación.

La Corte Interamericana de Derechos Humanos en los casos Escher y otros vs. Brasil (CIDH, 2009) y Asociación Civil CAJAR vs. Colombia (CIDH, 2023b) han establecido que tanto el contenido de las comunicaciones como los metadatos pueden contener información sensible, por tanto, cualquier tipo de injerencia debe observar los principios de legalidad, necesidad y proporcionalidad, además de contener estrictas salvaguardias.

Dentro de este escenario normativo, constitucional, procesal penal, sectorial, y ahora integrado en la protección de datos, los ISP desempeñan un papel determinante como garantes intermedios de derechos. La forma en que interpretan sus obligaciones frente a solicitudes fiscales o judiciales impacta directamente en la protección efectiva de la privacidad de los usuarios.

Este criterio evalúa si la empresa adopta la interpretación más protectora posible dentro del marco legal actual y si tiene directrices internas y públicas que estructuran dicha respuesta, especialmente a la luz de la Ley № 7593/2025.

La existencia de protocolos estructurados, claros y accesibles al público demuestra el compromiso institucional de la empresa con el debido proceso y con la protección de la privacidad en el contexto de las investigaciones penales.

REPORTE POR CADA ISP

CRITERIO 1. Política de privacidad y protección de datos personales

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

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

Criterios de evaluación

I. Información sobre la recopilación

La empresa proporciona información clara y completa sobre:

a. qué datos personales se recopilan;

b. en qué situaciones se produce la recopilación;

c. si existe la posibilidad de recopilar datos disponibles públicamente;

d. una lista por nombre, en la política o aviso de privacidad, de los terceros que proporcionan datos a la empresa (incluidos los proveedores de datos públicos); y

e. si existe una evaluación del cumplimiento legal de dichos terceros en materia de protección de datos personales.;

II. Información sobre la finalidad

La empresa proporciona información clara y completa sobre:

a. la finalidad del tratamiento de los datos personales por parte de la propia empresa; y

b. el tipo o la forma en que se lleva a cabo dicho tratamiento.

III. Información sobre almacenamiento, seguridad y uso compartido

La empresa proporciona información clara y completa sobre el almacenamiento, la seguridad y el uso compartido de los datos personales, incluyendo:

a. durante cuánto tiempo y dónde se almacenan los datos;

b. en qué circunstancias los datos son eliminados;

c. si los datos pueden conservarse y en qué condiciones;

d. qué prácticas de seguridad administrativa y técnica se implementan, incluyendo la existencia de políticas de ciberseguridad o de tecnologías de la información (TI) que contemplen protecciones contra malware, ransomware, gusanos y otros tipos de amenazas;

e. si existen controles de acceso a los datos personales, considerando las diferentes categorías de colaboradores;

f. con qué terceros comparte la empresa los datos personales una vez recopilados;

g. con qué fines se realiza dicho uso compartido, incluyendo el uso de software, plataformas digitales, redes o servicios en la nube para fines internos; y

h. cuáles son las hipótesis de transferencia internacional de datos personales.

IV. Información sobre derechos

a. La empresa informa a las personas usuarias sobre sus derechos en materia de protección de datos personales;

b. la empresa informa de manera clara cuáles son los medios disponibles (por ejemplo, correos electrónicos, formularios o portales web) para el ejercicio de dichos derechos.

V. Respuestas a solicitudes de derechos

a. La empresa proporciona información clara y completa sobre la conservación o el acceso a los datos personales cuando estos son solicitados por sus titulares, incluyendo el origen de los datos, la inexistencia de registro, los criterios utilizados y la finalidad del tratamiento, en un plazo máximo de treinta (30) días o en formato simplificado de forma inmediata, según la Ley Nº 7593/25;

b. la empresa responde a las solicitudes de ejercicio de derechos de las personas usuarias en un plazo máximo de un mes.

La verificación de este subcriterio puede realizarse a partir de solicitudes efectivas de acceso a datos personales.

VI. Actualización de la política de privacidad

La empresa se compromete a notificar a las personas usuarias, por ejemplo, mediante correo electrónico, SMS u otros medios directos, en caso de modificaciones en sus prácticas de tratamiento de datos personales.

VII. Accesibilidad

a. La empresa presenta información clara y completa sobre la privacidad y la protección de datos personales de forma accesible en su sitio web (por ejemplo, mediante un portal de privacidad o sección equivalente), garantizando que dicha información también esté disponible en los contratos de adhesión o en las políticas de privacidad aplicables.

Estándar de desempeño:

Estrella llena		La ISP cumple 6 a 7 criterios
Tres cuartos de estrella		La ISP cumple 4 a 5 criterios
Media estrella		La ISP cumple 2 a 3 criterios
Un cuarto de estrella		La ISP cumple 1 solo criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE POR EMPRESA SOBRE LA POLÍTICA DE PRIVACIDAD Y DATOS PERSONALES

STARLINK

Política de privacidad y datos personales		
	Sí	**No**
Información sobre la recopilación La empresa proporciona información clara y completa sobre: (a) qué datos personales se recopilan; (b) en qué situaciones se produce la recopilación; (c) si existe la posibilidad de recopilar datos disponibles públicamente; (d) una lista por nombre, en la política o aviso de privacidad, de los terceros que proporcionan datos a la empresa (incluidos los proveedores de datos públicos); y (e) si existe una evaluación del cumplimiento legal de dichos terceros en materia de protección de datos personales.;		●
Información sobre la finalidad La empresa proporciona información clara y completa sobre: (a) la finalidad del tratamiento de los datos personales por parte de la propia empresa; y (b) el tipo o la forma en que se lleva a cabo dicho tratamiento.	●	
Información sobre almacenamiento, seguridad y uso compartido La empresa proporciona información clara y completa sobre el almacenamiento, la seguridad y el uso compartido de los datos personales, incluyendo: (a) durante cuánto tiempo y dónde se almacenan los datos; (b) en qué circunstancias los datos son eliminados; (c) si los datos pueden conservarse y en qué condiciones; (d) qué prácticas de seguridad administrativa y técnica se implementan, incluyendo la existencia de políticas de ciberseguridad o de tecnologías de la información (TI) que contemplen protecciones contra malware, ransomware, gusanos y otros tipos de amenazas; (e) si existen controles de acceso a los datos personales, considerando las diferentes categorías de colaboradores; (f) con qué terceros comparte la empresa los datos personales una vez recopilados; (g) con qué fines se realiza dicho uso compartido, incluyendo el uso de software, plataformas digitales, redes o servicios en la nube para fines internos; y (h) cuáles son las hipótesis de transferencia internacional de datos personales.		●
Información sobre derechos (a) La empresa informa a las personas usuarias sobre sus derechos en materia de protección de datos personales; (b) la empresa informa de manera clara cuáles son los medios disponibles (por ejemplo, correos electrónicos, formularios o portales web) para el ejercicio de dichos derechos.	●	

Respuestas a solicitudes de derechos (a) La empresa proporciona información clara y completa sobre la conservación o el acceso a los datos personales cuando estos son solicitados por sus titulares, incluyendo el origen de los datos, la inexistencia de registro, los criterios utilizados y la finalidad del tratamiento, en un plazo máximo de treinta (30) días o en formato simplificado de forma inmediata; (b) la empresa responde a las solicitudes de ejercicio de derechos de las personas usuarias en un plazo máximo de un mes. La verificación de este subcriterio puede realizarse a partir de solicitudes efectivas de acceso a datos personales.		●
Actualización de la política de privacidad (a) La empresa se compromete a notificar a las personas usuarias —por ejemplo, mediante correo electrónico, SMS u otros medios directos— en caso de modificaciones en sus prácticas de tratamiento de datos personales.		●
Accesibilidad (a) La empresa presenta información clara y completa sobre la privacidad y la protección de datos personales de forma accesible en su sitio web (por ejemplo, mediante un portal de privacidad o sección equivalente), garantizando que dicha información también esté disponible en los contratos de adhesión o en las políticas de privacidad aplicables.	●	

Starlink proporciona una política de privacidad pública (Starlink, 2026) que describe cómo procesa datos personales en todo el mundo para servicios de Internet que incluyen sus servicios de Internet por satélite. Este documento delimita los diferentes tipos de datos que recopila, las razones de su procesamiento, las medidas de seguridad que tiene implementadas y cómo ponerse en contacto con ellos, permitiendo así una cierta evaluación del cumplimiento de criterios.

No obstante, el análisis debe comprender un componente metodológico esencial: la documentación contractual de la sección sobre Paraguay incluye un “Acuerdo para Honduras”, en el documento versión español (Starlink, s. f.-c), lo que demuestra que la empresa no proporciona un contrato adaptado a la jurisdicción de Paraguay. Este hecho afecta la comprensión del régimen legal aplicable a los usuarios en Paraguay y, en consecuencia, la valoración sobre la accesibilidad y transparencia.

En la evaluación del subcriterio I, nos referimos al informe de Starlink sobre las categorías de datos que podrían recopilar potencialmente, que incluyen datos de identidad, datos de contacto, datos de perfil, datos de carácter financiero, relacionados con transacciones, técnico del cliente o del sitio web técnico, datos de carácter general de localización y datos sobre comunicaciones (Starlink, 2026). También describe las fuentes generales de recopilación, que incluyen la recopilación del usuario, de terceros y mediante cookies/u otras tecnologías de rastreo. Sin embargo, el subcriterio no solo solicita generalizaciones, sino que requiere que la empresa explique si recopila datos de acceso público, nombre a los terceros respectivos de los que obtiene los datos, incluidos los proveedores de datos públicos, e indique la evaluación del cumplimiento legal de los terceros mencionados. En la política actualizada de Starlink, se indica “socios comerciales, subcontratistas, redes publicitarias, proveedores de análisis y proveedores de información de búsqueda”, pero no los nombran, ni proporcionan la evaluación del cumplimiento de las leyes aplicables, si las hay, por parte de los terceros. Por lo tanto, aunque esta información existe, no es clara ni completa según la normativa extendida, y también se debe marcar como no cumplido este subcriterio.

Con respecto al subcriterio II, Starlink cumple con las condiciones. La política enumera los propósitos de recopilación de datos de manera bastante amplia, como la provisión de bienes y servicios, procesamiento de pedidos, pagos, gestión y protección de servicios de relaciones con clientes, servicios de protección empresarial, servicios de soporte y servicios de defensa proactiva contra abusos, entrenamiento de modelos de aprendizaje automático o inteligencia artificial, comunicaciones comerciales, cumplimiento de leyes y solicitudes legales gubernamentales. La política también enumera servicios para protección contra fraudes y otros problemas técnicos, y recopilación de datos para encuestas y análisis para mejorar productos, servicios y marketing. Además, la política describe cómo se procesan los datos mediante el uso de cookies y otras tecnologías de seguimiento con fines de operación del sitio, publicidad, monitoreo de actividades del sitio y del usuario, y análisis del tráfico de actividades del sitio. En esta etapa, el usuario obtiene una idea general de los propósitos del procesamiento de datos y las principales modalidades de procesamiento de datos.

El subcriterio III no se cumple completamente. Starlink afirma que mantiene la información personal mientras la recopilación lo requiera o mientras la ley lo permita. La información de la cuenta se mantiene durante la vida de la cuenta más dos años adicionales, según Starlink. Además, Starlink menciona algunas medidas de protección general, como la encriptación de la información durante la transmisión mediante la tecnología de Starlink, la protección contra brechas físicas y la respuesta de los empleados ante brechas de información personal. La norma exige una explicación transparente y exhaustiva sobre la ubicación de los datos y el calendario de retención, la justificación de la retención, una graduación de restricciones de acceso por rol de empleado y protecciones explícitas contra varios tipos de amenazas en línea. Sin embargo, el estándar requiere la lista completa de destinatarios de transferencia de datos, los motivos por los cuales se permite la transferencia de datos y posibles destinatarios de transferencia de datos en diferentes países.

Esta política aborda algunos de estos temas, pero todavía hay importantes omisiones, como no aclarar la ubicación del almacenamiento de datos o los controles de acceso al almacenamiento de datos en términos del rango de los colaboradores. Además, aunque la Política de Uso Aceptable (Starlink, s. f.-a) y la Política de Gestión del Tráfico (Starlink, s. f.-b) especifican que SpaceX puede evaluar el tráfico de datos para mejorar los servicios y defenderse contra virus o código malicioso, esto sólo puede interpretarse como una forma de gestión de redes, y no como un sistema integral de ciberseguridad o protección de datos personales.

En lo que respecta al uso compartido, Starlink dice que los datos pueden ser compartidos con empleados, proveedores de servicios, empresas socios, procesadores de datos, proveedores de servicios de internet, proveedores de servicios de publicidad y análisis, empresas de respaldo y almacenamiento de datos, y compañías que ayudan con servicios de pago y comunicación. Starlink también afirma que los procesadores de datos y los responsables conjuntos del tratamiento de datos pueden comprar y vender datos, proporcionar datos a sus socios comerciales, y utilizar los datos de los clientes para entrenar su IA, comunicarse con los clientes, analizar y ayudar a los clientes con sus derechos legales. Sin embargo, no especificaron a qué terceros están vendiendo datos ni cómo se transferirían internacionalmente sus datos. Por lo tanto, está parcialmente completo, pero no cumple con la totalidad del subcriterio.

El subcriterio IV, información sobre derechos, sí se cumple. Starlink informa al usuario que puede tener derechos legales para acceder, actualizar, eliminar, restringir u oponerse al procesamiento de cierta información personal. Además, se proporciona la dirección de correo electrónico privacy@spacex.com como medio para ejercer dichos derechos. También se hace referencia a anexos específicos para ciertas jurisdicciones, incluyendo los EE. UU., EEE+, México, Brasil, Nigeria y Corea del Sur. Aunque no existe un anexo para Paraguay, el estándar se refiere a la notificación de derechos y los medios para ejercer estos derechos, ambos presentes, por lo que esto debe considerarse cumplido.

La respuesta a las solicitudes de derechos, subcriterio V, no se cumple. Aunque la política menciona un canal para hacer valer los derechos, no indica que Starlink brindará una respuesta en un plazo de quince días, ni una respuesta simplificada e inmediata, ni en un plazo máximo de un mes. La política tampoco menciona que la respuesta incluirá información sobre la existencia o inexistencia de datos personales del solicitante en sus bases de datos, así como los criterios y finalidades del tratamiento realizado. La política incluso señala que puede solicitar información adicional para verificar la identidad de la persona solicitante, pero no desarrolla los plazos ni el contenido de respuesta exigidos por el criterio.

Para el subcriterio VI, sobre actualizaciones de la política de privacidad, Starlink no cumple. Starlink afirma que las actualizaciones de la política pueden reflejar cambios en las prácticas, mandatos legales y los servicios ofrecidos, y que la política debe ser revisada periódicamente. La política también indica que, al continuar usando el sitio o los servicios, los usuarios aceptan los términos actualizados. Esta política carga la responsabilidad del cumplimiento en el usuario, y no compromete a notificar directamente mediante medios electrónicos los cambios en las prácticas de procesamiento de datos. La Política de Uso Aceptable (Starlink, s. f.-a) establece que los cambios entran en vigencia después de que SpaceX publica o envía los cambios en starlink.com/legal. Esto tampoco incluye una notificación directa de actualización de la política de procesamiento de datos personales.

Finalmente, el subcriterio VII, accesibilidad, se cumple en términos formales. Starlink pública su política de privacidad y materiales adicionales en su portal legal. El texto se estructura en secciones claras: información recopilada, fuentes de información recopilada, propósitos de la recopilación, intercambio de información, protección de la información, derechos del usuario, política infantil, retención de información, política sobre sitios de terceros, política de cambios y contacto. Aunque el documento es global, no incluye un anexo específico para Paraguay, la información existe en español y se explica en un documento de privacidad que es específico para el servicio. Dentro de este subcriterio, se justifica el cumplimiento, teniendo en cuenta que la accesibilidad en la práctica está parcialmente limitada debido a la ausencia de adaptación local.

Conforme al estándar de desempeño establecido, Starlink cumple
con 3 de 7 subcriterios por lo que califica con media estrella.

Claro

CLARO – AMX PARAGUAY S.A

Política de privacidad y datos personales		
	Sí	**No**
Información sobre la recopilación La empresa proporciona información clara y completa sobre: (a) qué datos personales se recopilan; (b) en qué situaciones se produce la recopilación; (c) si existe la posibilidad de recopilar datos disponibles públicamente; (d) una lista por nombre, en la política o aviso de privacidad, de los terceros que proporcionan datos a la empresa (incluidos los proveedores de datos públicos); y (e) si existe una evaluación del cumplimiento legal de dichos terceros en materia de protección de datos personales.;		●
Información sobre la finalidad La empresa proporciona información clara y completa sobre: (a) la finalidad del tratamiento de los datos personales por parte de la propia empresa; y (b) el tipo o la forma en que se lleva a cabo dicho tratamiento.	●	
Información sobre almacenamiento, seguridad y uso compartido La empresa proporciona información clara y completa sobre el almacenamiento, la seguridad y el uso compartido de los datos personales, incluyendo: (a) durante cuánto tiempo y dónde se almacenan los datos; (b) en qué circunstancias los datos son eliminados; (c) si los datos pueden conservarse y en qué condiciones; (d) qué prácticas de seguridad administrativa y técnica se implementan, incluyendo la existencia de políticas de ciberseguridad o de tecnologías de la información (TI) que contemplen protecciones contra malware, ransomware, gusanos y otros tipos de amenazas; (e) si existen controles de acceso a los datos personales, considerando las diferentes categorías de colaboradores; (f) con qué terceros comparte la empresa los datos personales una vez recopilados; (g) con qué fines se realiza dicho uso compartido, incluyendo el uso de software, plataformas digitales, redes o servicios en la nube para fines internos; y (h) cuáles son las hipótesis de transferencia internacional de datos personales.		●
Información sobre derechos (a) La empresa informa a las personas usuarias sobre sus derechos en materia de protección de datos personales; (b) la empresa informa de manera clara cuáles son los medios disponibles (por ejemplo, correos electrónicos, formularios o portales web) para el ejercicio de dichos derechos.	●	

Respuestas a solicitudes de derechos (a) La empresa proporciona información clara y completa sobre la conservación o el acceso a los datos personales cuando estos son solicitados por sus titulares, incluyendo el origen de los datos, la inexistencia de registro, los criterios utilizados y la finalidad del tratamiento, en un plazo máximo de treinta (30) días o en formato simplificado de forma inmediata; (b) la empresa responde a las solicitudes de ejercicio de derechos de las personas usuarias en un plazo máximo de un mes. La verificación de este subcriterio puede realizarse a partir de solicitudes efectivas de acceso a datos personales.		●
Actualización de la política de privacidad (a) La empresa se compromete a notificar a las personas usuarias —por ejemplo, mediante correo electrónico, SMS u otros medios directos— en caso de modificaciones en sus prácticas de tratamiento de datos personales.		●
Accesibilidad (a) La empresa presenta información clara y completa sobre la privacidad y la protección de datos personales de forma accesible en su sitio web (por ejemplo, mediante un portal de privacidad o sección equivalente), garantizando que dicha información también esté disponible en los contratos de adhesión o en las políticas de privacidad aplicables.	●	

Claro cuenta con una política de privacidad (AMX Paraguay S.A., s. f.-a) pública y localizada para Paraguay, en la que identifica a AMX Paraguay S.A. como responsable del tratamiento de datos personales. Este documento tiene una estructura diseñada para explicar qué datos se recopilan, el propósito, el proceso de recopilación y el uso final, y proporciona, en el contexto de las telecomunicaciones, un examen bastante exhaustivo del procesamiento de datos personales. Asimismo, los términos y condiciones del servicio de Internet WiFi (AMX Paraguay S.A., s. f.-c) y de la plataforma Mi Claro (AMX Paraguay S.A., s. f.-b) ofrecen información adicional, especialmente relacionada con la firma de contratos, análisis crediticio y el uso de medios digitales.

Los documentos analizados no indican fecha de última actualización visible. Por lo tanto, no es posible establecer la validez temporal de las políticas aplicables y el estado real del procesamiento de datos personales al que apuntan las prácticas. Aunque este elemento no afecta directamente la puntuación asignada, constituye una restricción significativa respecto a la evaluación de la transparencia de la empresa.

Con respecto al subcriterio I Información sobre la recopilación, Claro identifica el tipo de datos personales recopilados que son principalmente de identificación, contacto y referencia, datos de activos y/o datos técnicos asociados al uso de los servicios. Además, Claro menciona que los datos personales pueden ser recopilados u obtenidos por otros medios, incluyendo repositorios públicos y/o privados, y a través de evaluaciones comerciales crediticias y/o comerciales.

Aun así, el criterio de evaluación busca un mayor nivel de detalle. Específicamente, la empresa no menciona a los terceros, ni elabora sobre la posible evaluación del cumplimiento legal en protección de datos de dichos terceros. Finalmente, tampoco categoriza de manera diferenciada la recopilación de información pública disponible.

En consecuencia, si bien existe información sobre recopilación, esta no es lo suficientemente clara y completa conforme al estándar exigido.

Con el subcriterio II Información sobre la finalidad, Claro cumple con este requisito ya que su política de privacidad explica los propósitos primarios y secundarios del procesamiento de datos personales. Los propósitos primarios están relacionados con la prestación de servicios, facturación, administración del cliente, atención al cliente, evaluación de crédito y obligaciones contractuales. Los propósitos secundarios están asociados al marketing, investigación y mejora de servicios.

Además, los términos y condiciones de Mi Claro (AMX Paraguay S.A., s. f.-b) amplían aún más estos propósitos, añadiendo usos como la autogestión, evaluación de comportamiento, autenticación de identidad y personalización de servicios.

La información puesta a disposición es adecuada para que los usuarios comprendan el propósito del uso de sus datos personales, así como la forma de procesamiento involucrada.

En el ámbito del subcriterio III Información sobre almacenamiento, seguridad y uso compartido, Claro proporciona información general sobre el uso compartido de datos personales y algunas referencias a medidas de seguridad. En su política de privacidad indica que los datos pueden ser compartidos con terceros en determinados supuestos, como el consentimiento de la persona usuaria, el procesamiento externo de datos y el cumplimiento de obligaciones legales. Asimismo, menciona que puede transferir información a afiliadas, subsidiarias y proveedores de servicios que participan en la prestación del servicio.

En materia de seguridad, la empresa señala la implementación de medidas generales, como mecanismos de protección de la información, restricciones de acceso a datos personales y el uso de herramientas orientadas a resguardar la confidencialidad de la información.

Sin embargo, esta información no cubre de manera suficiente el núcleo del subcriterio. La política no establece plazos concretos de conservación de los datos personales, ni detalla las condiciones específicas en las que estos son eliminados o retenidos. Tampoco desarrolla de manera clara los controles de acceso diferenciados según categorías de colaboradores, ni describe de forma precisa las medidas técnicas de seguridad frente a riesgos específicos como malware, ransomware u otras amenazas.

Por lo tanto, la ausencia de información detallada sobre la estructura del almacenamiento, mantenimiento y protección de los datos personales impide que este subcriterio pueda considerarse cumplido.

En materia del subcriterio IV Información sobre derechos, Claro informa a las personas usuarias sobre la existencia de ciertos derechos en materia de protección de datos personales, incluyendo acceso, actualización, rectificación, cancelación y revocación del consentimiento, y como tal, Claro ofrece vías a través de sus centros de atención y plataformas digitales para facilitar el ejercicio de estos derechos.

Dicho esto, el proceso, aunque amigable para los participantes, carece de componentes que hagan que el proceso sea robusto y correcto, como lo demuestra el hecho de que la política no tenga una sección que explique metódicamente el alcance de los derechos a la protección de la privacidad de los datos y el proceso mediante el cual estos derechos pueden ser ejercidos.

La empresa, sin embargo, cumple con el requisito del subcriterio, que implica explicar los derechos y la manera en que estos pueden ser ejercidos a los clientes de la empresa.

En cuanto al subcriterio V Respuestas a solicitudes de derechos, Claro no detalla de manera clara ningún plazo ni proceso que se refiera a las solicitudes de derechos de los usuarios. La política carece de un plazo de respuesta y no brinda orientación respecto a la respuesta y qué incluir. Además, debe incluir la fuente de los datos y los criterios, y el propósito del procesamiento.

La ausencia de estos elementos indica que la empresa puede reconocer los derechos, pero no asegura que estos sean ejercidos a través de un proceso verificable.

Respecto al subcriterio VI Actualización de la política de privacidad, la política de privacidad de Claro establece que puede ser modificada en cualquier momento, con las revisiones publicadas en el sitio y se recomienda a los usuarios que consulten regularmente.

Sin embargo, la política de Claro no menciona la obligación directa de notificaciones por correo electrónico, SMS u otros medios de comunicación directa a los usuarios en caso de algunos cambios que puedan ocurrir en las prácticas de procesamiento de datos.

Este método pone la carga de supervisión en los usuarios y no cumple con el estándar esperado.

Para el subcriterio VII Accesibilidad, Claro exhibe su política de privacidad y otros documentos en su sitio web en español y en una presentación institucional transparente. Además, los múltiples documentos contractuales están relacionados entre sí y permiten la identificación del marco general para el tratamiento de datos personales.

La información proporcionada, a pesar de estar dividida en varios documentos, sigue siendo localizable y accesible para el usuario.

Conforme al estándar de desempeño establecido, Claro cumple con
3 de 7 subcriterios por lo que califica con media estrella.

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

Política de privacidad y datos personales		
	Sí	**No**
Información sobre la recopilación La empresa proporciona información clara y completa sobre: (a) qué datos personales se recopilan; (b) en qué situaciones se produce la recopilación; (c) si existe la posibilidad de recopilar datos disponibles públicamente; (d) una lista por nombre, en la política o aviso de privacidad, de los terceros que proporcionan datos a la empresa (incluidos los proveedores de datos públicos); y (e) si existe una evaluación del cumplimiento legal de dichos terceros en materia de protección de datos personales.		●
Información sobre la finalidad La empresa proporciona información clara y completa sobre: (a) la finalidad del tratamiento de los datos personales por parte de la propia empresa; y (b) el tipo o la forma en que se lleva a cabo dicho tratamiento.	●	
Información sobre almacenamiento, seguridad y uso compartido La empresa proporciona información clara y completa sobre el almacenamiento, la seguridad y el uso compartido de los datos personales, incluyendo: (a) durante cuánto tiempo y dónde se almacenan los datos; (b) en qué circunstancias los datos son eliminados; (c) si los datos pueden conservarse y en qué condiciones; (d) qué prácticas de seguridad administrativa y técnica se implementan, incluyendo la existencia de políticas de ciberseguridad o de tecnologías de la información (TI) que contemplen protecciones contra malware, ransomware, gusanos y otros tipos de amenazas; (e) si existen controles de acceso a los datos personales, considerando las diferentes categorías de colaboradores; (f) con qué terceros comparte la empresa los datos personales una vez recopilados; (g) con qué fines se realiza dicho uso compartido, incluyendo el uso de software, plataformas digitales, redes o servicios en la nube para fines internos; y (h) cuáles son las hipótesis de transferencia internacional de datos personales.		●
Información sobre derechos (a) La empresa informa a las personas usuarias sobre sus derechos en materia de protección de datos personales; (b) la empresa informa de manera clara cuáles son los medios disponibles (por ejemplo, correos electrónicos, formularios o portales web) para el ejercicio de dichos derechos.	●	

Respuestas a solicitudes de derechos (a) La empresa proporciona información clara y completa sobre la conservación o el acceso a los datos personales cuando estos son solicitados por sus titulares, incluyendo el origen de los datos, la inexistencia de registro, los criterios utilizados y la finalidad del tratamiento, en un plazo máximo de treinta (30) días o en formato simplificado de forma inmediata; (b) la empresa responde a las solicitudes de ejercicio de derechos de las personas usuarias en un plazo máximo de un mes. La verificación de este subcriterio puede realizarse a partir de solicitudes efectivas de acceso a datos personales.		●
Actualización de la política de privacidad (a) La empresa se compromete a notificar a las personas usuarias —por ejemplo, mediante correo electrónico, SMS u otros medios directos— en caso de modificaciones en sus prácticas de tratamiento de datos personales.		●
Accesibilidad (a) La empresa presenta información clara y completa sobre la privacidad y la protección de datos personales de forma accesible en su sitio web (por ejemplo, mediante un portal de privacidad o sección equivalente), garantizando que dicha información también esté disponible en los contratos de adhesión o en las políticas de privacidad aplicables.	●	

Tigo ha establecido un marco de documentación bastante completo para la protección de datos personales, que incluye su Política de Privacidad (Tigo Paraguay, 2025a), sus Términos y condiciones de uso de web (Tigo Paraguay, 2025b) y su Contrato único de servicios de telecomunicaciones (Tigo Paraguay, 2025c). En conjunto, estos instrumentos ayudan a construir una imagen más completa de cómo se procesan los datos personales tanto durante la contratación como en la prestación de servicios.

Un elemento positivo es que la Política de Privacidad de Tigo indica de manera expresa su fecha de última actualización, siendo la versión vigente al 5 de agosto de 2025. Esto garantiza un grado de transparencia, ya que se puede verificar el período de vigencia del documento, así como cualquier cambio en las prácticas de procesamiento de datos de las personas.

No obstante, tener una estructura de documento más compleja no garantiza el cumplimiento en todos los aspectos. Según el estándar actual, el análisis distingue entre información suficiente sobre la esencia de un subcriterio e información insuficiente si falta un elemento estructural crucial.

Con respecto al subcriterio I Información sobre la recopilación, Tigo proporciona una descripción amplia de los datos personales que recopila. En su Política de Privacidad describe categorías de datos personales y los medios de recopilación, incluyendo interacción directa con la persona usuaria, uso de servicios digitales y recopilación automática mediante cookies u otras tecnologías.

El Contrato único de servicios complementa presenta esta información al establecer que se recopilan datos personales, crediticios y financieros, así como datos biométricos, incluyendo huellas dactilares, voz e imagen del rostro. Asimismo, señala que la provisión de estos datos es obligatoria para la contratación del servicio y que la empresa puede verificar su veracidad o recabar información adicional a través de terceros, como burós de crédito o entidades especializadas.

Sin embargo, el estándar exige aún mayor precisión. En particular, la empresa no identifica a los terceros que proporcionan datos personales, ni proporciona ninguna descripción de un mecanismo para evaluar el cumplimiento legal de estos terceros. Esta ausencia afecta el corazón del subcriterio, ya que priva de una comprensión clara de los orígenes externos de los datos y de las garantías existentes para los proveedores de datos.

Tigo cumple con el subcriterio II Información sobre la finalidad. La Política de Privacidad establece finalidades generales del tratamiento, que se complementan con mayor detalle con el contenido del contrato único de servicios.

En este sentido, el contrato explica que los datos se procesan con fines de prestación del servicio, gestión de la relación contractual, comercialización de productos y servicios, realización de comunicaciones y encuestas, análisis del consumo, mejora del servicio y prevención del fraude.

Además, establece el procesamiento específico de datos biométricos para los fines de identidad, ciberseguridad y prevención de delitos.

La información divulgada facilita al usuario del servicio tener una visión clara de los objetivos generales y los medios del procesamiento.

En materia del subcriterio III Información sobre almacenamiento, seguridad y uso compartido, Tigo comparte algunos detalles sobre el intercambio de datos personales, parte del almacenamiento y parte de la seguridad, permitiendo al usuario adquirir una comprensión amplia del proceso de gestión de datos en el contexto de su operación.

El Contrato único establece que el usuario otorga permiso a la empresa para transmitir sus datos personales a terceros que proporcionen servicios o productos, socios comerciales, empresas afiliadas, filiales y empresas del mismo grupo, ya sea dentro del país o en el extranjero, como parte de la prestación de los servicios.

La Política de Privacidad menciona que los datos pueden ser compartidos con terceros para servicios de almacenamiento internos y externos, recopilación, atención al cliente y cumplimiento de requisitos legales.

No obstante, la información revela algunas restricciones importantes. La empresa no especifica cuánto tiempo retendrá los datos, indicando solo que los datos se conservarán el tiempo necesario para lograr el propósito para el cual fueron procesados o mientras sea necesario de acuerdo con los requisitos legales. Además, no explica las condiciones para la eliminación, controles de acceso diferenciados o medidas específicas para la protección de datos contra amenazas específicas.

La información no cubre de manera completa todos los elementos exigidos por el criterio, y no resulta suficiente para cumplido con la exigencia del estándar.

Tigo cumple con el subcriterio IV Información sobre derechos ya que el Contrato único establece expresamente que el usuario tiene el derecho a conocer los mecanismos para acceder, actualizar, rectificar, eliminar, suprimir, oponerse y portar sus datos personales, a través del aviso de privacidad.

Este reconocimiento explícito es más exhaustivo y está mejor organizado que la mayoría de las otras ISPs analizadas, ya que especifica los derechos y los relaciona con el tratamiento de los datos personales.

No obstante, la política podría mejorarse definiendo mejor cada derecho, así como los procedimientos para su ejercicio.

En cuanto al subcriterio V Respuestas a solicitudes de derechos, Tigo no cumple con este subcriterio. Reconoce derechos en cierta medida, pero no especifica procedimientos ni crea marcos para responder a solicitudes de acceso, rectificación, eliminación, dentro de períodos definidos.

Este estándar requiere que se indiquen plazos de respuesta, al menos el marco de respuesta, y qué mecanismos de respuesta estarán en su lugar. La ausencia de estos elementos sugiere que no hay garantía para el ejercicio de estos derechos.

En lo relativo al subcriterio VI Actualización de la política de privacidad, Tigo menciona cuándo actualiza su política de privacidad, sin embargo, hay una falta de evidencia de que Tigo se comprometa a notificar a los usuarios cuando los métodos de procesamiento de datos personales sean actualizados.

El Contrato Único indica que la comunicación puede realizarse mediante medios electrónicos. Sin embargo, esto no está específicamente relacionado con cambios en la política de privacidad, ni existe una obligación de notificar directamente al usuario sobre los cambios.

En términos del subcriterio VII (Accesibilidad), Tigo cumple con los requisitos evaluados. La Política de Privacidad se encuentra disponible en la página web institucional y puede accederse fácilmente desde el pie de página. Asimismo, la empresa permite consultar el contrato único de servicios de telecomunicaciones antes de la contratación, lo que contribuye a una mayor transparencia en la relación con las personas usuarias.

Si bien los distintos documentos vinculados al tratamiento de datos personales, como la política de privacidad, el contrato de servicios y otros términos aplicables, no necesariamente presentan el mismo nivel de visibilidad o facilidad de acceso, en conjunto permiten a la persona usuaria obtener una comprensión razonablemente completa sobre el tratamiento de sus datos personales durante la contratación y la prestación de los servicios. La relación entre estos instrumentos contribuye a generar un entendimiento adecuado de las prácticas de tratamiento de datos implementadas por la empresa.

Conforme al estándar de desempeño establecido, Tigo cumple con 3 de 7 subcriterios por lo que califica con media estrella.

personal

PERSONAL - NÚCLEO S.A.

Política de privacidad y datos personales		
	Sí	**No**
Información sobre la recopilación La empresa proporciona información clara y completa sobre: (a) qué datos personales se recopilan; (b) en qué situaciones se produce la recopilación; (c) si existe la posibilidad de recopilar datos disponibles públicamente; (d) una lista por nombre, en la política o aviso de privacidad, de los terceros que proporcionan datos a la empresa (incluidos los proveedores de datos públicos); y (e) si existe una evaluación del cumplimiento legal de dichos terceros en materia de protección de datos personales.;		●
Información sobre la finalidad La empresa proporciona información clara y completa sobre: (a) la finalidad del tratamiento de los datos personales por parte de la propia empresa; y (b) el tipo o la forma en que se lleva a cabo dicho tratamiento.	●	
Información sobre almacenamiento, seguridad y uso compartido La empresa proporciona información clara y completa sobre el almacenamiento, la seguridad y el uso compartido de los datos personales, incluyendo: (a) durante cuánto tiempo y dónde se almacenan los datos; (b) en qué circunstancias los datos son eliminados; (c) si los datos pueden conservarse y en qué condiciones; (d) qué prácticas de seguridad administrativa y técnica se implementan, incluyendo la existencia de políticas de ciberseguridad o de tecnologías de la información (TI) que contemplen protecciones contra malware, ransomware, gusanos y otros tipos de amenazas; (e) si existen controles de acceso a los datos personales, considerando las diferentes categorías de colaboradores; (f) con qué terceros comparte la empresa los datos personales una vez recopilados; (g) con qué fines se realiza dicho uso compartido, incluyendo el uso de software, plataformas digitales, redes o servicios en la nube para fines internos; y (h) cuáles son las hipótesis de transferencia internacional de datos personales.		●
Información sobre derechos (a) La empresa informa a las personas usuarias sobre sus derechos en materia de protección de datos personales; (b) la empresa informa de manera clara cuáles son los medios disponibles (por ejemplo, correos electrónicos, formularios o portales web) para el ejercicio de dichos derechos.	●	

Respuestas a solicitudes de derechos (a) La empresa proporciona información clara y completa sobre la conservación o el acceso a los datos personales cuando estos son solicitados por sus titulares, incluyendo el origen de los datos, la inexistencia de registro, los criterios utilizados y la finalidad del tratamiento, en un plazo máximo de treinta (30) días o en formato simplificado de forma inmediata; (b) la empresa responde a las solicitudes de ejercicio de derechos de las personas usuarias en un plazo máximo de un mes. La verificación de este subcriterio puede realizarse a partir de solicitudes efectivas de acceso a datos personales.		●
Actualización de la política de privacidad (a) La empresa se compromete a notificar a las personas usuarias —por ejemplo, mediante correo electrónico, SMS u otros medios directos— en caso de modificaciones en sus prácticas de tratamiento de datos personales.		●
Accesibilidad (a) La empresa presenta información clara y completa sobre la privacidad y la protección de datos personales de forma accesible en su sitio web (por ejemplo, mediante un portal de privacidad o sección equivalente), garantizando que dicha información también esté disponible en los contratos de adhesión o en las políticas de privacidad aplicables.	●	

Personal presenta un conjunto documental compuesto por su Política de Privacidad (Personal Paraguay, s. f.-a), Términos y condiciones generales (Personal Paraguay, s. f.-b) y Términos y condiciones de aplicaciones (Personal Paraguay, s. f.-c). Los parámetros de estos documentos delinean los componentes principales del procesamiento de datos personales en el ámbito del servicio, aunque con un nivel de integración menor en comparación con otras ISPs analizadas.

A diferencia de Tigo y de igual forma que Claro, la política de privacidad no establece, de manera clara y evidente, una fecha de última modificación, lo que dificulta la evaluación de la vigencia temporal de las prácticas descritas. Este elemento constituye una deficiencia en materia de transparencia.

Respecto al subcriterio I Información sobre la recopilación, Personal proporciona información sobre las categorías de datos personales que recopila a través de su Política de Privacidad y documentos asociados. Los datos recolectados describen identificación y contacto, datos necesarios para proporcionar servicios, e información creada al utilizar plataformas y aplicaciones.

Los Términos y Condiciones para las aplicaciones complementan esta información y establecen que también se puede recopilar información sobre el uso de los servicios proporcionados digitalmente, cómo interactúa el usuario con las plataformas y datos sobre el comportamiento de los usuarios.

Sin embargo, el subcriterio necesita más detalle. Personal no nombra formalmente a las terceras partes que comparten datos personales. Tampoco mencionan un mecanismo para garantizar que las terceras partes actúen legalmente. Tampoco explican la recolección diferenciada de datos de fuentes públicas.

Sin estos elementos diferenciados, es imposible comprender el origen externo de los datos personales y las protecciones existentes para las terceras partes que los suministran.

Personal cumple con el subcriterio II Información sobre la finalidad, la Política de Privacidad y los Términos y Condiciones indican que el procesamiento de datos personales tiene como finalidad proporcionar servicios, gestionar la contratación de servicios, atender a los clientes, facturar, comunicarse, ofrecer productos y servicios y mejorar los servicios.

Los términos de uso de la aplicación describen los propósitos en el contexto del uso de la plataforma digital, incluyendo la personalización, análisis de comportamiento y mejora de la experiencia del usuario.

Esta información hace evidente el propósito y el contexto del procesamiento de datos personales.

De la misma forma en el subcriterio III Información sobre almacenamiento, seguridad y uso compartido, Personal no cumple este subcriterio. Aunque describe en términos generales el procesamiento de datos personales y menciona la posibilidad de compartir datos con terceros en la prestación de servicios o en caso de cumplimiento de la ley, lo cual es insuficiente para cubrir la sustancia del subcriterio.

La documentación no determina límites de tiempo específicos para el almacenamiento de datos y no especifica bajo qué circunstancias los datos pueden ser eliminados o, prolongados, ni especifica las medidas técnicas de seguridad o el control de acceso diferenciado, y no detalla los terceros a quienes se comparte la información.

Desde este punto de vista, los datos disponibles no explican de manera adecuada y suficiente el almacenamiento de datos personales, la seguridad del almacenamiento y la gestión de los datos desde el inicio hasta el fin del ciclo de vida del almacenamiento.

La Política de Privacidad informa a las personas sobre sus derechos de protección de datos personales y detalla en cierta medida el marco procedimental sobre cómo deben ejercerse.

Se reconocen y describen los derechos de acceso, rectificación y actualización de datos, junto con los medios y canales disponibles para que los usuarios presenten sus solicitudes de datos personales.

No obstante, se debería proporcionar información más transparente sobre el alcance de cada derecho y el marco procedimental correspondiente de cómo pueden ejercerse.

En relación con el subcriterio V, relativo a la respuesta a las solicitudes de ejercicio de derechos, Personal no cumple con dicho subcriterio. Aunque acepta derechos, no ha establecido plazos ni métodos para responder a las solicitudes para que los usuarios ejerzan derechos.

El estándar requiere información sobre el tiempo de respuesta, el contenido mínimo de las respuestas y mecanismos específicos de atención. Si alguno de estos elementos falta, no se garantiza el ejercicio efectivo de los derechos.

En materia del subcriterio VI Actualización de la política de privacidad, Personal no cumple este subcriterio. Si bien puede actualizar sus políticas y condiciones, no hay una obligación de informar a los usuarios sobre los cambios relacionados con sus operaciones respecto a la recopilación y el procesamiento de sus datos personales.

La ausencia de sistemas de notificación directa en esencia responsabiliza a los usuarios de monitorear los documentos periódicamente para detectar cambios y/o otras actualizaciones en los documentos. Esto no cumple con el nivel adecuado en este aspecto.

Por lo que se refiere al subcriterio VII. Accesibilidad, Personal cumple con este subcriterio. La Política de Privacidad y los Términos y Condiciones están publicados en el sitio web institucional y se pueden acceder fácilmente por los usuarios.

Además, los documentos están estructurados en secciones fáciles de usar en el sitio web, permitiendo a los usuarios encontrar fácilmente la información relevante.

Conforme al estándar de desempeño establecido, Personal cumple con 3 de 7 subcriterios por lo que califica con media estrella.

CRITERIO 2. Autorización judicial

¿Se compromete la ISP a divulgar información del cliente, metadatos y contenidos de las comunicaciones únicamente en presencia de una orden judicial?

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

Criterios de evaluación

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

II. Si diferencia la entrega de los datos con respecto a los metadatos y se compromete a hacerlo siempre que medie la existencia de una orden judicial previa.

Estándar de desempeño:

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

REPORTE - AUTORIZACIÓN JUDICIAL

STARLINK

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

Starlink regula el acceso a los datos personales de sus usuarios principalmente a través de su Política de Privacidad (Starlink, 2026) y sus Términos de Servicio (Starlink, s. f.-c). Estos documentos contienen disposiciones sobre divulgación de información a autoridades, pero no establecen garantías suficientes en relación con la exigencia de orden judicial previa.

En cuanto al subcriterio I Entrega de contenido de comunicaciones Starlink no hace mención acerca de entregar contenido de comunicaciones exclusivamente en caso de una orden judicial.

Según su Política de Privacidad, la empresa puede divulgar información personal para cumplir con demandas legales, regulatorias o gubernamentales. Este uso del lenguaje donde “la empresa está obligada por ley”, o “para cumplir con obligaciones legales”, no está cerrado a la existencia de una orden judicial, sino que mantiene la opción de proporcionar datos ante diversos niveles de requerimientos gubernamentales.

Este enfoque es problemático desde el estándar evaluado, ya que no diferencian los niveles de exigencias legales, ni garantizan que los datos de comunicación de los usuarios permanezcan sujetos a un control previo judicial de acceso.

A partir de la ausencia del requisito expreso de una orden judicial, podemos concluir que la empresa puede tener una discreción amplia para determinar cuándo divulgar los datos, lo que afecta negativamente la privacidad de los usuarios.

Respecto al subcriterio II Diferenciación de metadatos y exigencia de orden judicial Starlink tampoco cumple con este subcriterio. En los documentos evaluados, no hay una diferenciación identificable entre el contenido de las comunicaciones y los metadatos.

En la política de privacidad, la compañía recurre a categorías amplias y genéricas, por ejemplo, en relación con “información personal” o “datos del usuario”, sin necesariamente hacer una diferenciación respecto a los diversos tipos de datos o los niveles de protección que puedan aplicar. También no articula ninguna diferenciación respecto a la provisión de metadatos y no solicita la existencia de una orden para el acceso por parte de las autoridades.

Esta ausencia es relevante, ya que el subcriterio exige no solo la diferenciación entre contenido y metadatos, sino también el compromiso de someter ambos a la exigencia de orden judicial previa.

Al no cumplir ninguna de estas condiciones, la empresa no satisface el estándar establecido.

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

CLARO - AMX PARAGUAY S.A.

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

Claro Paraguay no menciona en su política de privacidad ni en sus documentos contractuales públicos una promesa de restringir el acceso de las autoridades a los contenidos de comunicación o metadatos a situaciones en las que exista una orden judicial previa. Su política de privacidad (AMX Paraguay S.A., s. f.-a) contempla una amplia discreción por parte de la empresa, mencionando la posibilidad de compartir datos personales para cumplir con disposiciones, directrices, procedimientos legales o requerimientos del gobierno. Tal formulación no limita la solicitud a una orden judicial, sino que sostiene un alcance amplio de solicitudes gubernamentales.

Para un análisis más completo, se revisó el Informe de Transparencia en las Comunicaciones 2025 (América Móvil, 2025) de la empresa matriz de Claro Paraguay. Según el informe, América Móvil protege la privacidad de las comunicaciones y describe su política respecto al procesamiento, recepción, análisis y respuesta a las solicitudes realizadas por las autoridades. Sin embargo, "autoridades competentes" se refiere a las autoridades públicas con el poder, por ley, por una orden judicial o por un requisito previo, para solicitar datos de personas usuarias. En general, esta definición no establece restricciones de orden judicial previa para acceder a los datos.

El informe señala que América Móvil realiza un procedimiento de debida diligencia para los requerimientos de autoridades, y que la entrega de información puede ser exigible mediante un "requerimiento u orden" de autoridad competente que cumpla con los elementos esenciales. Esta fórmula es relevante porque distingue entre "requerimiento" y "orden", y no establece que toda entrega de información deba depender necesariamente de una orden judicial.

Con referencia al subcriterio I Entrega de contenido de comunicaciones, Claro no cumple con este subcriterio. La documentación pública analizada no permite concluir que la entrega de contenidos de las comunicaciones a las autoridades esté sujeta exclusivamente y en todos los casos a una orden judicial previa. Si bien algunos documentos hacen referencia a la necesidad de una orden escrita de autoridad competente para determinadas actuaciones, tanto la política de privacidad como el Informe de Transparencia en las Comunicaciones utilizan formulaciones más amplias, incluyendo referencias a

requerimientos, procedimientos legales y solicitudes de autoridades competentes. En consecuencia, la empresa no establece de manera expresa, uniforme e inequívoca que toda entrega de contenidos de comunicaciones dependa necesariamente de una orden judicial previa, requisito exigido por este criterio de evaluación.l

Respecto al subcriterio II Diferenciación de metadatos y exigencia de orden judicial, Claro tampoco cumple con este subcriterio. Si bien el Informe de Transparencia distingue entre categorías como “entrega de datos conservados”, “geolocalización en tiempo real” e “intervención de comunicaciones privadas”, no especifica con suficiente claridad qué tipos de datos comprende cada categoría ni establece expresamente que la entrega de los datos conservados se encuentre sujeta a una orden judicial previa.

Esta distinción permite inferir que la empresa diferencia entre el contenido de las comunicaciones y otras categorías de información asociadas a las comunicaciones. Sin embargo, la documentación analizada no desarrolla una política específica para los metadatos ni asume públicamente el compromiso de someter su entrega al mismo estándar de protección aplicable al contenido de las comunicaciones. Esta omisión resulta particularmente relevante considerando que los metadatos pueden revelar información sensible sobre las actividades, relaciones, ubicación y patrones de comportamiento de las personas usuarias.s

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

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

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

La política de privacidad de Tigo Paraguay no hace mención específica de la necesidad de una orden judicial para la interceptación de comunicaciones. De hecho, su aviso de privacidad (Tigo Paraguay, 2025a) estipula que la empresa puede proporcionar datos personales en muchas circunstancias, incluyendo demandas de las autoridades competentes, sin que sea necesario presentar una orden judicial como condición necesaria.

Esta formulación amplia permite la entrega de datos en respuesta a distintos tipos de requerimientos estatales, lo que no satisface el estándar exigido en este criterio.

Para complementar el análisis, se revisó el Informe anual sobre divulgación a autoridades judiciales (Millicom International Cellular S.A., 2024) de la empresa matriz de Tigo Paraguay. En dicho informe, Millicom afirma que, en Paraguay, las filiales solo entregan el contenido de las comunicaciones con una orden judicial, y que existen protocolos para confirmar la legitimidad de dichas órdenes antes de comenzar cualquier intercepción.

Además, este informe toma en cuenta y diferencia entre las distintas formas de solicitudes. Esto incluye solicitudes de interceptación de comunicaciones, acceso a servicios financieros móviles y la recopilación de diversos tipos de datos. También indica que las solicitudes de dichos datos son evaluadas en cuanto a la legalidad de la petición antes de la difusión de la información solicitada.

Sin embargo, este informe tiene muchos problemas graves que afectan la forma en que lo evaluamos. Primero, no aparece en el sitio web de Tigo Paraguay, sino en el sitio web corporativo de Millicom. Segundo, no está incluido en los contratos ni en las declaraciones de privacidad disponibles para los usuarios en Paraguay. Por lo tanto, este informe, por definición, no puede considerarse completamente integrado en el marco de transparencia.

En ese sentido, incluso si el grupo corporativo afirma que los estándares son más altos a nivel corporativo, de manera concreta, no están claramente estipulados en la documentación local de Tigo Paraguay.

Tigo no cumple con el subcriterio I Entrega de contenido de comunicaciones porque, aunque el informe LED de Millicom indica que el contenido de comunicaciones se entrega solo con una orden judicial, la política de privacidad y los acuerdos de Tigo Paraguay no consagran esta seguridad.

El criterio establece que esta información debe estar fácilmente disponible para los usuarios a través de la documentación pública del ISP. Por lo tanto, no es posible considerar este subcriterio cumplido mediante información que no está disponible públicamente.

Respecto al subcriterio II Diferenciación de metadatos y exigencia de orden judicial, Tigo tampoco cumple con este subcriterio. Si bien el informe LED de Millicom distingue entre distintas categorías de información, incluyendo contenido de comunicaciones, metadatos de clientes y otros tipos de datos, la documentación pública de Tigo Paraguay no establece de manera clara y accesible que la entrega de metadatos se encuentre siempre sujeta a una orden judicial previa.

Asimismo, aunque Millicom señala que las solicitudes son sometidas a una revisión de legalidad antes de la entrega de información, no existe un compromiso público e inequívoco que garantice que todas las categorías de metadatos únicamente serán entregadas en cumplimiento de una orden judicial. Esta falta de claridad resulta particularmente relevante considerando que los metadatos pueden revelar información sensible sobre las actividades, ubicación, relaciones y patrones de comportamiento de las personas usuarias.

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

personal

PERSONAL - NÚCLEO S.A.

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

A diferencia de otras ISP analizadas, Personal ofrece un marco regulatorio más limitado en el contexto del control gubernamental de datos privados accesibles. Ni su Política de Privacidad (Personal Paraguay, s. f.-a) ni sus Términos y condiciones (Personal Paraguay, s. f.-b, s. f.-c) revelan las instancias exactas en las que la empresa divulga información a las autoridades públicas.

En los documentos revisados, la empresa recurre a principios generales relacionados con el cumplimiento de obligaciones legales o regulatorias, sin aclarar si la transmisión de datos, y en particular los datos relacionados con comunicaciones, está sujeta a la existencia de una orden judicial.

Esta falta de precisión es importante ya que el criterio en revisión exige una garantía específica, inequívoca y comprensible para los usuarios respecto a las circunstancias bajo las cuales sus datos podrían ser entregados a las autoridades.

En materia del subcriterio I Entrega de contenido de comunicaciones Personal al igual que las demás ISP no cumple con este subcriterio. En su Política de Privacidad y contratos, no hay ninguna mención que indique que el contenido de las comunicaciones solo será divulgado a las autoridades públicas en presencia de una orden judicial preexistente.

La compañía simplemente afirma que puede divulgar información personal para cumplir con sus obligaciones legales o solicitudes de las autoridades públicas. Dicha redacción no indica ninguna jerarquía de requisitos legales y no garantiza que los datos sensibles, incluido el contenido de las comunicaciones, sean accedidos con la aprobación de una autoridad judicial independiente.

La falta de una referencia clara a una orden judicial implica que la compañía no está brindando a los usuarios una garantía de protección de sus comunicaciones frente a posibles accesos por parte del Estado.

Respecto al subcriterio II Diferenciación de metadatos y exigencia de orden judicial, Personal tampoco cumple con este subcriterio. En los documentos analizados no se identifica una diferenciación clara entre el contenido de las comunicaciones y los metadatos, ni se establecen condiciones específicas para el tratamiento o la entrega de estos últimos.

Además, no existen disposiciones que requieran que la transmisión de metadatos sea precedida por una orden judicial. La ausencia de una distinción es pertinente, ya que los metadatos que comprenden datos de registro de llamadas, ubicación e IP pueden, y a menudo contienen, datos altamente sensibles relacionados con los usuarios.

La falta de distinción en este asunto no garantiza a la empresa que esté implementando normas de protección diferenciadas de acuerdo con el tipo de dato, lo cual es incoherente con el criterio evaluado.

En lo que ha publicado, Personal no parece adoptar una posición clara de compromiso con la necesidad de obtener una orden judicial en la provisión de datos sobre el contenido de las comunicaciones o metadatos.

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

CRITERIO 3. Notificación a la persona usuaria

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

Criterio de evaluación

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

Estándar de desempeño:

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

REPORTE - NOTIFICACIÓN A LA PERSONA USUARIA

STARLINK

Notificación a la persona usuaria		
	Sí	**No**
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible		●

Starlink regula el tratamiento y la divulgación de datos personales principalmente a través de su Política de Privacidad (Starlink, 2026) y sus Términos de Servicio (Starlink, s. f.-c). Estos documentos describen sus procesos para gestionar y divulgar información personal. En ellos, la empresa se reserva el derecho de entregar información privada para satisfacer obligaciones legales, regulatorias o gubernamentales.

En los documentos examinados, no hay ninguna disposición que establezca una promesa de alertar a los usuarios cuando el gobierno requiera su información, independientemente del momento de dicha solicitud.

La política de privacidad se limita a explicar las condiciones bajo las cuales la empresa puede divulgar información, pero no incluye medidas dinámicas de transparencia para el usuario sobre las solicitudes de acceso a datos del gobierno. En particular, no contempla mecanismos de notificación posterior o diferida que permitan informar a la persona usuaria una vez que hayan cesado las restricciones legales o procesales que pudieran impedir dicha notificación. .

En los documentos analizados, también falta referencia a medidas de defensa legal, regulatoria o institucional para estos contextos que promuevan los mecanismos de notificación del usuario.

La ausencia de garantías disminuye la transparencia en cómo se procesa la información personal y frustra en gran medida la capacidad de los usuarios para comprender y, en última instancia, cuestionar el acceso del Estado a su información.

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

CLARO - AMX PARAGUAY S.A.

Notificación a la persona usuaria		
	Sí	**No**
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible		●

Claro Paraguay regula el tratamiento y la divulgación de datos personales a través de su política de privacidad (AMX Paraguay S.A., s. f.-a) y condiciones contractuales (AMX Paraguay S.A., s. f.-c, s. f.-b). En la política de privacidad y en los contratos, la empresa afirma que la información personal puede ser compartida para cumplir con las obligaciones legales y regulatorias de la empresa o para los requerimientos de las autoridades.

Sin embargo, no existe ninguna disposición en la documentación revisada que indique que la empresa se comprometerá a informar a los usuarios cuando su información personal sea solicitada por el gobierno, ya sea antes o después de que dicha información haya sido entregada.

La política de privacidad describe los casos en los que los datos pueden ser divulgados, como para cumplir con un requisito legal o una solicitud de las autoridades, pero no estipula los medios que se utilizarían para brindar a los usuarios proactividad respecto a estos asuntos. No hay disposición alguna sobre si las personas usuarias pueden ser notificados conforme a la ley, ni sobre las condiciones ad hoc en la ausencia de notificación en caso de cese de las restricciones legales.

El análisis del Informe de Transparencia en las Comunicaciones 2025 (América Móvil, 2025) tampoco evidencia la existencia de políticas de notificación a usuarios. Aunque el informe describe pasos internos para recibir, evaluar y procesar solicitudes de las autoridades, el enfoque está en verificaciones de legalidad limitadas a las solicitudes, y no existe un procedimiento para notificar a los usuarios afectados.

El informe describe sus procesos internos respecto a la recepción, evaluación y procesamiento de solicitudes de las autoridades. Sin embargo, estos procesos internos solo describen las solicitudes y no proporcionan mecanismos para que los usuarios afectados sean informados sobre las solicitudes.

De la misma manera, no hay referencias a esfuerzos legales o regulatorios para la promoción de mecanismos de notificación, ni a esfuerzos de defensa pública con este propósito.

En este contexto, la falta de cualquier compromiso de notificación es una omisión de una estructura que no permite a los usuarios saber si sus datos han sido accedidos por el estado, incluso cuando no existen barreras legales para informarlos.

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

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

Notificación a la persona usuaria		
	Sí	**No**
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible		●

La Política de Privacidad (Tigo Paraguay, 2025a), sus Términos y condiciones (Tigo Paraguay, 2025b) y documentación complementaria (Tigo Paraguay, 2025c) describen cómo la empresa recopila y divulga los datos de los usuarios. La política indica que la empresa puede compartir los datos de los usuarios para cumplir con requisitos legales, regulatorios u otros requisitos de autoridad.

No obstante, los documentos accesibles a los usuarios en Paraguay carecen de una disposición, o declaración, que describa la intención de la empresa de informar a los usuarios sobre la transmisión de datos a las autoridades gubernamentales, ya sea antes o después de dicha transmisión.

Como parte de este análisis, se revisó el Informe anual sobre divulgación a autoridades judiciales (Law Enforcement Disclosure Report – LED) de Millicom, empresa matriz de Tigo Paraguay (Millicom International Cellular S.A., 2024). Este informe muestra los procesos internos del grupo para recibir y procesar solicitudes de datos por parte de las autoridades y también los tipos de datos a solicitar, incluyendo el contenido y los metadatos de las comunicaciones.

Sin embargo, el mismo no muestra el compromiso de la empresa con la notificación a los usuarios. Dado que el documento se ocupa de la legalidad de las solicitudes y los controles internos de cumplimiento de la empresa, no tiene en cuenta la falta del derecho del usuario a saber cuándo el gobierno está accediendo a sus datos.

De manera similar, los documentos revisados no muestran referencias a acciones de defensa legal, regulatoria o institucional para promover mecanismos de notificación a los usuarios en este contexto.

Por lo tanto, la omisión estructural de cualquier referencia a los medios de notificación significa que los usuarios no sabrán si sus datos personales han sido solicitados por un Estado, o si han sido objeto de una solicitud estatal, incluso cuando no exista una prohibición legal de una notificación.

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

personal

PERSONAL - NÚCLEO S.A.

Notificación a la persona usuaria		
	Sí	**No**
¿Notifica a la persona usuaria sobre la entrega a terceros de datos personales? La empresa se compromete a notificar a las personas usuarias antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible		●

Personal regula el tratamiento y la divulgación de datos personales a través de su Política de Privacidad (Personal Paraguay, s. f.-a), sus Términos y condiciones generales (Personal Paraguay, s. f.-b) y los Términos y condiciones de aplicaciones(Personal Paraguay, s. f.-c). De acuerdo con las declaraciones de la empresa en estos documentos, el intercambio de datos personales puede tener lugar para cumplir con obligaciones legales, reglamentarias u otras ante las autoridades competentes.

Sin embargo, en los documentos revisados, no hay ninguna cláusula que establezca o describa la obligación de informar a las personas usuarias sobre los datos solicitados por las autoridades públicas, ni siquiera después del intercambio de datos.

La política de privacidad describe de forma general las condiciones de divulgación de información de la empresa, pero carece de protección de la privacidad de los consumidores. Por ejemplo, la política no contempla notificaciones diferidas o notificaciones retroactivas, y no considera el derecho del usuario a ser informado después de la solicitud estatal de información dentro del plazo legal establecido.

De manera similar, lo mismo puede decirse acerca de los Términos y Condiciones, que son generales y específicamente para la aplicación. No están complementados con disposiciones adicionales que construirían comunicación con el usuario en estos casos.

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

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

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

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

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

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

Criterios de evaluación

I. Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales;

II. Si la ISP lleva a cabo actividades, jornadas, publicidades o 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 impugnó judicialmente la legislación, o la interpretación de la legislación, que considera que viola la privacidad de los usuarios de Internet. La impugnación se basó en que la legislación es desproporcionada, no define de manera clara, precisa y detallada los casos y circunstancias en los que se deben proporcionar los datos y/o no prevé las salvaguardias adecuadas para inhibir posibles abusos.

IV. Si la empresa impugnó, ya sea judicial o administrativamente, al menos una vez durante el período analizado, solicitudes abusivas de acceso a datos de usuarios. Dichas impugnaciones se basaron en que las solicitudes excedían las prerrogativas legales de la autoridad solicitante y/o eran desproporcionadas por su falta de claridad y precisión sobre los datos requeridos y la motivación. Además, cualquier otra razón que comprometa el derecho a la privacidad de los usuarios puede ser motivo de impugnación;

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

Estándar de desempeño:

Estrella llena		La ISP cumple con 4 o 5 de los criterios
Tres cuartos de estrella		La ISP cumple con 3 de los criterios
Media estrella		La ISP cumple con 2 criterios
Un cuarto de estrella		La ISP cumple con 1 criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - POLÍTICAS DE PROMOCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS

STARLINK

Políticas de promoción y defensa de los derechos humanos		
	Sí	**No**
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		●
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.		●
Si la empresa impugnó judicialmente la legislación, o la interpretación de la legislación, que considera que viola la privacidad de los usuarios de Internet. La impugnación se basó en que la legislación es desproporcionada, no define de manera clara, precisa y detallada los casos y circunstancias en los que se deben proporcionar los datos y/o no prevé las salvaguardias adecuadas para inhibir posibles abusos.		●
Si la empresa impugnó, ya sea judicial o administrativamente, al menos una vez durante el período analizado, solicitudes abusivas de acceso a datos de usuarios. Dichas impugnaciones se basaron en que las solicitudes excedían las prerrogativas legales de la autoridad solicitante y/o eran desproporcionadas por su falta de claridad y precisión sobre los datos requeridos y la motivación. Además, cualquier otra razón que comprometa el derecho a la privacidad de los usuarios puede ser motivo de impugnación		●
Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).		●

Starlink no ofrece ninguna prueba pública y verificable de que tenga una política activa que defienda o promueva alguna forma de derechos humanos respecto a la privacidad de los individuos, protección de datos o resistencia a los abusos en las solicitudes gubernamentales de datos. En comparación con las otras ISP analizadas, no existen informes de transparencia documentados, informes de derechos humanos, informes ESG ni ningún documento institucional que demuestre que la empresa tenga compromisos específicos en la defensa de la expresión de los derechos de los individuos, o en la protección de la privacidad, o la protección de datos personales respecto a la provisión de un servicio de internet por parte de la empresa.

En el subcriterio I “Iniciativas políticas o legales para proteger la privacidad”, no se identificaron iniciativas políticas o legales emprendidas por Starlink o SpaceX para proteger la privacidad de sus usuarios en el Congreso, tribunales u otros ámbitos institucionales. La evidencia disponible se limita principalmente a los términos de servicio, privacidad del contrato, servicio y operación, y sostenibilidad legal, en lugar de la ausencia de defensa en caso de ausencia de derechos digitales.

La conclusión de la revisión de los documentos oficiales es que no hay muestra de ninguna acción pública por parte de Starlink para promover la legislación, participar en la defensa institucional para fortalecer la protección legal de la privacidad frente a la recopilación de datos de los usuarios por parte de las agencias estatales. Por lo tanto, no hay evidencia de que se cumpla este subcriterio.

En cuanto al subcriterio II “Actividades, jornadas, campañas o informes sobre privacidad o protección de datos”, Starlink tampoco cumple este subcriterio. Aunque existen documentos públicos sobre privacidad y sostenibilidad publicados por SpaceX, estos no equivalen a campañas, sesiones, informes o actividades orientadas a la promoción del derecho a la privacidad y la protección de datos.

El documento público de SpaceX sobre sostenibilidad espacial (SpaceX, s. f.) habla de la sostenibilidad del entorno espacial y de la mitigación de residuos orbitales y la protección del entorno espacial. Este documento público no abarca la protección de la privacidad de los usuarios ni la protección de datos personales. Del mismo modo, la política de privacidad de SpaceX (SpaceX, 2024) informa derechos y tratamiento de datos, pero no constituye una iniciativa de sensibilización pública sobre privacidad o protección de datos.

Por tanto, no se identifican acciones públicas que cumplan con el estándar exigido.

En referencia al subcriterio III Impugnación de legislación o interpretaciones legales lesivas de la privacidad, no se identificó evidencia pública verificable de que Starlink o SpaceX hayan impugnado alguna ley o interpretación legal argumentando que dichas leyes son desproporcionadas, incorrectas o insuficientes en materia de leyes de privacidad.

Para este subcriterio, la participación de la empresa en discusiones generales sobre regulaciones en la industria de satélites o conectividad es insuficiente. Es necesario una acción concreta legal verificable en relación con la privacidad de los usuarios de internet. Este tipo de evidencia tampoco fue encontrado en registros públicos u otros registros oficiales.

Con respecto al subcriterio IV “Impugnación de solicitudes abusivas de acceso a datos”, Starlink tampoco cumple este subcriterio. No se identificaron informes de transparencia, reportes de solicitudes gubernamentales ni documentación pública donde la empresa declare haber impugnado judicial o administrativamente solicitudes abusivas de acceso a datos de usuarios.

Esta omisión tiene una relevancia significativa dado que Starlink proporciona un servicio de internet global y no ofrece un informe independiente sobre las solicitudes del estado para acceder a datos, además de los criterios de posible rechazo, impugnación u oposición a solicitudes excesivas.

Finalmente, en el subcriterio V Participación en mecanismos sectoriales o multisectoriales de derechos humanos tampoco se encontró evidencia de que Starlink o SpaceX participen en mecanismos sectoriales o multisectoriales específicamente orientados a la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales.

La revisión de registros institucionales muestra que la Global Network Initiative pública su nómina de miembros (Global Network Initiative, s. f.), sin que Starlink o SpaceX aparezcan identificadas en esa membresía. El Pacto Global de Naciones Unidas también cuenta con una base pública de participantes empresariales (United Nations Global Compact., s. f.), pero no se identificó a Starlink o SpaceX como participantes.

Si bien SpaceX/Starlink puede participar en foros técnicos o regulatorios del sector espacial o de telecomunicaciones, no se identificó participación en mecanismos de derechos humanos equivalentes a GNI, Telecommunications Industry Dialogue, Pacto Global u otros espacios similares.

Por ello, corresponde asignar una estrella vacía, al no cumplir con ninguno de los subcriterios.

CLARO - AMX PARAGUAY S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	**No**
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		●
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	●	
Si la empresa impugnó judicialmente la legislación, o la interpretación de la legislación, que considera que viola la privacidad de los usuarios de Internet. La impugnación se basó en que la legislación es desproporcionada, no define de manera clara, precisa y detallada los casos y circunstancias en los que se deben proporcionar los datos y/o no prevé las salvaguardias adecuadas para inhibir posibles abusos.		●
Si la empresa impugnó, ya sea judicial o administrativamente, al menos una vez durante el período analizado, solicitudes abusivas de acceso a datos de usuarios. Dichas impugnaciones se basaron en que las solicitudes excedían las prerrogativas legales de la autoridad solicitante y/o eran desproporcionadas por su falta de claridad y precisión sobre los datos requeridos y la motivación. Además, cualquier otra razón que comprometa el derecho a la privacidad de los usuarios puede ser motivo de impugnación		●
Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).	●	

Claro muestra un progreso significativo en el ámbito amplio de los derechos humanos, la privacidad y la seguridad digital a través de documentos e iniciativas de su organización matriz, América Móvil. Sin embargo, en el período más reciente, no hay acciones públicas de defensa jurídica o política para proteger la privacidad de los usuarios contra normas abusivas, interpretaciones de la ley o demandas gubernamentales.

En cuanto al subcriterio I “Iniciativas políticas o legales para proteger la privacidad”, no hay iniciativas de carácter político o legal patrocinadas por Claro Paraguay en los últimos años dirigidas a abordar la protección de la privacidad de los usuarios en el Congreso, en los sistemas judiciales u otros espacios relevantes.

Claro cumple el subcriterio II “Actividades, campañas, publicidades o informes”. El Informe de Sostenibilidad 2024 de América Móvil cuenta con una sección titulada “Protección de la Privacidad y Uso Responsable de Datos de Clientes”. El Informe detalla, con subinformes y políticas corporativas declaradas, la construcción de equipos de protección de datos en las filiales, varios controles y capacitación que se hace obligatoria sobre privacidad y protección de datos personales. También se informa que al final de 2024, se había impartido capacitación en privacidad y protección de datos personales al 93% de los empleados, así como a 1,035 socios comerciales (América Móvil, 2024).

Además, el informe señala que América Móvil respalda la protección de la privacidad, la seguridad de la información y el derecho a la libertad de expresión. También menciona que la empresa no interviene en la comunicación de sus clientes de ninguna manera, como monitoreo o restricción de la comunicación, ni otros medios de manipulación.

Aunque buena parte de estas acciones se enmarcan en capacitaciones internas y reportes corporativos, constituyen evidencia pública suficiente de actividades e informes vinculados a privacidad, protección de datos y derechos digitales.

En cambio, en el subcriterio III “Impugnación de legislación o interpretaciones legales”, no hay evidencia pública de que Claro Paraguay o América Móvil hayan impugnado judicialmente legislación o interpretaciones legales en un tribunal en relación con la privacidad de los usuarios de internet y/o la desproporcionalidad.

El Informe de Transparencia 2025 (América Móvil, 2025) indica que describen procedimientos de revisión legal para demandas de autoridades, pero no menciona que hayan tomado acciones legales contra leyes o interpretaciones legales que limiten la privacidad.

El Informe de Transparencia 2025 indica que América Móvil rechaza solicitudes que contravienen la ley o que son inapropiadas, y que la compañía tiene sus propios procedimientos de verificación.

Sin embargo, el subcriterio requiere que la compañía haya impugnado, cuestionado o rechazado efectivamente al menos una solicitud abusiva durante el período analizado. La documentación disponible únicamente permite identificar la existencia de mecanismos internos de revisión, verificación y eventual rechazo de solicitudes. Además, de acuerdo con la información publicada por América Móvil para Paraguay, no se registran solicitudes rechazadas durante el período evaluado, a diferencia de lo observado en algunos otros países donde opera el grupo. Por lo tanto, no existe evidencia pública que permita concluir que la empresa haya impugnado o rechazado efectivamente una solicitud abusiva en Paraguay durante el período analizado. .

Con respecto al subcriterio V “Participación en mecanismos sectoriales o multisectoriales”, Claro si cumple con este subcriterio a través de América Móvil. El Informe de Sostenibilidad 2024 señala que América Móvil alinea su estrategia de sostenibilidad con los principios del Pacto Mundial de Naciones Unidas y los Objetivos de Desarrollo Sostenible. Asimismo, el informe indica que la compañía participa activamente en la GSMA, incluyendo grupos de trabajo sectoriales.

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

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

Políticas de promoción y defensa de los derechos humanos		
	Sí	**No**
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		●
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.	●	
Si la empresa impugnó judicialmente la legislación, o la interpretación de la legislación, que considera que viola la privacidad de los usuarios de Internet. La impugnación se basó en que la legislación es desproporcionada, no define de manera clara, precisa y detallada los casos y circunstancias en los que se deben proporcionar los datos y/o no prevé las salvaguardias adecuadas para inhibir posibles abusos.		●
Si la empresa impugnó, ya sea judicial o administrativamente, al menos una vez durante el período analizado, solicitudes abusivas de acceso a datos de usuarios. Dichas impugnaciones se basaron en que las solicitudes excedían las prerrogativas legales de la autoridad solicitante y/o eran desproporcionadas por su falta de claridad y precisión sobre los datos requeridos y la motivación. Además, cualquier otra razón que comprometa el derecho a la privacidad de los usuarios puede ser motivo de impugnación		●
Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).	●	

Tigo Paraguay presenta una estructura corporativa relativamente desarrollada en materia de derechos humanos a través de su empresa matriz, Millicom. Sin embargo, como en otros criterios analizados, se observa una brecha en los compromisos corporativos en relación con su implementación o visibilidad local, lo que en efecto reduce el cumplimiento de los criterios evaluados.

En el subcriterio I “Iniciativas políticas o legales para proteger la privacidad”, no se han documentado iniciativas recientes de Tigo Paraguay que promuevan directamente la protección de la privacidad de los usuarios ante el Congreso, el poder judicial u otros espacios institucionales.

Aunque informes anteriores documentaron la participación de la empresa en algunos procesos regulatorios, como la aprobación del reglamento de protección al usuario de telecomunicaciones y el rol de Ciberseguridad y la protección de la privacidad del usuario, no se documentan iniciativas de protección de derechos digitales ni defensa política pública durante el período evaluado.

Las propias declaraciones de Millicom respecto a su intención de apoyar procesos para fortalecer el marco regulatorio y la ciberseguridad no se correlacionan con ninguna acción local demostrada.

En cuanto al subcriterio II "Actividades, campañas, publicidades o informes", el cumplimiento de este subcriterio se sustenta principalmente en la existencia de instrumentos corporativos de Millicom, más que en evidencia local directamente atribuible a la Tigo Paraguay.

En particular, Millicom cuenta con una política de derechos humanos (Millicom International Cellular S.A., 2023b) que incorpora compromisos en materia de privacidad, protección de datos personales y libertad de expresión, alineados con estándares internacionales. Asimismo, el Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024) constituye un mecanismo de transparencia institucional que aborda la gestión de solicitudes de autoridades y la protección de comunicaciones, aportando información relevante sobre la gobernanza de datos y el enfoque de la empresa frente a derechos digitales.

A nivel local, el sitio web institucional de Tigo (Tigo Paraguay, s. f.) muestra que existen programas enfocados en la responsabilidad social corporativa, especialmente en desarrollos de inclusión y educación digital. Sin embargo, la información proporcionada es insuficiente para verificar que hayan sido implementados durante el período analizado, ya que no hay fechas de ejecución o actualización.

Por lo tanto, a pesar de la existencia de compromisos corporativos y mecanismos de transparencia a nivel del grupo empresarial, la ausencia de información clara, actualizada y verificable sobre campañas o iniciativas específicas desarrolladas por Tigo Paraguay limita el alcance de este subcriterio a nivel local.

Con respecto al subcriterio III Impugnación de legislación o interpretaciones legales no se encontró evidencia pública verificable de que Tigo Paraguay o Millicom hayan impugnado judicialmente legislación o interpretaciones legales por considerarlas contrarias al derecho a la privacidad de las personas usuarias.

Mientras que el informe LED indica la posibilidad de presentar reclamaciones ante órganos judiciales por violaciones a la ley, esta referencia no prueba la existencia de una acción concreta y/o una estrategia de litigio para proteger los derechos digitales.

Tigo tampoco cumple el subcriterio IV Impugnación de solicitudes abusivas de acceso a datos. Si bien, Millicom informa que cuenta con procedimientos internos para evaluar la legalidad de las solicitudes de acceso a datos y que puede rechazar aquellas que no cumplan con los requisitos legales.

La norma establece que se debe presentar prueba de que la empresa ha impugnado judicial o administrativamente, solicitudes abusivas durante el período examinado. El documento no prueba la existencia de una impugnación en particular, sino que muestra la existencia de mecanismos internos de revisión y rechazo.

Por último, Tigo si cumple el subcriterio V Participación en mecanismos sectoriales o multisectoriales. Millicom participa en espacios sectoriales relevantes como la GSMA (GSMA, s. f.), lo que significa que forma parte de un ecosistema internacional de relaciones en el que se discuten las directrices del sector, prácticas y teorías de sostenibilidad y gobernanza digital.

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

personal

PERSONAL - NÚCLEO S.A.

Políticas de promoción y defensa de los derechos humanos		
	Sí	**No**
Si la ISP promueve iniciativas políticas o legales para proteger la privacidad de sus usuarios, usuarias en el Congreso, por ejemplo, a través de proyectos legislativos o participación en audiencias, o en los Tribunales.		●
Si la ISP lleva a cabo actividades, jornadas, publicidades o pública informes con el fin de generar conciencia en la sociedad sobre el derecho a la privacidad y/o la protección de los datos personales.		●
Si la empresa impugnó judicialmente la legislación, o la interpretación de la legislación, que considera que viola la privacidad de los usuarios de Internet. La impugnación se basó en que la legislación es desproporcionada, no define de manera clara, precisa y detallada los casos y circunstancias en los que se deben proporcionar los datos y/o no prevé las salvaguardias adecuadas para inhibir posibles abusos.		●
Si la empresa impugnó, ya sea judicial o administrativamente, al menos una vez durante el período analizado, solicitudes abusivas de acceso a datos de usuarios. Dichas impugnaciones se basaron en que las solicitudes excedían las prerrogativas legales de la autoridad solicitante y/o eran desproporcionadas por su falta de claridad y precisión sobre los datos requeridos y la motivación. Además, cualquier otra razón que comprometa el derecho a la privacidad de los usuarios puede ser motivo de impugnación		●
Participa en algún mecanismo sectorial o multisectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales. (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).	●	

Personal Paraguay muestra un estado de política pública poco desarrollado en relación con la defensa de los derechos humanos en cuanto a la privacidad y protección de datos personales. En comparación con otros proveedores de servicios de Internet, no se identificaron documentos institucionales, reportes corporativos ni evidencia pública que den cuenta de una estrategia estructurada en esta materia a nivel local.

Para el subcriterio I Iniciativas políticas o legales para proteger la privacidad, o hay evidencia de que Personal Paraguay haya emprendido iniciativas para promover la privacidad de los usuarios ante el Congreso, la Justicia u otra institución. Además, no se ha detectado participación reciente de Personal Paraguay en el proceso legislativo ni en los procesos regulatorios para desarrollar e implementar marcos normativos relacionados con los derechos digitales o la protección de datos personales.

En cuanto al subcriterio II Actividades, campañas, publicidades o informes, no hay evidencia pública durante el período analizado de que Personal Paraguay haya establecido iniciativas, eventos, programas o informes para promover la conciencia sobre la protección de datos personales o la protección de la privacidad.

En el subcriterio III Impugnación de legislación o interpretaciones legales, no se encontró evidencia que demuestre que Personal Paraguay cuestionara legislación o interpretaciones legales que se consideraran desproporcionadas o contrarias al derecho a la privacidad de los usuarios.

Respecto al subcriterio IV Impugnación de solicitudes abusivas de acceso a datos, tampoco se encontraron registros públicos, informes o descripciones de instituciones estatales que confirmen que Personal Paraguay defendió a los usuarios en el período analizado, contra una solicitud abusiva de acceso a datos, ya sea de manera administrativa o judicial.

Personal si cumple este subcriterio V Participación en mecanismos sectoriales o multisectoriales a través de su grupo empresarial, participa en la GSMA, organización global del sector móvil que promueve estándares, buenas prácticas y espacios de diálogo sobre sostenibilidad, gobernanza digital y desarrollo del ecosistema de telecomunicaciones (GSMA, s. f.).

Por ello, corresponde asignar una calificación de un cuarto de estrella, al cumplir uno de los criterios.

CRITERIO 5. Transparencia

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

El informe de transparencia notifica el origen de las solicitudes para el bloqueo o retiro de contenidos de Internet —incluyendo pornografía infantil, infracción al derecho de autor, cumplimiento de sus propias políticas, etc. Si bien las ISP en Paraguay no están bajo ninguna obligación de producir informes de transparencia activa, esto podría ser una ventana de oportunidad para mostrar que están preocupadas por la construcción de confianza en sus relaciones con los clientes, basadas en la transparencia.

Criterios de evaluación

I. La ISP publica informes de transparencia para que la persona usuaria pueda enterarse de la colaboración con las autoridades gubernamentales sobre los datos proveídos;

II. La ISP publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando:

   a. la cantidad de solicitudes y divulgaciones clasificadas por tipo de datos –si se trata de información de cuenta o de conexión de registros;

   b. la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud;

   c. la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental –presentación de pruebas en materia civil, penal, o los casos administrativos, etc.

Estándar de desempeño:

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

REPORTE - TRANSPARENCIA

STARLINK

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.		●

Starlink no publica informes de transparencia que detallen el número de solicitudes de datos realizadas a ellos por agencias gubernamentales, ni con qué frecuencia la empresa proporciona este tipo de información.

Los documentos que están disponibles, incluyendo la política de privacidad y los términos de servicio, dicen que la empresa puede proporcionar los datos de los usuarios si así lo requiere el cumplimiento de la ley, o mediante una solicitud hecha por las autoridades correspondientes. Sin embargo, estos términos no son informes de transparencia, ya que no contienen información cuantitativa o sistemática sobre las solicitudes de acceso a datos.

Asimismo, no se identifican reportes institucionales, documentos corporativos ni secciones específicas en el sitio web de Starlink o de su empresa matriz, SpaceX, que detallen estadísticas sobre solicitudes gubernamentales de datos, su origen o su motivación.

La falta de informes de transparencia demuestra la falta de acceso público a datos para medir o describir la extensión, volumen, o incluso la forma en que Starlink proporciona datos a varias instituciones gubernamentales. Esto obstaculiza severamente la capacidad de los usuarios finales y la sociedad civil para evaluar si los datos proporcionados están en equilibrio y en conformidad con las normas y prácticas internacionales.

Por lo tanto, la ausencia de un informe de transparencia implica que no se cumplen los requisitos del subcriterio, en lo que respecta a describir la información solicitada por tipo, la autoridad que solicitó la información y el razonamiento detrás de la solicitud.

Conforme al estándar de desempeño, corresponde asignar una estrella vacía a Starlink por no cumplir con ninguno de los criterios.

CLARO - AMX PARAGUAY S.A.

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

Claro Paraguay, a través de su empresa matriz América Móvil, publica informes de transparencia regulares. Estos contienen datos sobre solicitudes de información de las autoridades estatales y cómo la empresa ha respondido a dichas solicitudes.

El Informe de Transparencia en las Comunicaciones 2025 (América Móvil, 2025) es una fuente disponible al público, que permite a los usuarios evaluar el nivel de cooperación de la empresa con las autoridades judiciales, cumpliendo así con el primer subcriterio.

En cuanto al subcriterio I Publicación de informes de transparencia, América Móvil Publica informes de transparencia que muestran el número total de solicitudes de información recibidas de autoridades gubernamentales y el porcentaje de solicitudes que fueron atendidas y/o denegadas.

También presenta estadísticas por país, lo que ayuda a encontrar información sobre Paraguay, incluido el número de solicitudes y su clasificación según los tipos de autoridades. Además, incluye descripciones de la revisión interna de las solicitudes, incluyendo criterios de legalidad y proporcionalidad.

Respecto al subcriterio II Contenido y desagregación del informe, el Informe de Transparencia 2025 presenta información desagregada que cumple con los estándares exigidos por este subcriterio.

En particular, el informe incluye: clasificación de solicitudes según el tipo de datos requeridos (por ejemplo, datos conservados, geolocalización o intervención de comunicaciones); identificación de las autoridades que realizan las solicitudes (incluyendo autoridades judiciales y fiscales); descripción del marco legal aplicable y de los tipos de requerimientos procesados.

Dentro del alcance del contexto analizado, Claro se ha establecido como el ISP con mayor compromiso con la transparencia al difundir, a través de su matriz America Movil, informes detallados sobre las solicitudes de datos del gobierno, que se publican periódicamente y de manera comprensible para describir su tamaño y características.

Todavía hay algunas áreas de mejora, como ofrecer más detalles para desglosar las motivaciones y categorías de las solicitudes, pero la calidad de los datos supera las mejores prácticas internacionales de la industria y la de los ISP cubiertos en este informe.

Por ello, corresponde asignar una calificación de estrella llena,
por cumplir con todos los criterios establecidos.

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

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

Tigo Paraguay, a través de su empresa matriz, Millicom, publica el Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024), el cual constituye un mecanismo de transparencia institucional sobre la colaboración de la empresa con autoridades gubernamentales en materia de acceso a datos.

Este documento permite la evaluación del cumplimiento del primer subcriterio, pero presenta importantes deficiencias en lo que respecta a los niveles de desglose de datos, lo que limita el cumplimiento del segundo subcriterio.

En cuanto al subcriterio I Publicación de informes de transparencia, Millicom publica de forma periódica el Law Enforcement Disclosure Report (LED), que proporciona datos sobre el número de solicitudes de información realizadas por agencias estatales.

Este informe abarca los países en los que opera la empresa, incluido Paraguay, y proporciona información sobre el número total de solicitudes recibidas, así como las categorías generales de las solicitudes.

Este informe permite a los usuarios entender los parámetros de las solicitudes de datos procesadas y el marco de las interacciones de la empresa con el estado, cumpliendo con el estándar exigido por este subcriterio.

Aunque el informe LED muestra cierta categorización de las solicitudes, por ejemplo, separando interceptación de comunicaciones y metadatos, así como servicios financieros móviles, el estándar de desagregación sigue siendo insuficiente.

Específicamente, el informe señala las siguientes deficiencias: los números de solicitudes presentados no están desglosados por país, sino que por región (América del Sur); la diferenciación por tipo de datos no es ni detallada ni consistente en la mayoría de los casos; la categorización de las autoridades solicitantes no se realiza de manera sistemática en la mayoría de los casos; y las motivaciones de las solicitudes, por ejemplo, la distinción entre procedimientos civiles, penales o incluso administrativos, siguen siendo poco claras.

Estas limitaciones dificultan una comprensión completa del contexto y las circunstancias que rodean las solicitudes de acceso a los datos.

Por lo tanto, aunque el informe representa un avance notable hacia la transparencia, aún no cumple con el estándar de desagregación de este criterio.

Por ello, corresponde asignar una calificación de media estrella al cumplir con uno de los criterios.

personal

PERSONAL - NÚCLEO S.A.

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

Personal Paraguay no publica informes de transparencia para que los usuarios puedan evaluar cuántas solicitudes de datos de usuario han realizado las agencias gubernamentales ni a qué ritmo la empresa proporciona datos a estas autoridades.

En comparación con otros ISP analizados que han publicado informes a nivel local (o a nivel de sus empresas matriz), no hay informes que contengan datos cuantitativos sobre solicitudes de acceso a datos gubernamentales en el sitio web de la Compañía ni en la documentación corporativa a la que tiene acceso el público.

Personal no cumple con el subcriterio I Publicación de informes de transparencia por falta de divulgación de informes de transparencia e institucionales. Asimismo, no se localizaron segmentos especiales de este sitio web que proporcionen información sobre las secciones del sitio web para atender solicitudes de datos gubernamentales.

Dado que el personal no publica informes de transparencia, tampoco cumple con el subcriterio II Contenido y desagregación del informe ya que la información pública no permite determinar: el número de solicitudes de datos recibidas; la clasificación de solicitudes por tipo de datos (contenido o metadatos); las autoridades que realizan las solicitudes o los propósitos de dichas solicitudes.

Conforme al estándar de desempeño, corresponde asignar una estrella vacía, al no cumplir con ningún criterio.

CRITERIO 6. Guías para la solicitud de información personal

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

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

Criterios de evaluación

I. Si la ISP tiene lineamientos, guías o protocolos que determinen cómo recibirán las solicitudes de información de sus clientes;

II. Si los lineamientos, guías o protocolos se encuentran disponibles públicamente;

III. Si dichos lineamientos, guías o protocolos explican detalladamente los pasos a seguir ante el requerimiento y el procedimiento para brindar los datos a la autoridad requirente.

Estándar de desempeño:

Estrella llena		La ISP cumple con todos los criterios
Media estrella		La ISP cumple con 2 de los criterios
Un cuarto de estrella		La ISP cumple con 1 criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - GUÍAS PARA LA SOLICITUD DE INFORMACIÓN PERSONAL

STARLINK

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

Starlink no divulga directivas, instrucciones ni protocolos para las agencias gubernamentales sobre cómo deben manejar las solicitudes de datos específicos de los usuarios o procesos internos.

Los documentos disponibles, a saber, su política de privacidad (Starlink, 2026) y términos de servicio (Starlink, s. f.-c), indican que la compañía puede revelar datos personales para cumplir una obligación legal o para responder a solicitudes de las autoridades gubernamentales correspondientes. Sin embargo, estas cláusulas no son protocolos ni instrucciones para las agencias gubernamentales, ni estipulan cómo deben solicitar la información.

En particular, no se encuentran documentos que sean equivalentes a directrices de acceso a datos que estipulen los requisitos de solicitud formal, estándares de validación, canales de recepción o procedimientos de evaluación interna.

Starlink no cumple con el subcriterio I Existencia de lineamientos o protocolos ya que no se encontró evidencia pública de la existencia de lineamientos o protocolos específicos que regulen la forma en que la empresa recibe solicitudes de información por parte de autoridades.

Dado que no se identificaron lineamientos o protocolos, tampoco se cumple el subcriterio II Disponibilidad pública porque no existen documentos públicos que puedan ser consultados por autoridades o por la ciudadanía para conocer los procedimientos de solicitud de información.

Finalmente, Starlink tampoco cumple con el subcriterio III Nivel de detalle de los procedimientos dado que la empresa no proporciona información detallada sobre los pasos que deben seguir las autoridades para solicitar datos, ni sobre los procedimientos internos para la entrega de dicha información.

Por ello, corresponde asignar una calificación de estrella vacía, debido a que no cumple con ningún criterio.

CLARO - AMX PARAGUAY S.A.

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

Claro Paraguay, a través de su empresa matriz América Móvil, tiene políticas y procedimientos públicos que rigen cómo se reciben y procesan las solicitudes de acceso a datos de las entidades gubernamentales.

La mayoría de estas políticas se contienen en el Informe de Transparencia en Comunicaciones 2025 (América Móvil, 2025), que también describe los procedimientos internos paso a paso de la empresa para gestionar las solicitudes legales.

Por ende, Claro cumple con el subcriterio I Existencia de lineamientos o protocolos. El Informe de Transparencia señala que América Móvil implementa un mecanismo formal para recibir, procesar y responder a las solicitudes de las autoridades, que incluye la evaluación de la fundamentación legal de la solicitud, la competencia de la autoridad solicitante y la evaluación de la proporcionalidad de la solicitud.

Además, se señala que, para ser consideradas válidas, las solicitudes deben cumplir con requisitos particulares, lo que ejemplifica la existencia de un marco interno para gestionar este tipo de demandas.

Claro cumple con el subcriterio II Disponibilidad pública a través de su matriz America Movil. El Informe de Transparencia es un documento público y de fácil acceso publicado en línea que proporciona a las autoridades, usuarios y organizaciones de la sociedad civil conocimiento de los protocolos generales que la empresa tiene al interactuar con el Estado respecto al acceso a datos.

Esta disponibilidad ayuda a lograr transparencia y previsibilidad en los procesos estableciendo los requisitos públicos que deben cumplir las solicitudes.

En cuanto al subcriterio III Nivel de detalle de los procedimientos, Claro también cumple con este subcriterio. El Informe de Transparencia explica la secuencia de actividades de las solicitudes de acceso a datos, que son: recepción y registro formal de la solicitud; confirmación de la autoridad solicitante y su capacidad legal; determinación del cumplimiento de requisitos formales y sustantivos; determinación de la aprobación o rechazo de la solicitud; y envío de la información cuando la solicitud es aprobada.

Los documentos analizados permiten identificar de manera relativamente clara las etapas del proceso de recepción, evaluación y respuesta a solicitudes de autoridades, lo que permite considerar cumplido el subcriterio, aunque se recomienda mayor nivel de detalle operativo.

En base al estándar de desempeño, corresponde asignar una calificación de estrella llena a Claro por cumplir todos los criterios.

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

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

Tigo Paraguay, a través de su empresa matriz, Millicom, cuenta con lineamientos generales para la gestión de solicitudes de acceso a datos por parte de autoridades, los cuales se reflejan principalmente en el Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024).

No obstante, estos lineamientos presentan limitaciones en cuanto a su nivel de detalle y especificidad, lo que impacta el cumplimiento del tercer subcriterio.

Tigo cumple con el subcriterio I Existencia de lineamientos o protocolos. El Informe LED describe los procedimientos internos para la recepción y evaluación de solicitudes de las autoridades, incluyendo la revisión de legalidad, la evaluación de las solicitudes conforme a los requisitos legales y el rechazo de aquellas solicitudes que no cumplen con los requisitos legales.

Además, la empresa menciona mecanismos para cuestionar solicitudes que presentan inconsistencias legales, lo que también refleja la existencia de un sistema interno para la gestión de solicitudes.

También Tigo cumple con el subcriterio II Disponibilidad pública. El informe LED es un documento público accesible a través del sitio web corporativo de Millicom, lo que permite conocer de manera general cómo la empresa gestiona las solicitudes de acceso a datos.

Sin embargo, cabe señalar que este documento no se encuentra publicado directamente en el sitio web local de Tigo Paraguay, lo que puede limitar su accesibilidad para las personas usuarias del país. Además, no se encuentra disponible una versión en español, solo en inglés.

En cuanto al subcriterio III Nivel de detalle de los procedimientos, Tigo no cumple con el mismo. Aunque el informe LED incluye descripciones generales de los procedimientos internos de la empresa, no explica adecuadamente los pasos necesarios que deben seguir las autoridades para solicitar datos, ni el procedimiento completo para la entrega de la información.

Más específicamente, el documento: describe principios generales, pero no define un protocolo específico; no prescribe los requisitos formales que debe cumplir una solicitud; no detalla de manera precisa los canales de recepción y las directrices para respuestas oportunas; y adopta una narrativa en lugar de un enfoque procesal.

Si bien existen lineamientos generales, estos no permiten identificar con suficiente claridad el procedimiento operativo ni los pasos concretos a seguir ante solicitudes de autoridades, por lo que no se considera cumplido el subcriterio

Por ello, corresponde asignar una calificación de media estrella.

personal

PERSONAL - NÚCLEO S.A.

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

Personal Paraguay no pone a disposición las pautas o instrucciones para las autoridades sobre cómo solicitar datos personales de los usuarios, ni los términos y procesos relacionados con la entrega de dichos datos.

A diferencia de todos los demás proveedores de servicios de internet que estudiamos, que tienen dichos documentos, ya sea localmente o de la empresa matriz, no hemos encontrado nada similar que sea una guía para las autoridades o protocolos de acceso a datos en el sitio institucional o en los documentos disponibles al público.

Por ello, corresponde asignar una calificación de estrella vacía.

CRITERIO 7. Accesibilidad

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

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

Criterios de evaluación

I. La ISP tiene una interfaz de sitio Web que cuenta con información perceptible y con alternativas equivalentes para mostrar contenido, propósito o función;

II. La ISP tiene un sitio Web con una interfaz navegable, funcional y que cuenta con soporte para teclado;

III. La ISP tiene un sitio Web con información comprensible, que aparece y opera de forma predecible;

IV. El contenido en el sitio Web de la ISP es compatible con las herramientas actuales de la persona usuaria (diferentes navegadores, tecnologías de apoyo y otros agentes de la persona usuaria).

Estándar de desempeño:

Estrella llena		La ISP cumple con todos los criterios
Media estrella		La ISP cumple con 2 de los criterios
Un cuarto de estrella		La ISP cumple con 1 criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - ACCESIBILIDAD

STARLINK

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

El diseño, la estructura y la funcionalidad del sitio web de Starlink muestran un nivel alto de accesibilidad. Los usuarios pueden navegar y localizar contenido útil como documentos legales, gracias al diseño claro y lógico y a la estructura sencilla de la información.

La evaluación técnica mediante la herramienta WAVE Web Accessibility Evaluation Tool no detectó errores críticos de accesibilidad, registrando una puntuación de 9.9 sobre 10 (Web Accessibility Tool., s. f.-c). Si bien se identificaron algunas alertas menores, éstas no comprometen la funcionalidad general ni la experiencia de usuario.

Respecto al subcriterio I Información perceptible el sitio tiene buen contraste, proporciona tipografía legible y presenta la información con una estructura comprensible, facilitando la percepción de la información.

En cuanto al subcriterio II Navegación funcional, el sitio también es de sencilla utilización, sin barreras de acceso y con una estructura de menú lógica y ordenada.

En materia del subcriterio III Comprensibilidad, la información se presenta en una estructura fácil de leer y de manera predecible, utilizando un lenguaje fácilmente comprensible.

El subcriterio IV Compatibilidad sugiere que el sitio soporta navegadores convencionales, y no se observaron anomalías estructurales negativas significativas. La prueba de uso realizada por la herramienta de accesibilidad WAVE no encontró errores que afecten negativamente la localización de la información y la interacción con el sitio mediante tecnologías de asistencia

Conforme al estándar de desempeño, corresponde asignar una calificación de estrella llena.

CLARO - AMX PARAGUAY S.A.

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

Existen deficiencias notables en el sitio web de Claro que afectan tanto la facilidad de navegación como la capacidad del sitio para funcionar de manera compatible con tecnologías de asistencia. Aunque la información puede mostrarse al usuario en un sentido básico, la experiencia es problemática debido a una serie de problemas estructurales que inhiben un acceso completo al contenido.

La evaluación técnica mediante la herramienta WAVE Web Accessibility Evaluation Tool identificó múltiples fallas de accesibilidad, incluyendo errores estructurales, problemas de contraste y alertas relacionadas con la organización del contenido, obteniendo una puntuación de 5.8 sobre 10 (Web Accessibility Tool., s. f.-a). Estos resultados evidencian un nivel de accesibilidad medio-bajo en comparación con estándares actuales.

En cuanto al subcriterio I Información perceptible, el sitio cumple parcialmente con este subcriterio. El contenido es perceptible y el texto es legible, pero se han identificado algunos problemas de contraste que afectan la lectura y visibilidad de los usuarios con baja visión.

En relación con el subcriterio II Navegación funcional, Claro no cumple con este subcriterio. El sitio presenta problemas funcionales en la navegación debido a la dificultad de estructuras complejas, problemas en la organización de encabezados y problemas en el uso de la navegación por teclado.

Claro no cumple con el subcriterio III Comprensibilidad. Esto se debe a que la estructura del sitio no siempre es predecible, y la organización del contenido puede generar problemas de orden y navegación que afectan especialmente a los usuarios que dependen de tecnologías asistidas.

Finalmente, en cuanto al subcriterio IV Compatibilidad, los errores identificados afectan la compatibilidad del sitio con las herramientas, incluyendo los errores de contrastes y la falta de etiquetas adecuadas y problemas estructurales.

Dicho esto, en este caso se debe asignar un cuarto de estrella.

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

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

El sitio web de Tigo presenta un alto nivel de accesibilidad, con una interfaz clara, estructurada y funcional que permite una navegación fluida y un acceso efectivo a los contenidos relevantes.

La evaluación técnica mediante la herramienta WAVE Web Accessibility Evaluation Tool identificó un número mínimo de incidencias, incluyendo un error aislado y algunas alertas menores, alcanzando una puntuación de 9.1 sobre 10 (Web Accessibility Tool., s. f.-d). Estos resultados reflejan un desempeño sólido en términos de accesibilidad.

Con base al subcriterio I. Información perceptible, el sitio tiene una muy buena legibilidad. Todos los elementos tienen un contraste adecuado y el contenido presenta una organización visualmente clara, permitiendo una percepción adecuada de la información.

Para el subcriterio II Navegación funcional, la navegación principal y los elementos incluidos permiten un acceso fluido para facilitar la navegación sin obstaculizar significativamente la exploración.

En materia del subcriterio III Comprensibilidad, el contenido tiene una formación y legibilidad claras con predictibilidad. La predictibilidad de la formación del sitio permite llenar fácilmente los vacíos de información.

Y en base al subcriterio IV Compatibilidad, se ha observado que el sitio es compatible con los navegadores estándar y está adaptado a diversos tamaños de dispositivos de pantalla. Los errores detectados no afectan de manera significativa el uso con herramientas de asistencia.

Por lo tanto, se otorga una calificación de estrella completa.

personal

PERSONAL - NÚCLEO S.A.

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

El sitio web de Personal presenta deficiencias significativas en materia de accesibilidad, que afectan tanto la percepción de la información como la navegación y la compatibilidad con herramientas de apoyo.

La evaluación técnica mediante la herramienta WAVE Web Accessibility Evaluation Tool identificó un elevado número de errores, incluyendo fallas estructurales, problemas de contraste y múltiples alertas, obteniendo una puntuación de 3.9 sobre 10 (Web Accessibility Tool., s. f.-b). Estos resultados evidencian un nivel bajo de accesibilidad en comparación con estándares actuales.

Respecto al I Información perceptible, este subcriterio no se cumple debido a la gran cantidad de errores de contraste y presentación, que afectan, sobre todo, la legibilidad para las personas con baja visión.

Personal no cumple con el subcriterio II Navegación funcional, debido a la existencia de múltiples errores estructurales, así como a la ausencia de organización del contenido, lo que hace que la navegación, y particularmente la navegación con teclado y tecnología asistida, sea muy difícil.

Para el subcriterio III Comprensibilidad, tampoco se cumple este subcriterio. El diseño estructural del sitio no es completamente predecible y presenta inconsistencias que pueden dificultar la comprensión de la información.

Por último, en lo que respecta al subcriterio IV Compatibilidad, los errores detectados tendrán un impacto negativo en el nivel de compatibilidad del sitio con tecnologías asistidas y lectores de pantalla, así como con diversos agentes de usuario.

De esta manera, se asigna una calificación de estrella vacía.

CRITERIO 8. Protocolo de entrega de datos para investigaciones penales

¿Se compromete la empresa a seguir la interpretación más protectora del derecho a la privacidad ante solicitudes de datos personales por parte de agentes del Estado, y cuenta con políticas específicas para estos casos?

La provisión de datos personales en el contexto de investigaciones penales constituye uno de los puntos de mayor tensión entre la persecución penal y la protección del derecho a la intimidad. Este criterio evalúa si las empresas proveedoras de servicios de Internet (ISP) adoptan una interpretación restrictiva y garantista del marco normativo vigente al momento de responder a solicitudes de acceso a datos por parte de autoridades públicas.

En esta edición, el criterio adquiere especial relevancia a partir de la entrada en vigor de la **Ley Nº 7593/2025 de Protección de Datos Personales**, la cual establece principios rectores obligatorios para todo tratamiento y comunicación de datos personales, incluyendo su transferencia a autoridades públicas. Entre estos principios se destacan la legalidad, finalidad, proporcionalidad, minimización y responsabilidad demostrada.

Este análisis debe entenderse a la luz del marco jurídico nacional, que establece estándares exigentes: la Constitución Nacional (Presidencia de la Republica del Paraguay, 1992), los artículos 33 y 36 protegen la intimidad y la inviolabilidad de las comunicaciones, el Código Procesal Penal (Presidencia de la Republica del Paraguay, 1998b) en sus artículos 200 y 228 exige que control judicial para su intervención, y la Ley N.° 7593/2025 de Protección de Datos Personales en Paraguay (Presidencia de la Republica del Paraguay, 2025b) impone principios de legalidad, proporcionalidad y minimización en el tratamiento de datos.

Criterios de evaluación

I. I. Datos de registro (información de suscriptores)

Se evalúa si la empresa:

a. establece que los datos de registro solo serán entregados a autoridades competentes debidamente identificadas, limitando su acceso a supuestos legalmente habilitados;

b. y/o exige orden judicial cuando la solicitud excede los supuestos expresamente previstos por la legislación para requerimientos administrativos o regulatorios o cuando presenta riesgos para el derecho a la privacidad.

II. Datos de geolocalización

Se evalúa si la empresa:

a. distingue claramente los datos de geolocalización de otros tipos de datos personales;

b. y establece que su entrega —especialmente en tiempo real— requiere orden judicial, conforme a los estándares constitucionales de protección de las comunicaciones.

III. Registros de conexión (metadatos)

Se evalúa si la empresa se compromete a:

a. entregar registros de conexión únicamente bajo orden judicial;

b. o, en su defecto, establecer límites claros y restrictivos para su entrega, en línea con la protección constitucional de los metadatos como parte de la comunicación.

IV. Prohibición de órdenes genéricas

Se evalúa si la empresa:

a. se compromete a rechazar o impugnar solicitudes de acceso a datos que no identifiquen de manera específica a la persona afectada;

b. o que resulten desproporcionadas, amplias o carentes de fundamentación suficiente.

V. Protocolos específicos y transparencia

Se evalúa si la empresa:

a. cuenta con protocolos o lineamientos públicos que regulen la entrega de datos a autoridades en el marco de investigaciones penales;

b. y si estos protocolos contienen información clara, estructurada y comprensible sobre los criterios y procedimientos aplicables.

Estándar de desempeño:

Estrella llena		La ISP cumple con 5 criterios
Tres cuartos de estrella		La ISP cumple con 4 criterios
Media estrella		La ISP cumple con 3 criterios
Un cuarto de estrella		La ISP cumple con 1 criterio
Estrella vacía		La ISP no cumple ninguno de los criterios

REPORTE - PROTOCOLO DE ENTREGA DE DATOS PARA INVESTIGACIONES PENALES

STARLINK

Protocolo de entrega de datos para investigaciones penales		
	Sí	**No**
Datos de registro (información de suscriptores) Se evalúa si la empresa: (a) establece que los datos de registro solo serán entregados a autoridades competentes debidamente identificadas, limitando su acceso a supuestos legalmente habilitados; (b) y/o exige orden judicial cuando la solicitud excede los supuestos administrativos o presenta riesgos para el derecho a la privacidad.		●
Datos de geolocalización Se evalúa si la empresa: (a) distingue claramente los datos de geolocalización de otros tipos de datos personales;b) y establece que su entrega —especialmente en tiempo real— requiere orden judicial, conforme a los estándares constitucionales de protección de las comunicaciones.		●
Registros de conexión (metadatos) Se evalúa si la empresa se compromete a: (a) entregar registros de conexión únicamente bajo orden judicial; (b) o, en su defecto, establecer límites claros y restrictivos para su entrega, en línea con la protección constitucional de los metadatos como parte de la comunicación.		●
Prohibición de órdenes genéricas Se evalúa si la empresa: (a) se compromete a rechazar o impugnar solicitudes de acceso a datos que no identifiquen de manera específica a la persona afectada; (b) o que resulten desproporcionadas, amplias o carentes de fundamentación suficiente.		●
Protocolos específicos y transparencia Se evalúa si la empresa: (a) cuenta con protocolos o lineamientos públicos que regulen la entrega de datos a autoridades en el marco de investigaciones penales; (b) y si estos protocolos contienen información clara, estructurada y comprensible sobre los criterios y procedimientos aplicables.		●

Starlink no dispone de información pública que especifique los procedimientos para compartir datos personales relacionados con investigaciones penales. Los documentos disponibles, política de privacidad (Starlink, 2026) y términos de servicios (Starlink, s. f.-c), indican que la compañía puede compartir datos personales para cumplir con cuestiones legales u obligaciones de las autoridades competentes. Este lenguaje legal es vago y carece de detalles sobre qué datos podrían ser comprometidos, las razones

y justificaciones detrás de ello, quién los recibiría o cuáles serían las autorizaciones legales. Por lo tanto, la compañía no ofrece una representación pública de que su postura sea protectora o restrictiva del derecho a la privacidad.

En relación con el subcriterio I sobre datos de registro, Starlink no indica bajo qué circunstancias otorga datos básicos de suscriptores o información de la cuenta. No especifica a qué autoridades pueden ser entregados, o si son diferentes de las autoridades administrativas, fiscales o judiciales, o en qué circunstancias se requiere autorización judicial de una orden judicial. Esta insuficiencia dificulta la evaluación de si la compañía restringe la provisión de datos de registro a casos legalmente justificados o si impone alguna restricción adicional en caso de solicitudes estatales.

El subcriterio II, que se refiere a los datos de geolocalización, no menciona información sobre el procesamiento o la entrega de datos de geolocalización. La empresa no categoriza los datos de geolocalización como históricos o en tiempo real, ni determina si estos datos requieren la emisión de una orden previa. El silencio de la empresa en este aspecto es particularmente preocupante porque los datos de geolocalización revelan el movimiento del sujeto, su lugar de residencia, relaciones interpersonales y actividades o rutinas diarias. Esto sugiere que se requieren medidas de protección más estrictas.

En cuanto al subcriterio III, que se refiere a los registros de conexión, Starlink también no aplica principios diferenciados para el suministro de metadatos, registros técnicos o información sobre el uso del servicio. Los documentos arriba mencionados, no especifican si esta recopilación de datos está limitada a una orden judicial, o si estos datos se tratan con el mismo nivel de protección que el contenido de las comunicaciones. La ausencia de diferenciación es preocupante debido a que los registros de conexión pueden exponer a los usuarios a información sensible de su actividad digital, incluso si los registros no contienen contenido de comunicaciones.

En relación con el subcriterio IV de la prohibición de órdenes genéricas, no se ha realizado ninguna declaración pública sobre la aceptación, rechazo o limitación de solicitudes excesivamente amplias, genéricas o desproporcionadas. La empresa no divulga si obliga a las solicitudes a precisar la persona cuyos datos se solicitan, el tipo de datos, la duración o el objetivo de la medida. Sin esto, no se puede afirmar que Starlink implemente protecciones contra solicitudes estatales excesivas y posiblemente abusivas.

En relación con el subcriterio V sobre protocolos específicos y transparencia, Starlink no crea, comparte ni publica guías, protocolos o directrices para proporcionar información a las autoridades públicas o usuarios sobre el proceso mediante el cual responden a solicitudes de datos en temas de investigación criminal. La ausencia de directrices/documentación estructural no explica cómo se recibe, revisa, confirma y/o proporciona la información. Esto sitúa a la organización en un nivel bajo de transparencia en una dimensión que es particularmente sensible a la privacidad.

En consecuencia, Starlink no cumple con ninguno de los subcriterios evaluados. Su documentación pública no permite identificar reglas claras, diferenciadas y garantistas para la entrega de datos personales a autoridades en investigaciones penales, por lo que corresponde asignarle estrella vacía.

CLARO - AMX PARAGUAY S.A.

Protocolo de entrega de datos para investigaciones penales		
	Sí	**No**
Datos de registro (información de suscriptores) Se evalúa si la empresa: (a) establece que los datos de registro solo serán entregados a autoridades competentes debidamente identificadas, limitando su acceso a supuestos legalmente habilitados; (b) y/o exige orden judicial cuando la solicitud excede los supuestos administrativos o presenta riesgos para el derecho a la privacidad.		●
Datos de geolocalización Se evalúa si la empresa: (a) distingue claramente los datos de geolocalización de otros tipos de datos personales;b) y establece que su entrega —especialmente en tiempo real— requiere orden judicial, conforme a los estándares constitucionales de protección de las comunicaciones.		●
Registros de conexión (metadatos) Se evalúa si la empresa se compromete a: (a) entregar registros de conexión únicamente bajo orden judicial; (b) o, en su defecto, establecer límites claros y restrictivos para su entrega, en línea con la protección constitucional de los metadatos como parte de la comunicación.		●
Prohibición de órdenes genéricas Se evalúa si la empresa: (a) se compromete a rechazar o impugnar solicitudes de acceso a datos que no identifiquen de manera específica a la persona afectada; (b) o que resulten desproporcionadas, amplias o carentes de fundamentación suficiente.	●	
Protocolos específicos y transparencia Se evalúa si la empresa: (a) cuenta con protocolos o lineamientos públicos que regulen la entrega de datos a autoridades en el marco de investigaciones penales; (b) y si estos protocolos contienen información clara, estructurada y comprensible sobre los criterios y procedimientos aplicables.	●	

Claro Paraguay, a través de América Móvil, ofrece un desarrollo intermedio de la regulación de solicitudes de datos por parte de las autoridades. Mientras que otros proveedores de servicios de internet carecen de políticas, existen referencias a los procesos internos de Claro Paraguay en sus informes de transparencia (América Móvil, 2025) o documentos corporativos, como el informe de sustentabilidad (América Móvil, 2024). Sin embargo, estas políticas son generales y carecen de la especificidad para suponer que la empresa adopta una interpretación claramente restrictiva de las solicitudes de datos, por lo tanto, alineada con las facetas más protectoras del derecho a la privacidad en Paraguay.

En relación con el subcriterio I (datos de registro), Claro no ha declarado de manera transparente las circunstancias en las que podría proporcionar datos de clientes o información básica de cuentas. Claro ha afirmado que opera dentro de la ley, pero la descripción es tan vaga que es imposible determinar si Claro restringe los datos a ciertos tipos de autoridades o en qué situaciones se requiere una orden judicial. Tampoco hay una distinción clara entre los diferentes tipos de solicitudes para verificar una política restrictiva en esta área.

Esta conclusión no se modifica por el hecho de que el informe identifique como base normativa el artículo 228 del Código Procesal Penal. Dicha disposición habilita al Ministerio Público a requerir información a entidades públicas y privadas en el marco de investigaciones penales, pero no establece criterios específicos sobre categorías de datos, niveles de protección o exigencia de control judicial. Por ello, la sola referencia a esta norma no permite verificar que la empresa adopte una interpretación restrictiva y protectora respecto de los datos de registro.

La ausencia de regulaciones en relación con los datos de geolocalización es aún más marcada en el subcriterio II. No hay regulación sobre el procesamiento o transmisión de datos de ubicación. Tampoco hay disposición para diferenciar entre datos de ubicación que se generan y datos de ubicación que ya existen. Tampoco hay información sobre la existencia de la necesidad de supervisión judicial de este tipo de datos. En vista de que los datos de geolocalización son uno de los tipos de datos más sensibles, esta ausencia de regulaciones es una de las deficiencias más importantes en la protección de la privacidad.

Si bien el informe de América Móvil identifica la geolocalización en tiempo real como una categoría diferenciada de solicitudes, no desarrolla las condiciones jurídicas aplicables a su entrega ni precisa si existe una exigencia de orden judicial para acceder a esta información. Tampoco distingue entre datos históricos y datos en tiempo real. En consecuencia, la referencia normativa resulta insuficiente para demostrar una política alineada con estándares reforzados de protección de la privacidad.

En cuanto al subcriterio III (registros de conexión), aunque los informes de transparencia de América Móvil incluyen referencias a diferentes tipos de solicitudes, incluidas aquellas de naturaleza metadato, no existe una regla específica que restrinja la entrega de dichos informes a solicitudes por orden judicial, ni hay criterios que consideren los metadatos protegidos de manera coherente con los criterios de los estándares de jurisprudencia constitucional e interamericana. Por lo tanto, no se puede decir que la empresa adopte una interpretación restrictiva al respecto.

Del mismo modo, aunque el informe distingue la categoría de datos conservados o metadatos, las normas citadas no son acompañadas de una explicación sobre las garantías aplicables a estos registros ni sobre la necesidad de control judicial para su acceso. Esta ausencia de precisiones resulta particularmente relevante considerando que la jurisprudencia constitucional e interamericana reconoce que los metadatos pueden revelar información sensible sobre la vida privada de las personas.

Por otro lado, en el subcriterio IV (prohibición de órdenes genéricas) se puede observar un desarrollo positivo. América Móvil justifica en sus informes la legalidad de las solicitudes que puedan o no recibir, sugiriendo que puede haber algunos controles internos para las solicitudes inapropiadas. Aunque no existe un compromiso formal para rechazar solicitudes genéricas, amplias o desproporcionadas, y no hay un mecanismo o criterio público explícito para identificarlas, la existencia de mecanismos de revisión legal permite establecer algunas salvaguardas legales preliminares en este caso. Por lo tanto, este subcriterio se cumple en cierta medida.

Finalmente, en el subcriterio V (protocolos específicos y transparencia), no hay cumplimiento total, aunque se evidencia cierto progreso. La publicación de informes de transparencia es un medio relevante para ejercer rendición de cuentas, ya que muestran cómo se gestionan las solicitudes de las autoridades y qué tipo de controles se ejercen, aunque en términos generales. Sin embargo, estos informes no ofrecen un protocolo estructurado, detallado y accesible que describa el proceso para las solicitudes, evaluaciones y el envío de datos. Además, no existen guías accesibles públicamente para las autoridades o el público en general que les permitan comprender completamente los criterios aplicados. En este sentido, a pesar del bajo nivel de progreso en el desarrollo de la transparencia, no es un protocolo completamente desarrollado, por lo que se considera que este subcriterio se cumple parcialmente.

Claro presenta un desarrollo intermedio en este criterio. A diferencia de otras ISP, cuenta con mecanismos de evaluación interna y cierto nivel de transparencia, pero estos no se traducen en reglas claras, diferenciadas y plenamente garantistas para la entrega de datos en investigaciones penales. La empresa no define de manera precisa cómo trata distintos tipos de datos ni establece compromisos explícitos frente a riesgos como solicitudes genéricas o falta de control judicial.

En consecuencia, corresponde asignar una calificación de tres cuartos de estrella al cumplir con dos criterios.

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

Protocolo de entrega de datos para investigaciones penales		
	Sí	**No**
Datos de registro (información de suscriptores) Se evalúa si la empresa: (a) establece que los datos de registro solo serán entregados a autoridades competentes debidamente identificadas, limitando su acceso a supuestos legalmente habilitados; (b) y/o exige orden judicial cuando la solicitud excede los supuestos administrativos o presenta riesgos para el derecho a la privacidad.		●
Datos de geolocalización Se evalúa si la empresa: (a) distingue claramente los datos de geolocalización de otros tipos de datos personales;b) y establece que su entrega —especialmente en tiempo real— requiere orden judicial, conforme a los estándares constitucionales de protección de las comunicaciones.		●
Registros de conexión (metadatos) Se evalúa si la empresa se compromete a: (a) entregar registros de conexión únicamente bajo orden judicial; (b) o, en su defecto, establecer límites claros y restrictivos para su entrega, en línea con la protección constitucional de los metadatos como parte de la comunicación.		●
Prohibición de órdenes genéricas Se evalúa si la empresa: (a) se compromete a rechazar o impugnar solicitudes de acceso a datos que no identifiquen de manera específica a la persona afectada; (b) o que resulten desproporcionadas, amplias o carentes de fundamentación suficiente.	●	
Protocolos específicos y transparencia Se evalúa si la empresa: (a) cuenta con protocolos o lineamientos públicos que regulen la entrega de datos a autoridades en el marco de investigaciones penales; (b) y si estos protocolos contienen información clara, estructurada y comprensible sobre los criterios y procedimientos aplicables.	●	

Tigo Paraguay, a través de Millicom, presenta un nivel intermedio de desarrollo en la gestión de solicitudes de acceso a datos por parte de autoridades. Esto se refleja principalmente en el Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024)). A diferencia de las empresas que no tienen documentación en absoluto, en este caso es realmente posible identificar algunas políticas y citar algunos procesos internos. Sin embargo, estos aspectos no conforman un sistema normativo

claro, detallado y explícitamente alineado, que puede ser interpretado como orientado a garantizar el derecho a la privacidad en el contexto de Paraguay.

En relación con el subcriterio I (datos de registro), el informe LED menciona que la empresa evalúa la legalidad de las solicitudes realizadas antes de entregar los datos. Sin embargo, la declaración es bastante general, y no se pueden determinar reglas específicas y públicamente disponibles que dicten las circunstancias en las que se entregan los datos de registro, ni las circunstancias específicas que requieren una orden judicial. Tampoco se establece una distinción precisa entre los diversos tipos de autoridades solicitantes. La falta de detalles impide la evaluación de una política que sea restrictiva y protectora en esta área.

Respecto del subcriterio II (datos de geolocalización), el documento no especifica regulaciones que rigen la provisión de este tipo de datos. El documento no especifica la distinción entre datos de geolocalización en tiempo real y datos de geolocalización históricos. El documento no especifica si los datos de geolocalización, en general, están sujetos a un estándar de protección más fuerte, como un estándar que requiere una orden judicial. Por la evidente sensibilidad de los datos, esto puede considerarse una brecha importante.

En cuanto al subcriterio III (registros de conexión), el informe LED clasifica estos como incluyendo metadatos y otros tipos de información técnica. Esta clasificación en sí misma no proporciona una regla significativa que limite su provisión de metadatos a casos de una orden judicial. Además, no existen criterios desarrollados que reconozcan explícitamente la naturaleza protegida de los metadatos como consistente con los estándares constitucionales e interamericanos. Por lo tanto, no puede afirmarse que exista una política restrictiva respecto a este tipo de datos.

No obstante, Millicom muestra un desarrollo parcialmente positivo en el subcriterio IV respecto a la prohibición de órdenes genéricas. En el informe de la empresa, explica que evalúa la base legal de las órdenes que recibe y que, en caso de inconsistencias legales o posibles incumplimientos legales, cuestionará las órdenes e incluso podrá acudir a la justicia. Esto demuestra la existencia de mecanismos de control interno respecto a las demandas gubernamentales. Sin embargo, carece de una disposición explícita para rechazar órdenes genéricas, vagas o desproporcionadas y de una especificación pública de los criterios para identificar dichas órdenes. Por lo tanto, aunque existen algunos mecanismos elementales, no son sólidos, y la empresa se considera parcialmente cumplidora en este subcriterio.

Finalmente, bajo el subcriterio V (protocolos específicos y transparencia), el informe LED es un avance importante en transparencia, ya que describe, en términos generales, cómo la empresa responde a las solicitudes de acceso a datos y hace visibles algunos procesos internos. Sin embargo, este informe no proporciona un protocolo estructurado, sistemático y deliberadamente accesible para comprender los procesos de recepción, evaluación y entrega de información. También faltan en las pautas publicadas públicamente dirigidas a las autoridades o al público que especifican los estándares utilizados en los procedimientos penales. Por lo tanto, aunque hay algún desarrollo en términos de transparencia, es de una naturaleza muy básica y no es suficiente para alcanzar el estándar, y por lo tanto se evalúa como parcialmente cumplido en este subcriterio.

Por ello, corresponde asignar una calificación de tres cuartos de estrella al cumplir con dos criterios.

personal

PERSONAL - NÚCLEO S.A.

Protocolo de entrega de datos para investigaciones penales		
	Sí	**No**
Datos de registro (información de suscriptores) Se evalúa si la empresa: (a) establece que los datos de registro solo serán entregados a autoridades competentes debidamente identificadas, limitando su acceso a supuestos legalmente habilitados; (b) y/o exige orden judicial cuando la solicitud excede los supuestos administrativos o presenta riesgos para el derecho a la privacidad.		●
Datos de geolocalización Se evalúa si la empresa: (a) distingue claramente los datos de geolocalización de otros tipos de datos personales;b) y establece que su entrega —especialmente en tiempo real— requiere orden judicial, conforme a los estándares constitucionales de protección de las comunicaciones.		●
Registros de conexión (metadatos) Se evalúa si la empresa se compromete a: (a) entregar registros de conexión únicamente bajo orden judicial; (b) o, en su defecto, establecer límites claros y restrictivos para su entrega, en línea con la protección constitucional de los metadatos como parte de la comunicación.		●
Prohibición de órdenes genéricas Se evalúa si la empresa: (a) se compromete a rechazar o impugnar solicitudes de acceso a datos que no identifiquen de manera específica a la persona afectada; (b) o que resulten desproporcionadas, amplias o carentes de fundamentación suficiente.		●
Protocolos específicos y transparencia Se evalúa si la empresa: (a) cuenta con protocolos o lineamientos públicos que regulen la entrega de datos a autoridades en el marco de investigaciones penales; (b) y si estos protocolos contienen información clara, estructurada y comprensible sobre los criterios y procedimientos aplicables.		●

Personal Paraguay indica una capacidad limitada para gestionar las solicitudes de datos de la agencia en el contexto de los procesos de justicia. En comparación con otras empresas en el estudio, no se identifican, cuando corresponde, documentos locales ni de la matriz que establezcan instrucciones, criterios o protocolos para comprender cómo la empresa procesa las solicitudes de acceso a datos.

En relación con el subcriterio I (datos de registro), Personal no ha declarado públicamente las circunstancias bajo las cuales divulgan datos de suscriptores o cuentas. No existen criterios que establezcan las autoridades que están autorizadas a solicitar dichos datos o las situaciones en las que se consideraría necesaria una orden judicial. Esto hace que sea imposible confirmar si la empresa impone o no restricciones o controles sobre el intercambio de dicha información.

Respecto del subcriterio II (datos de geolocalización), no hay referencias al procesamiento o al suministro de datos de ubicación. La empresa no distingue entre datos en tiempo real y datos pasados, ni aclara si este tipo de información está bajo el control del poder judicial. La ausencia de regulaciones explícitas es una deficiencia notable, dado el nivel de sensibilidad de estos datos.

En cuanto al subcriterio III (registros de conexión), no existen reglas sobre la entrega de metadatos de relaciones o registros técnicos del uso del servicio. No hay reglas que estipulen restricciones, condiciones o requisitos de orden judicial para este tipo de datos, lo que significa que no hay forma de determinar una política en línea con los estándares constitucionales de protección de la comunicación.

En el subcriterio IV (prohibición de órdenes genéricas), no se identifican compromisos explícitos de rechazar o impugnar solicitudes amplias, genéricas o desproporcionadas. La empresa no informa si exige un nivel mínimo de especificidad en los requerimientos ni si cuenta con mecanismos de control frente a posibles abusos por parte de autoridades.

Finalmente, respecto del subcriterio V (protocolos específicos y transparencia), Personal no publica guías, protocolos ni lineamientos que regulen la entrega de datos a autoridades en investigaciones penales. Tampoco existen documentos que describan el procedimiento de recepción, evaluación y respuesta a este tipo de solicitudes, ni información orientada a autoridades o personas usuarias.

En consecuencia, corresponde asignar una calificación de
estrella vacía, al no cumplir con ningún criterio.

CONCLUSIÓN

La investigación para esta edición muestra el mismo patrón que ediciones anteriores para el mercado de Proveedores de Servicios de Internet (ISP) paraguayos, confirmando que existen inconsistencias, en relación con el tipo de empresa, así como la evolución de sus políticas y su disposición a adoptar prácticas de transparencia pública. En comparación con años anteriores, esta vez, la investigación ha incluido a Starlink y ha excluido a actores locales, como COPACO y VOX. Esto ha reestructurado parcialmente las comparaciones, pero no ha cambiado las conclusiones principales.

En general, entre las empresas con presencia internacional, América Móvil (Claro) y Millicom (Tigo) siguen siendo los actores que más han avanzado respecto a ciertos indicadores, especialmente en transparencia y formulación de políticas. Sin embargo, este progreso ha sido parcial, lento y, en muchos casos, más formal que real. En contraste, Personal sigue rezagada en casi todas las dimensiones, mientras que Starlink es una excepción al obtener mejores resultados en criterios vinculados a políticas y documentación pública, aunque mantiene bajos niveles de transparencia respecto al acceso estatal a datos de personas usuarias.

Políticas de privacidad y datos personales

Las ISPs revisadas en su mayoría tienen alguna forma de política de privacidad. Sin embargo, existen problemas principales, como la falta de claridad en los documentos de política, presencia de contradicciones y ausencia de elementos importantes. Claro, Tigo y Personal tienen documentos disponibles, pero ninguno aborda los períodos de retención de datos relevantes ni los criterios de procesamiento, lo que socava principios fundamentales de la Ley Nº 7593/2025, como la minimización de datos y la limitación de finalidad.

En el caso de Tigo, hay una falta de claridad y contradicciones internas en el alcance de los documentos contractuales y las políticas de privacidad, mientras que Personal presenta un bajo nivel de desarrollo y claridad. Por otro lado, Starlink ofrece documentos que en general son claros, pero carecen de adaptaciones en relación con el contexto paraguayo respecto a la ausencia de garantías a nivel local, lo que a su vez limita su evaluación en un contexto de cumplimiento sustantivo.

Autorización judicial

Este análisis reafirma una tendencia establecida en ediciones anteriores: los proveedores de servicios de Internet no adoptan de manera constante una posición garantista respecto a la exigencia de una orden judicial en relación con el tratamiento de metadatos.

Si generalmente existe una demanda de que se requiere una orden judicial para acceder al contenido de las comunicaciones y esa demanda está alineada con la Constitución Nacional (arts. 33 y 36) y el Código Procesal Penal, entonces esa demanda no se extiende (o no se extiende claramente) a otros tipos de datos (registro de conexiones, geolocalización, etc.).

Además, el análisis no resuelve las ambigüedades restantes sobre el papel del Ministerio Público como autoridad que solicita los datos y la tensión que esto genera en relación con el principio de control judicial previo que ha sido establecido tanto a nivel nacional como por la jurisprudencia de la Corte Interamericana de Derechos Humanos (Escher vs. Brasil, CAJAR vs. Colombia).

Notificación a la persona usuaria

Similar a las ediciones anteriores, los proveedores de servicios de internet examinados no notifican a los clientes sobre el acceso a sus datos.

Esta ausencia muestra un problema relacionado con la transparencia y el debido proceso, e ilustra una desalineación con los estándares internacionales que establecen la notificación como una salvaguarda básica contra la infracción de la privacidad de los ciudadanos.

Políticas para la promoción y defensa de los derechos humanos

Este compromiso entre los proveedores de servicios de Internet en promover los derechos humanos tiende a basarse más en requisitos corporativos internacionales que en un compromiso local concreto.

Mejores calificaciones en este indicador son registradas por Tigo y Claro, gracias a su alineación con parámetros globales y su membresía en iniciativas del sector. Sin embargo, no se detectan, en particular, acciones sustanciales y/o posturas públicas explícitas, especialmente sobre el tema de protección de la privacidad, a nivel local.

En cuanto a Personal, obtiene una puntuación aún más baja, con la ausencia de iniciativas de importancia considerable en la región.

Transparencia

La falta de transparencia sigue siendo una de las principales debilidades observadas entre las ISP analizadas. En Paraguay, únicamente Claro y Tigo publican informes de transparencia relacionados con solicitudes de acceso a datos por parte de autoridades. Estos documentos son elaborados por las empresas matrices de ambos grupos y constituyen avances relevantes en materia de rendición de cuentas.

No obstante, existen diferencias importantes entre ellos. El informe de América Móvil incorpora información específica para Paraguay, incluyendo referencias al marco normativo aplicable y desagregaciones de distintas categorías de solicitudes, lo que permite comprender con mayor precisión algunas prácticas de la empresa en el país. En cambio, el informe de Millicom ofrece un nivel de detalle más limitado respecto a Paraguay y presenta información principalmente desde una perspectiva regional. Aun así, en ambos casos persisten limitaciones relacionadas con la falta de información exhaustiva sobre determinadas categorías de datos y sobre los criterios concretos utilizados para atender solicitudes de las autoridades, lo que dificulta una evaluación completa del alcance de la colaboración estatal y de las salvaguardas aplicadas.

Starlink y Personal ni siquiera publican informes de transparencia, lo que indica una total falta de responsabilidad.

Guías para la solicitud de información

Existe una distinción notable entre las ISP en cuanto a la existencia de directrices para las autoridades. Claro y Tigo han desarrollado directrices hasta cierto punto, gracias nuevamente a la influencia impulsora de sus empresas matrices, pero Personal y Starlink carecen de cualquier tipo de directrices públicas concretas, lo cual tiene un impacto negativo en la previsibilidad y transparencia en los procedimientos de acceso a los datos.

Accesibilidad

El análisis de accesibilidad muestra variaciones significativas entre los proveedores. Tanto Tigo como Starlink superan las expectativas en accesibilidad y están respaldados por evaluaciones técnicas. Claro presenta deficiencias importantes, mientras que Personal tiene una accesibilidad pobre y múltiples fallas estructurales que perjudican su experiencia de usuario.

Este criterio demuestra que la accesibilidad no es homogénea y está determinada por las prioridades técnicas de la empresa y cuánto están dispuestos a invertir

Protocolo de entrega de datos para investigaciones penales

La incorporación de este criterio permite una mejor identificación de las deficiencias estructurales del sector. En general, las ISP carecen de políticas transparentes, diferentes y públicamente disponibles que rijan la información que proporcionan durante el contexto de procesos penales y la interpretación protectora del derecho a la privacidad.

Claro y Tigo muestran algunos avances, pero no logran establecer reglas formales respecto a los diferentes tipos de datos, ni establecen compromisos formales respecto a riesgos como órdenes amplias o solicitudes desproporcionadas. En el caso de Personal y Starlink, hay una total falta de desarrollo en este sentido.

RECOMENDACIONES

Esta evaluación indica que los proveedores de servicios de Internet en Paraguay han avanzado, sin embargo, existen prácticas problemáticas en transparencia, protección de datos y límites a la intervención del Estado. Para abordar estos problemas, las empresas deben mejorar sus políticas de privacidad para que sean claras, exhaustivas y coherentes, además de alinearlas con la Ley No. 7593/2025 e incorporar aspectos clave, como los plazos de conservación de datos y las bases legales para el procesamiento de datos.

También es importante que adopten una interpretación más estricta del marco legal y garanticen que el contenido, los metadatos y todas las demás formas de datos solo sean accedidos bajo el control del poder judicial y el principio de proporcionalidad. En este sentido, la ausencia de mecanismos de notificación para los usuarios es una de las deficiencias más significativas del campo. Por lo tanto, se recomienda que los esfuerzos se orienten a desarrollar dichos mecanismos como un criterio mínimo de transparencia y debido proceso.

En cuanto a la transparencia, los proveedores de servicios de Internet (ISP) deben elaborar informes públicos, especialmente relacionados con la información sobre solicitudes de datos recibidas y atendidas. Asimismo, existe un requisito de transparencia en el desarrollo de protocolos para la entrega de datos en investigaciones criminales, donde se clarifican las diferencias en los tipos de datos y las solicitudes abusivas son sujetas a exclusión.

También se recomienda la elaboración de guías dirigidas a autoridades y la adopción de procesos internos más firmes para la evaluación de requerimientos, así como mejoras en la accesibilidad de sus plataformas digitales, garantizando el acceso a la información para todas las personas usuarias.

Finalmente, las ISP deben asumir un rol más activo en la promoción de los derechos humanos, mediante iniciativas de concienciación, participación en espacios sectoriales y acciones frente a solicitudes indebidas. En definitiva, el fortalecimiento de la protección de datos en Paraguay no depende únicamente del marco normativo, sino de su implementación efectiva por parte de las empresas, lo que exige pasar de un enfoque formal a uno sustantivo en la protección del derecho a la privacidad.

BIBLIOGRAFÍA

América Móvil. (2024). Informe de sostenibilidad 2024. https://sostenibilidad.americamovil.com/portal/su/pdf/Informe-de-Sostenibilidad-2024.pdf

América Móvil. (2025). Informe de transparencia en las comunicaciones 2025. https://sostenibilidad.americamovil.com/portal/su/pdf/Informe-de-Transparencia-de-las-Comunicaciones-2025.pdf

AMX Paraguay S.A. (s. f.-a). Políticas de Privacidad. Claro Paraguay. Recuperado 26 de abril de 2026, de https://www.claro.com.py/personas/politicas-de-privacidad

AMX Paraguay S.A. (s. f.-b). Términos y Condiciones Mi Claro. Claro Paraguay. Recuperado 26 de abril de 2026, de https://www.claro.com.py/personas/legal-y-regulatorio/mi-claro

AMX Paraguay S.A. (s. f.-c). Términos y condiciones: Servicio de Internet WiFi. Claro Paraguay. Recuperado 26 de abril de 2026, de https://www.claro.com.py/personas/legal-y-regulatorio/servicio-de-internet-wifi

Asamblea General, N. U. (2016, febrero 1). Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. https://unctad.org/es/system/files/official-document/ares70d125_es.pdf

Banco Central del Paraguay. (2023, febrero 21). Resolución No 3/2023. https://www.bcp.gov.py/documents/20117/381887/Resolucion+3+acta+8%281%29.pdf/540aadf3-e563-4cee-f7f2-783b72cd4656?t=1742583379310

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

CIDH. (2013, diciembre 31). Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf

CIDH. (2023a, octubre 18). Resumen oficial emitido por la Corte Interamericana. https://corteidh.or.cr/docs/casos/articulos/resumen_506_esp.pdf

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

CIDH. (2025, septiembre 7). Relatoría Especial para la Libertad de Expresión. El impacto de la vigilancia digital en la libertad de expresión en las Américas. https://www.oas.org/es/cidh/expresion/informes/vigilanciaRELE.pdf

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

CONATEL. (2024, septiembre 20). Resolucion № 2583/2024 POR LA CUAL SE ESTABLECE LA OBLIGATORIEDAD PARA TODOS LOS LICENCIATARIOS DEL SERVICIO DE ACCESO A INTERNET Y TRANSMISIÓN DE DATOS DE CONSERVAR LOS REGISTROS DE CONEXIÓN. https://www.conatel.gov.py/conatel/wp-content/uploads/2024/09/resolucion-directorio-nro-2583-2024.pdf

CONATEL. (2025). Indicadores de mercado. Periodo 2025. https://www.conatel.gov.py/conatel/indicadores/

Consejo de Derechos Humanos, N. U. (2016, junio 27). Resolución sobre Promoción y protección de derechos humanos en Internet. https://ap.ohchr.org/documents/s/hrc/d_res_dec/a_hrc_32_l20.pdf

EFF. (2024, abril 3). En victoria histórica para los derechos humanos en Colombia, la Corte Interamericana declara que organismos estatales violaron derechos humanos de abogados que defendían a activistas. | Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/04/historic-victory-human-rights-colombia-inter-american-court-finds-state-agencies?language=es

Global Network Initiative. (s. f.). Members. Global Network Initiative. Recuperado 26 de abril de 2026, de https://globalnetworkinitiative.org/who-we-are/members/

GSMA. (s. f.). Our Members. Membership. Recuperado 26 de abril de 2026, de https://www.gsma.com/get-involved/gsma-membership/our-members/

INE. (2024). Tecnología de la Información y Comunicación en el Paraguay 2024. https://www.ine.gov.py/Publicaciones/Biblioteca/documento/280/Tics%202024_INE.pdf

InternetLab. (2025). Quem Defende Seus Dados? https://quemdefendeseusdados.org.br/pt/

La Política Online. (2024, enero 8). Tigo es víctima de un hackeo de su base de datos y se reaviva el debate sobre regulación en ciberseguridad—La Política Online. https://www.lapoliticaonline.com/paraguay/economia-py/tigo-es-victima-de-un-hackeo-de-su-base-de-datos-y-se-reaviva-el-debate-sobre-regulacion-en-ciberseguridad/

Millicom International Cellular S.A. (2023, junio 30). Human Rights Policy. https://www.millicom.com/media/5601/mic-tpl-gov-policy-human-rights-policy_vf-june-16-002.pdf

Millicom International Cellular S.A. (2024). Law Enforcement Disclosure Report (LED). https://ww2-cdn.tigocloud.net/2024_LED_Report2_0b0376e254.pdf

Naciones Unidas. (1948, diciembre 10). Declaración Universal de Derechos Humanos. https://paraguay.un.org/sites/default/files/2020-01/declaracion_universal_de_derechos_humanos_-_version_castellano.pdf

Naciones Unidas. (2006, diciembre 12). CONVENCIÓN SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD. https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-persons-disabilities

Naciones Unidas. (2011). Principios Rectores Sobre las Empresas y los Derechos Humanos: Puesta en Práctica del marco de las Naciones Unidas para “proteger, Respetar y Remediar”. United Nations. https://doi.org/10.18356/3b7fe68b-es

Naciones Unidas. (2013, abril 17). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión. A/HRC/23/40. https://docs.un.org/es/A/HRC/23/40

Necesario y proporcionado. Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. (2014, mayo). https://necessaryandproportionate.org/files/spanish_principles_2014.pdf

Personal Paraguay. (s. f.-a). Privacidad de datos. Personal Paraguay. Recuperado 26 de abril de 2026, de https://www.personal.com.py/institucional/privacidad-de-datos.html

Personal Paraguay. (s. f.-b). Términos y Condiciones. Personal Paraguay. Recuperado 26 de abril de 2026, de https://www.personal.com.py/institucional/terminos-y-condiciones.html

Personal Paraguay. (s. f.-c). Términos y condiciones de Aplicaciones de Personal. Personal Paraguay. Recuperado 26 de abril de 2026, de https://www.personal.com.py/institucional/terminos-y-condiciones-apps.html

Presidencia de la Republica del Paraguay. (1989, agosto 8). Ley No 1 / APRUEBA Y RATIFICA LA CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS O PACTO DE SAN JOSÉ DE COSTA RICA. https://www.bacn.gov.py/leyes-paraguayas/2619/aprueba-y-ratifica-la-convencion-americana-sobre-derechos-humanos-o-pacto-de-san-jose-de-costa-rica

Presidencia de la Republica del Paraguay. (1992, junio 20). CONSTITUCION DE LA REPUBLICA DEL PARAGUAY. Baccn. https://www.bacn.gov.py/leyes-paraguayas/9580/constitucion-nacional-

Presidencia de la Republica del Paraguay. (1995, diciembre 29). LEY No 642/95 DE TELECOMUNICACIONES. https://www.conatel.gov.py/conatel/wp-content/uploads/2025/05/ley-nro.-642-95-de-telecomunicaciones.pdf

Presidencia de la Republica del Paraguay. (1998a). Código Procesal Penal de la República del Paraguay—Ley 1286/98.

Presidencia de la Republica del Paraguay. (1998b). LEY No 1286/1998 CÓDIGO PROCESAL PENAL DE LA REPÚBLICA DEL PARAGUAY. https://www.pj.gov.py/ebook/libros_files/codigo-procesal-penal.pdf

Presidencia de la Republica del Paraguay. (2013, marzo 1). LEY № 4868 COMERCIO ELECTRONICO. https://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico

Presidencia de la Republica del Paraguay. (2014, enero 27). Decreto N.o 1.165/14 POR EL CUAL SE APRUEBA EL REGLAMENTO DE LA LEY No 4868 DEL 26 DE FEBRERO DE 2013 «DE COMERCIO ELECTRÓNICO». https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/decreto__1165_2014_ce0.pdf

Presidencia de la Republica del Paraguay. (2020, octubre 27). Ley No 6534/2020 DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS. Baccn. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

Presidencia de la Republica del Paraguay. (2021a, junio 1). Ley No 6738 / ESTABLECE LA MODALIDAD DEL TELETRABAJO EN RELACIÓN DE DEPENDENCIA. https://www.bacn.gov.py/leyes-paraguayas/9582/ley-n-6738-establece-la-modalidad-del-teletrabajo-en-relacion-de-dependencia

Presidencia de la Republica del Paraguay. (2021b, diciembre 30). LEY No 6822 DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS. https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/Ley%20Nro%206822-2021pdf.pdf

Presidencia de la Republica del Paraguay. (2025a, noviembre 27). Gaceta № 287. https://www.gacetaoficial.gov.py/index/detalle_publicacion/93911

Presidencia de la Republica del Paraguay. (2025b, noviembre 27). Ley No 7593/2025 / DE PROTECCIÓN DE DATOS PERSONALES EN LA REPÚBLICA DEL PARAGUAY. Baccn. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-2025-de-protecci-n-de-datos-personales-en-la-rep-blica-del-paraguay

Sequera. M (2024). Starlink en Paraguay: ¿existen riesgos o preocupaciones sobre esta tecnología? TEDIC. https://www.tedic.org/starlink-en-paraguay-existen-riesgos-o-preocupaciones-sobre-esta-tecnologia/

SpaceX. (s. f.). Commitment to space sustainability. Recuperado https://starlink.com/public-files/Commitment%20to%20Space%20Sustainability.pdf?srsltid=AfmBOoqpB5Q028-H-SxQqZ4xSmgt7_sfCiUnVSNilFMMvi8iml6zPidz&utm

SpaceX. (2024, abril 1). SpaceX website privacy policy. https://www.spacex.com/assets/media/privacy_policy_spacex.pdf?

Starlink. (s. f.-a). Política de Uso Aceptable de Starlink. Starlink. Recuperado 23 de abril de 2026, de https://starlink.com/legal/documents/DOC-1001-59234-61?regionCode=PY

Starlink. (s. f.-b). Política de Uso Razonable y Política de Gestión Del Tráfico. Starlink. Recuperado 23 de abril de 2026, de https://starlink.com/legal/documents/DOC-1469-65206-75?regionCode=PY

Starlink. (s. f.-c). Términos de servicio de Starlink. Starlink. Recuperado 23 de abril de 2026, de https://starlink.com/legal/documents/DOC-1526-27522-68?regionCode=PY

Starlink. (2026, enero 15). Política de Privacidad de Starlink. Starlink. https://starlink.com/legal/documents/DOC-1000-41799-67?regionCode=PY

TEDIC. (2017). ¿QUIÉN DEFIENDE TUS DATOS? 2017. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2017.pdf

TEDIC. (2020). ¿QUIÉN DEFIENDE TUS DATOS? 2020. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2020.pdf

TEDIC. (2022). ¿QUIÉN DEFIENDE TUS DATOS? 2022. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2022_v2.pdf

TEDIC. (2024a). ¿QUIÉN DEFIENDE TUS DATOS? 2024. https://www.tedic.org/wp-content/uploads/2025/02/QDTD_Paraguay_2024-WEB.pdf

TEDIC. (2025, noviembre 28). La ley sobre la protección de datos personales en Paraguay: Un logro colectivo basado en evidencia y participación plural. TEDIC. https://www.tedic.org/la-ley-sobre-la-proteccion-de-datos-personales-en-paraguay-un-logro-colectivo-basado-en-evidencia-y-participacion-plural/

Tigo Paraguay. (s. f.). Responsabilidad Corporativa. Tigo Paraguay. Recuperado 26 de abril de 2026, de https://www.tigo.com.py/conocenos/responsabilidad-corporativa

Tigo Paraguay. (2025a, agosto 5). Politica de privacidad. Tigo Paraguay. Tigo. https://www.tigo.com.py/legales#terminos-y-condiciones-politica-de-privacidad

Tigo Paraguay. (2025b, agosto 5). Términos y Condiciones de Uso web. Tigo. Tigo. https://www.tigo.com.py/legales#terminos-y-condiciones-uso-de-web

Tigo Paraguay. (2025c, diciembre). CONTRATO ÚNICO DE SERVICIOS DE TELECOMUNICACIONES. https://discovery-content-py.tigocloud.net/uploads/TIGO_Contrato_unico_diciembre_2025_final_2165d13302.pdf

United Nations Global Compact. (s. f.). Our Participants. Recuperado 26 de abril de 2026, de https://unglobalcompact.org/what-is-gc/participants

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

Web Accessibility Tool. (s. f.-a). Resultado evaluacion Claro Py. WAVE. Recuperado https://wave.webaim.org/report#/https://www.claro.com.py/personas

Web Accessibility Tool. (s. f.-b). Resultado evaluacion Personal Py. WAVE. Recuperado https://wave.webaim.org/report#/https://www.personal.com.py/

Web Accessibility Tool. (s. f.-c). Resultado evaluacion Starlink. WAVE. Recuperado https://wave.webaim.org/report#/https://starlink.com/py

Web Accessibility Tool. (s. f.-d). Resultado Evaluacion Tigo Py. WAVE. Recuperado https://wave.webaim.org/report#/https://www.tigo.com.py/

Tecnología
& Derechos
Humanos

ISBN 978-99989-999-4-7