Telefónica

Informe de **Transparencia** en las Comunicaciones 2019

Índice

Introducción

En nuestro compromiso con los derechos fundamentales de privacidad y libertad de expresión publicamos el cuarto informe de transparencia de las Comunicaciones con el objetivo de contribuir a generar una sociedad más abierta y transparente.

El respeto y la promoción de los derechos humanos, y en particular la privacidad y la libertad de expresión, adquieren en el mundo digital una nueva dimensión gracias al uso de las nuevas tecnologías y el protagonismo de los datos a escala global.

Las operadoras de telecomunicaciones tenemos el deber y la obligación legal de responder a las peticiones de las autoridades competentes en los países donde operamos para garantizar la seguridad y los derechos de sus ciudadanos, siempre bajo el respeto de la ley y los derechos y libertades fundamentales.

Por ello, la transparencia es un ejercicio imprescindible en un mundo en el que se comparten espacios de responsabilidad a la hora de preservar y garantizar los derechos de las personas.

Nuestra gobernanza

Tenemos establecido un modelo de gestión de responsabilidades claras en la protección de los derechos humanos en general y en privacidad y libertad de expresión en particular.

La promoción y protección recae bajo la supervisión del Consejo de Administración, a través de la Comisión de Regulación y Asuntos Institucionales. El Consejo de Administración es el órgano responsable de aprobar las Políticas Globales del Grupo.

Más información, en el apartado **"Políticas y procedimientos de aplicación"**.

La Comisión de Regulación y Asuntos Institutionales (Comité permanente del Consejo) se encarga de impulsar y seguir la implementación de nuestro Plan Global de Negocio Responsable, que incluye objetivos específicos en materia de privacidad y libertad de expresión. Es informado mensualmente sobre la implementación del Plan a través de la Dirección de Ética Corporativa y Sostenibilidad que dirige la Oficina de Negocio Responsable que integra los máximos responsables de las áreas operativas a nivel global.

La dirección de Ética Corporativa y Sostenibilidad coordina el trabajo de identificar, evaluar y abordar los riesgos y oportunidades relacionados con los derechos humanos y promover el diálogo sobre estos asuntos con todos los grupos de interés.

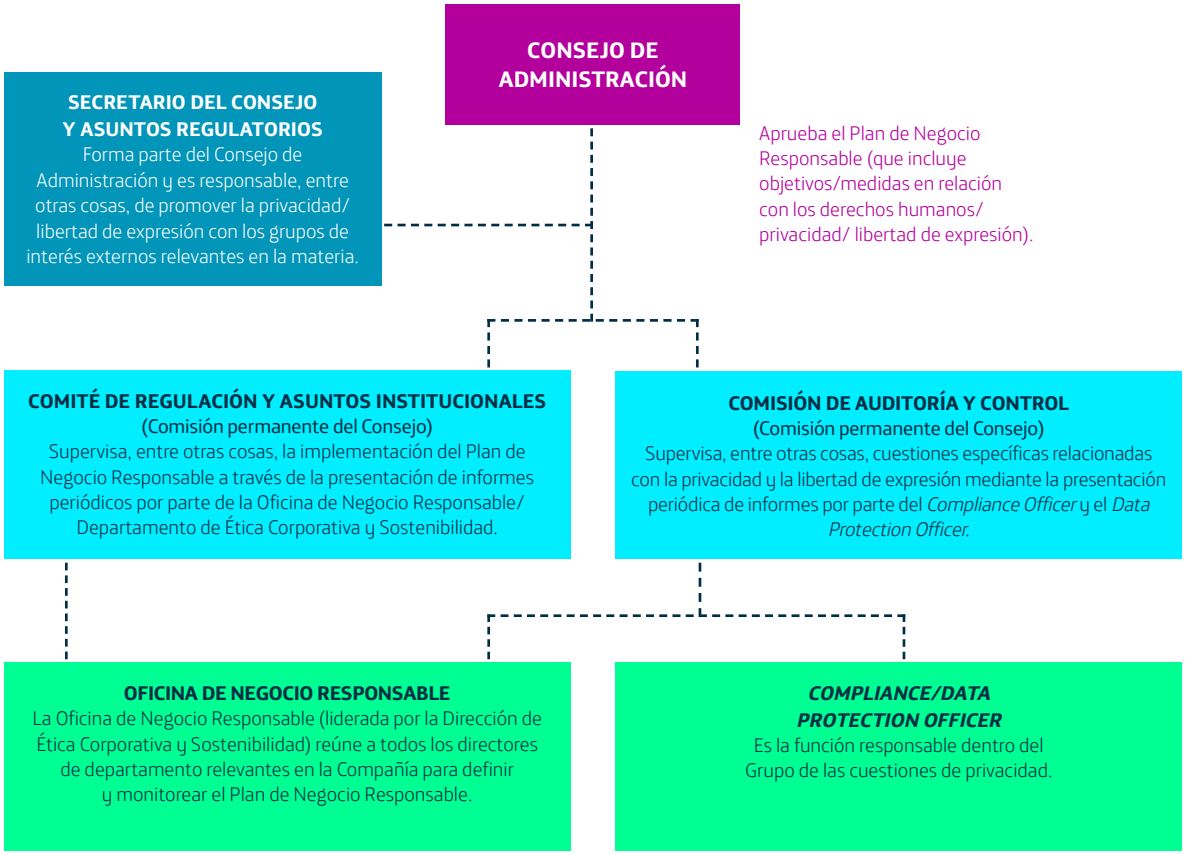
Los resultados de las evaluaciones de impacto en derechos humanos son presentados a la Oficina de Negocio Responsable, así como a la Comisión del Consejo de Administración encargada del seguimiento del Plan de Negocio Responsable, para que se tenga en cuenta en sus procesos de toma de decisiones.

El *"Data Protection Officer"* (DPO) es el responsable dentro del Grupo de la protección de datos personales y reporta directamente al Consejo de Administración a través de la Comisión de Auditoría y Control (Comisión permanente del Consejo). El DPO coordina el *"Steering Committee"* en el que participan todas las áreas corporativas relevantes para asuntos específicos relacionados con la privacidad y la libertad de expresión. Como miembro de la Oficina de Negocio Responsable, el DPO también reporta regularmente a dicha Oficina las cuestiones relacionadas con su función.

Además, el Secretario General y Asuntos Regulatorios forma parte del Consejo de Administración y es responsable, entre otras cosas, de promover la privacidad y la libertad de expresión con los grupos de interés externos relevantes en la materia. En esta función, también dirigió la publicación y difusión del "Manifiesto Digital" en 2018, en el que se aboga por la cooperación entre los gobiernos, las empresas y la sociedad civil para definir un *"New Digital Deal"* que adapte el entorno normativo actual a la era digital, prestando especial atención a las cuestiones de la privacidad y la libertad de expresión.

Más información, en el estudio de caso:
www.telefonica.com/manifiesto-digital

La siguiente figura resume gráficamente este modelo de gobernanza.



Para los asuntos de privacidad y libertad de expresión relacionados con las peticiones de las autoridades contamos con un Comité de Transparencia integrado por los responsables de las áreas globales de Secretaría General, Cumplimiento, Auditoría Interna y Ética Corporativa y Sostenibilidad. Estos analizan los datos reportados y pueden realizar las observaciones que consideren pertinentes, con carácter general o específicamente en relación con la información facilitada por las operadoras. El objetivo es asegurar en todo momento la calidad de la información como evidencia del cumplimiento de la normativa vigente y de la protección de los derechos fundamentales de las personas.

Aquellas peticiones que, por sus características y excepcionalidad así lo requieren, son analizadas por los máximos responsables de cada unidad mediante la adecuada ponderación de todos los intereses potencialmente comprometidos. Entre ellos, se incluyen los derechos humanos, libertades fundamentales u otros intereses que pudieran ser de aplicación y, si se diesen las circunstancias, por los órganos que dentro de cada compañía tengan entre sus funciones la evaluación y gestión de situaciones que pudieran eventualmente desembocar en una crisis.

Nuestro compromiso y procesos de debida diligencia

Desde 2006 los derechos humanos forman parte integral de nuestros Principios de Negocio Responsable. Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas nos han servido de guía fundamental para fomentar la garantía y respeto del derecho de las personas y, específicamente, en lo referente a la privacidad y libertad de expresión.

Somos miembros constituyentes del Grupo de Diálogo de la Industria de Telecomunicaciones para la Libertad de Expresión y la Privacidad (TID) , grupo que se fusionó con el *Global Network Initiative* (GNI) en 2017. Se trata de una organización de escala global de la que son miembros inversores, *think tanks* y sociedad civil y compañías privadas: operadores de telecomunicaciones, proveedores de servicios sobre internet, y fabricantes de equipos y software.

Como miembros de GNI, Telefónica es una de las empresas firmantes de los principios del sector de las comunicaciones sobre libertad de expresión y privacidad y asume el compromiso de su implementación y rendición de cuentas mediante evaluaciones de cumplimiento por parte de asesores independientes.

Como parte de nuestro proceso de debida diligencia, cada cuatro años, llevamos a cabo una evaluación de impacto de cómo nuestras actividades (bien directamente o a través de nuestros socios comerciales) pueden estar afectando a los derechos fundamentales de las personas. Para ello, trabajamos con expertos internos y externos para identificar dónde y cómo nuestra actividad puede estar causando ese impacto y definimos un proceso formal que nos facilita la gestión proactiva de los riesgos

y el aprovechamiento de las oportunidades, implicando a nuestros principales grupos de interés.

En 2013, de la mano de *Business for Social Responsability* (BSR), realizamos nuestra primera evaluación de impacto en todas nuestras operaciones. La privacidad y la libertad de expresión fueron identificados como dos asuntos a gestionar dentro de la matriz y publicamos nuestro compromiso específico en derechos humanos.

En 2017 actualizamos nuestra matriz de impacto con una nueva evaluación de la mano de BHR (*Business & Human Rights*) con el objetivo de comprender los impactos potenciales derivados de nuestra estrategia, de las nuevas actividades del Grupo y de un entorno digital en constante cambio.

Los derechos de privacidad y libertad de expresión fueron identificados como relevantes en las siguientes actividades:

- Condiciones de productos y/o servicios.
- Nuevas tecnologías y desarrollos relacionados con la inteligencia artificial.
- Fusiones, adquisiones y alianzas estratégicas.

Una vez concluido el análisis, se identificaron varias actividades y temáticas que merecían una evaluación específica. Así, durante 2018 se empezó a trabajar en la evaluación del impacto de nuestra actividad con foco en: el proceso de despliegue de red, el desarrollo de nuevos productos y servicios –incluidos aquellos en los que se aplique la Inteligencia Artificial–, y en los derechos de niños, niñas y adolescentes. En estos dos últimos se identificaron como asuntos a evaluar la privacidad y la libertad de expresión.

En 2019 y como consecuencia de este proceso de debida diligencia, se actualizó nuestro compromiso explícito a través de la aprobación de nuestra Política Global de Derechos Humanos.

Políticas y procedimientos de aplicación

Hemos impulsado y revisado diferentes políticas y procedimientos para asegurar la protección de los derechos de privacidad y libertad de expresión:

» **Política Global de Derechos Humanos:** Aprobada en el 2019, esta política formaliza nuestro compromiso con los derechos humanos recogido, de forma general, en los Principios de Negocio Responsable de Telefónica, y de forma más específica, en un conjunto de políticas y normas que velan por el respeto y aplicación de derechos humanos sociales, económicos y culturales internacionalmente reconocidos.

» **Política de Privacidad:** Actualizada en el 2018, forma parte de la estrategia de Telefónica para diseñar una nueva experiencia digital basada en la confianza.

Consciente de la importancia de merecer la confianza de nuestros clientes y/o usuarios y, con carácter general, de nuestros grupos de interés, esta política les garantiza el control y el valor de sus datos personales cuando son objeto de tratamiento por Telefónica.

Establece unas normas de comportamiento común obligatorias para todas las entidades del grupo y establece un marco para una cultura de privacidad basada en los principios de licitud, transparencia, compromiso con los derechos de los interesados, seguridad y limitación del plazo de conservación.

» **Reglamento de Modelo de Gobierno de Protección de Datos:** Tiene por objetivo englobar los aspectos más importantes a tener en cuenta para una correcta gestión y protección de los datos de carácter personal.

Se establece un modelo organizativo y de relación donde el máximo responsable de la Función de Protección de Datos Personales es el Delegado de Protección de Datos (DPO), quien reporta directamente al Consejo de Administración de Telefónica, S.A. Además, se articula a través de una estructura de relacionamiento y gobierno:

› Oficina DPO: Se encarga de la coordinación de cumplimiento y datos (asegurar la ejecución global de cumplimiento de todo el Grupo) y una función técnica de protección de datos (la supervisión del cumplimiento de la normativa de protección de datos del Grupo Telefónica).

› Comité de Seguimiento: Cuenta con la representación de diferentes áreas de la compañía (Seguridad, Secretaría General, Regulación, Tecnología, CDO, Cumplimiento, Ética y Sostenibilidad y Auditoría Interna). Se revisa el estado general de cumplimiento del modelo de gobierno.

› Comités de Negocio: La Oficina DPO mantiene a través de la función técnica de protección de datos, interacciones permanentes con otras áreas, mediante los Responsables de Cumplimiento. El objetivo es asegurar la máxima uniformidad en la aplicación de los procesos comunes, y/o la identificación y tratamiento de problemáticas específicas de privacidad en el ámbito de actividad de cada área.

» **Reglamento de peticiones por parte de las Autoridades Competentes:** En 2019 se aprobó el reglamento para reforzar el procedimiento ya existente desde 2016, con el objetivo de alinearlo con otras políticas existentes y nuestro

compromiso con el respeto a los derechos y libertades fundamentales. Define los principios y directrices mínimas que deben ser contemplados en los procedimientos internos propios de cada una de las compañías del Grupo/unidades de negocio para cumplir con su deber de colaboración con las autoridades competentes de acuerdo con cada legislación nacional y con los derechos fundamentales de los interesados en este tipo de procedimientos.

Los principios que rigen el proceso son confidencialidad, exhaustividad, fundamentación, proporcionalidad, neutralidad política, respuesta diligente y seguridad.

Nuestro compromiso es asegurar la participación en el proceso de áreas legales o áreas similares con competencias legales en la recepción de las peticiones. Contamos con interlocutores fijos como ventanilla única en nuestra relación con las autoridades competentes, de manera que rechazamos cualquier petición que no viene por este conducto reglamentario.

» **Política Global de Seguridad:** Actualizada en el 2016, esta política se rige por los estándares y regulaciones nacionales e internacionales en la materia, y establece los principios rectores en materia de seguridad que resultan aplicables a todas las empresas que integran el Grupo Telefónica.

Las actividades de seguridad se rigen por los siguientes principios:

› **Legalidad:** Necesario cumplimiento de las leyes y regulaciones, nacionales e internacionales, en materia de seguridad.

› **Eficiencia:** Se destaca el carácter anticipativo y preventivo sobre cualquier potencial riesgo y/o amenaza con el objetivo de adelantarse y prevenir cualquier potencial efecto dañino y/o mitigar los perjuicios que pudieran causarse.

› **Corresponsabilidad:** El deber de los usuarios de preservar la seguridad de los activos que Telefónica pone a su disposición.

› **Cooperación y Coordinación:** Para alcanzar los niveles de eficiencia se prioriza la cooperación y la coordinación entre todas las unidades de negocio y empleados.

Fruto de esta política durante el 2017 y 2018 se actualizaron varias normativas de desarrollo para el efectivo cumplimiento de la misma. (Reglamento Gestión de Incidentes y Emergencias; Reglamento Análisis de Riesgos de Seguridad; Reglamento Seguridad en Redes y Comunicaciones; Reglamento de Ciberseguridad; Reglamento Seguridad en la Cadena de Suministro y el Reglamento Gobierno de la Seguridad entre otras).

» **Política de Comunicación Responsable:** Aprobado en octubre de 2018 tiene por objetivo establecer las pautas de actuación para Telefónica en torno a nuestros canales de comunicación y generación de contenidos. Se basa en los principios de legalidad, integridad y transparencia, neutralidad y protección de menores. En el principio de neutralidad nos comprometemos a evitar posicionarnos políticamente como compañía y promovemos el derecho a la libertad de expresión, dentro de los marcos regulatorios a los que estamos sometidos.

» **Principios de Inteligencia Artificial:** Aprobados por el Comité Ejecutivo en octubre de 2018, nos comprometemos a diseñar, desarrollar y usar la Inteligencia Artificial con integridad y transparencia. Son principios que sitúan a las personas en el centro y garantizan el respeto de los derechos humanos en cualquier entorno y proceso en el que se use la Inteligencia Artificial: hacen hincapié en la igualdad e imparcialidad, la transparencia, la claridad, la privacidad y la seguridad. Son normas que aplican en todos los mercados en los que operamos y se extienden a toda nuestra cadena de valor, a través de socios y proveedores.

» **Riesgo básico de Derechos Humanos:** Los riesgos relacionados con impactos en DD.HH. siempre han estado presentes en el modelo de levantamiento de riesgos de Telefónica, sin embargo, en el 2017 se incluyó de forma específica el riesgo básico de DD.HH.

El objetivo es levantar cualquier riesgo de impacto, directo o indirecto, en las operaciones del Grupo Telefónica debido a posibles vulneraciones de derechos humanos, como consecuencia de la propia actividad de la Compañía o de la actividad que llevan a cabo nuestros proveedores u otras relaciones comerciales. Este análisis contempla cualquier cambio legislativo o de actividad que pueda tener un impacto en los derechos humanos.

Este levantamiento de riesgos facilita definir las pautas de actuación necesarias en las operaciones directamente afectadas con el objetivo de mitigar y/o evitar estos riesgos y priorizar las actuaciones de Auditoría Interna, de cara a su planificación de actividades de supervisión de las estructuras de control interno.

» **Evaluación de Riesgos en la Reputación e impacto en los Derechos Humanos en los nuevos Productos y Servicios del Grupo Telefónica:** El objetivo es evaluar el posible impacto en la creación y comercialización de los productos y servicios del Grupo Telefónica, tanto para particulares (B2C), como para clientes (B2B) e indirectamente (B2B2C). Entre las cuestiones evaluadas se incluyen privacidad y libertad de expresión, tanto en el diseño como en la comercialización.

» **Canal de Negocio Responsable**

Más información, en la web:
www.telefonica.com/es/web/about_telefonica/canal-de-negocio-responsable

Creado a finales de 2016 y vinculado directamente a los Principios de Negocio Responsable y nuestra Política de Derechos Humanos. Tiene por objetivo ser un canal de comunicación donde cualquier grupo de interés puede plantear quejas o consultas relativas a nuestro impacto en la Privacidad y Libertad de Expresión a través del formulario publicado en nuestra web.

Contamos con un procedimiento que garantiza el adecuado funcionamiento del Canal.

Más información, en la web: www.telefonica.com/documents/153952/141150866/Canal_Negocio_Responsable_Proceso_Recepcion_Tramitacion_Comunicaciones.pdf

Alcance del informe

Tal y como ocurre en otras empresas de nuestro sector, en Telefónica recibimos peticiones de información referidas a las comunicaciones de nuestros clientes o usuarios, solicitudes de bloqueo de acceso a ciertos sitios o contenido o de filtrado de contenidos, o solicitudes con el objetivo de suspender temporalmente el servicio en determinadas zonas (por ejemplo, en caso de disturbios o de orden público), cursadas por los cuerpos y fuerzas de seguridad del Estado, organismos gubernamentales y/o juzgados según la legislación de cada país.

El informe muestra:

- **Los compromisos, políticas y procesos** que seguimos cuando respondemos a las peticiones de las Autoridades Competentes.
- **La información sobre el contexto legal** que da potestad legal a las autoridades para hacer este tipo de solicitudes. El marco legal específico de cada país señala también limitaciones de cara a facilitar la información sobre las peticiones que Telefónica recibe, por lo que en el informe se señalan ese tipo de limitaciones a la información que se aporta. Cuando no aportamos datos, explicamos por qué no los aportamos.
- **Las Autoridades que tienen potestad** según la legislación local para cada uno de los indicadores que reportamos.
- **El número total de peticiones** que recibimos durante el último año en cada uno de nuestros países de operación, a menos que se nos prohíba hacerlo o a menos que un gobierno u otra entidad pública ya revele dicha información.

Además, y cuando técnicamente es posible, reportamos el número de **peticiones que rechazamos y los accesos** que son afectados por cada indicador.

Indicadores de este informe

En los apartados siguientes reportamos el número de peticiones que recibimos por parte de las autoridades nacionales competentes en los países donde operamos. No hemos incluido Guatemala, Nicaragua y Panamá, ya que a fecha de publicación de este informe estaba finalizado el proceso de desinversión.

Cualquier petición que se pueda recibir por parte de una autoridad no nacional debe cumplir con los procesos judiciales y/o legales que corresponda a cada país. En Telefónica solo atendemos solicitudes que provengan de una autoridad nacional competente siguiendo nuestro Manual de peticiones por parte de las autoridades competentes. En Telefónica no atendemos solicitudes privadas, solo se tramitan las peticiones que provienen de autoridades determinadas por ley.

Más información, en el apartado **"Glosario"**.

Los indicadores que reportamos son:

- **Interceptación legal:** Aquellas solicitudes que proceden de las autoridades competentes en el marco de investigaciones criminales y, en su caso, civiles con el objetivo de interceptar comunicaciones o acceder a datos de tráfico en tiempo real. Se incluyen intervenciones nuevas, prórrogas y cese.

- **Metadatos asociados a las comunicaciones:** Aquellas solicitudes procedentes de las autoridades competentes que tienen por objetivo obtener datos históricos referidos a:

  - El nombre y dirección del usuario registrado (datos de abonado).
  - Los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet).
  - La fecha, hora y duración de una comunicación.
  - El tipo de comunicación.
  - La identidad de los equipos de comunicación (incluyendo IMSI o IMEI).
  - La localización del usuario o del dispositivo.

- **Bloqueo y restricción de contenidos:** Aquellas solicitudes de las autoridades competentes para bloquear el acceso a sitios web específicos o a un determinado contenido. Se trata de solicitudes para bloquear el acceso a un sitio web o a un contenido, no una petición para eliminar el contenido del usuario. A título de ejemplo, las demandas de bloqueo se emiten porque los sitios web o determinados contenidos que publican son contrarios a las leyes locales (suelen estar relacionados con material de abuso sexual infantil, los juegos de azar online, violación de derechos de autor, difamación, venta ilegal de medicamentos, armas, marca comercial, etc.).

- **Suspensiones geográficas o temporales de servicio:** Aquellas solicitudes por petición de las autoridades competentes para limitar temporal y/o geográficamente la prestación de un servicio. Estas peticiones suelen estar relacionados con situaciones de fuerza o causa mayor como catástrofes naturales, actos de terrorismo, etc.

Además, para cada indicador reportamos también los siguientes subindicadores:

- **Peticiones rechazadas** o atendidas parcialmente: número de veces que hemos rechazado una petición o que solo hemos proporcionado información parcial o ninguna información en respuesta a una petición por alguna de las siguientes razones:

- Por no ajustarse a la legislación local para ese tipo de petición.
- Por no contener todos los elementos necesarios que posibilita la ejecución (firmas necesarias, autoridad competente, descripción técnica de las peticiones, etc.).
- Porque técnicamente es imposible ejecutar la petición.

» **Número de accesos afectados:** número de accesos que se ven afectados por cada petición. Así, pueden ocurrir los siguientes escenarios:

- Que una petición afecte a un solo acceso.
- Que una misma petición afecte a varios accesos (por ejemplo, en acceso a metadatos una petición puede solicitar datos de varios teléfonos móviles o fija).
- Que varias peticiones afecten a un mismo acceso (por ejemplo, en acceso a metadatos pueden solicitarse a lo largo de periodo de reporte varias peticiones para un mismo acceso de móvil o fija).

Por lo tanto, existen casos en este informe en los que el número de peticiones supera al número de accesos afectados y viceversa.

Para bloqueo de contenidos, el bloqueo de una web/url afecta a todos los usuarios que quieran acceder a su contenido. En tal caso, no se puede medir el número de accesos afectados. Sin embargo reportamos número de URLs afectadas.

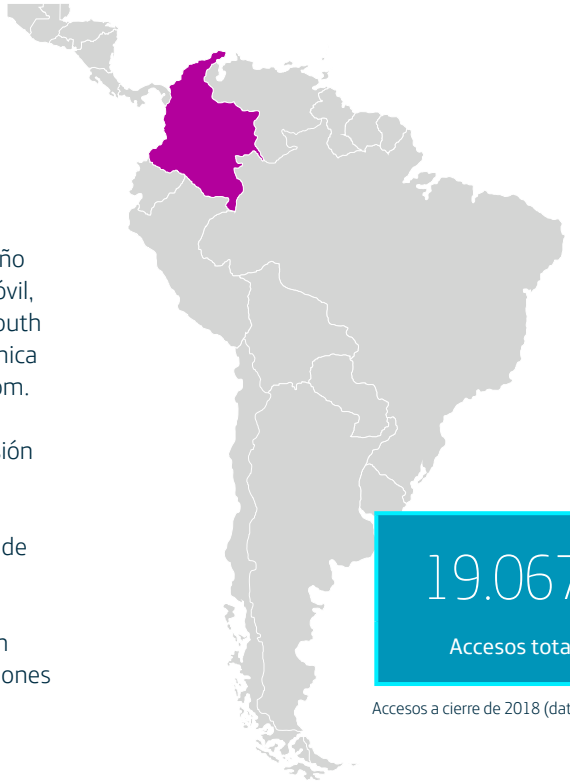
Por otra parte, en este Informe de Transparencia, nuestro objetivo es informar de forma transparente sobre nuestros esfuerzos en relación con las peticiones o demandas con potencial impacto relevante sobre el derecho a la libertad de expresión en las telecomunicaciones. Identificamos dicha solicitud y demandas como "*major events*".

Más información, en el apartado **"Glosario"**.

A este respecto, debemos destacar la situación de excepcionalidad en la que se encuentra Venezuela y los retos a los que nos enfrentamos para la verificación de nuestros procesos globales en el país. En esta situación, Telefónica debe priorizar el cumplimiento con la legislación vigente, el mantenimiento de la conectividad en el país y el bienestar de nuestros empleados.

Colombia

www.telefonica.co



Telefónica tiene presencia en Colombia desde el año 2004. Comenzó con actividades en el mercado móvil, tras la adquisición de la operación celular de Bellsouth en el país. Posteriormente, en el año 2006, Telefónica adquirió el control y la gestión de Colombia Telecom. Telefónica proporciona hoy en el país servicios de telecomunicaciones de voz, banda ancha y televisión de pago.

Telefónica Colombia gestiona mas de 19 millones de accesos a diciembre de 2018.

Los ingresos de Telefónica en Colombia alcanzaron 1.468 millones de euros y el OIBDA sumó 556 millones de euros a cierre de 2018.

19.067,8
Accesos totales

Accesos a cierre de 2018 (datos en miles).

Accesos

1.582,4	15.716,3	1.220,4	548,2
Telefonía fija	Telefonía móvil	Datos e Internet	TV de pago

Accesos a cierre de 2018 (datos en miles).

Interceptación legal

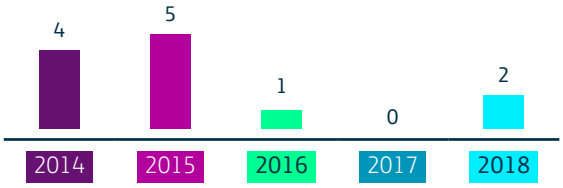
Contexto legal

- Constitución Colombiana: Artículo 15 y Artículo 250.
- Ley 906. Código Procedimiento Criminal de 200, Art. 235. Modificado por el artículo 52 de la Ley 1453 de 2011.
- Ley 1621 de 2013, Artículo 44.
- Decreto 1704 de 2012, Artículo 1-8.
- Decreto 2044 de 2013, Artículo 3.

Autoridades competentes

- Fiscalía General de la Nación.
- A través del grupo de Policía Judicial designado para la investigación del caso.

PETICIONES*



* Petición sobre líneas fijas.

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

Accesos afectados	2	Peticiones rechazadas	0

Metadatos asociados a las comunicaciones

Contexto legal

- Constitución Colombiana: Artículo 250.
- Ley 906 de 2004, Art. 235.
- Ley 1621 de 2013, Art. 44.
- Decreto 1704 de 2012, Art. 1-8.

Autoridades Competentes

- Autoridades con funciones de Policía Judicial y pueden ser de orden permanente o transitorio:

  El artículo 312 del nuevo código de Procedimiento Penal, define que las entidades que poseen facultades permanentes de Policía Judicial son las siguientes:

  - Fiscalía General de la Nación y todos sus servidores públicos que desempeñen funciones judiciales (Art. 249 CN y Art. 112, 113 CPP).
  - Policía Judicial: C.T.I., Policía Nacional y D.A.S., facultados por comisión de autoridad judicial competente y por mandato legal (Art. 311 a 320 CPP).
  - Grupos de Acción Unificado "Antisecuestro y Extorsión" (Ley 282 de 1996).

  Ejercen funciones especiales de Policía Judicial, en asuntos de su competencia:

  - Contraloría General de la Nación (Art. 267 CN y Art. 312 CPP).
  - Procuraduría General de la Nación (Art. 275 CN y Art. 312 CPP).
  - Dirección Nacional de Impuestos y Aduanas Nacionales - DIAN (ver numeral 2, Capitulo II).
  - Entidades públicas que ejerzan funciones de vigilancia y control.(1)
  - Los alcaldes e inspectores de policía, en los lugares del territorio donde no hubiere miembros de la Policía Judicial de la Policía Nacional.
  - Directores Nacional y regional del INPEC, los directores de los establecimientos de reclusión y el personal de custodia y vigilancia, conforme a lo señalado en el Código Penitenciario y Carcelario.
  - Inspecciones de Policía (Art. 312 CPP).

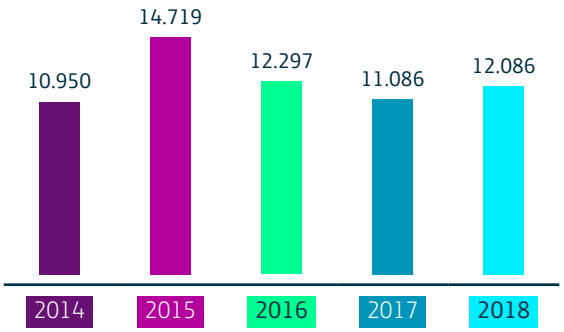
  Para investigaciones de índole disciplinarias (la **Ley 734 de 2002 código único Disciplinario**) están

Metadatos asociados a las comunicaciones *(cont.)*

facultados las oficinas de control disciplinario interno.

- Policías con autorización del Ministerio Público y orden de investigar.
- Juez del Sumario en Procedimiento Penal Inquisitivo (Código Procedimiento Penal).
- Agencias de Inteligencia de Estado con autorización judicial previa.

PETICIONES



Accesos afectados	36.204	Peticiones rechazadas	120

Bloqueo y restricción de contenidos

Material de abuso sexual infantil

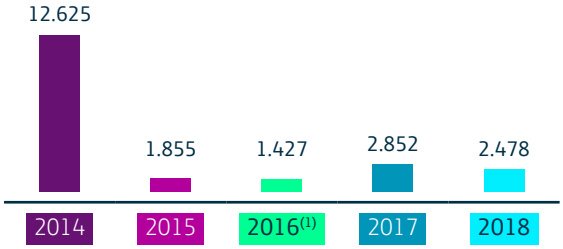
Contexto legal

- Ley 679 de 2001: Artículos 7 y 8.
- Decreto 1524 de 2002: Artículos 5 y 6.
- Ley 1450 de 2011: Artículo 56.
- Resolución CRC 3502 de 2011.

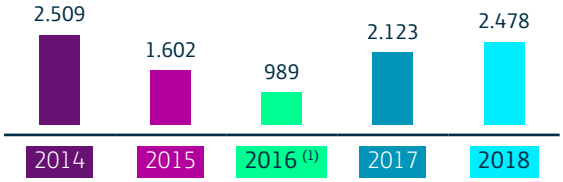
Autoridades Competentes:

- La Policía Nacional le envía al Ministerio de las Tecnologías de la Información y las Comunicaciones un listado de URLs con orden de bloqueo para que el Ministerio lo publique en su página web y pueda ser consultado por los PSI. Para acceder a este listado, los PSI deben contar con un usuario y una contraseña que es suministrada previamente por el Ministerio, para evitar que cualquier persona pueda consultar los URLs que tienen orden de bloqueo por contener material de pornografía infantil.

Nº URLS NUEVAS*



Nº URLS INCREMENTALES**



* Número de URLs agregados al listado publicado por MinTIC durante ese año.

** Número de URLs que se incrementaron con respecto al año. Este dato excluye a su vez las URLs que se eliminaron del listado durante ese año.

(1) Desde septiembre de 2016 entró en operación la plataforma "WOLF Control de Contenidos", la cual filtra de manera especializada todo el contenido ilegal tipificado por las autoridades locales como pornografia infantil.

El listado se continua actualizando y publicando de manera periódica por medio de la página web del Ministerio de las Tecnologías de la Información y las Comunicaciones.

URLs afectadas	2.478	Peticiones rechazadas	0

Juegos Ilegales

Contexto legal

- Ley 1753 de 2015, Artículo 93, párrafo 3.
- Ley 1450 de 2011, Artículo 56.
- Resolución CRC 3502 de 2011.

Autoridades Competentes

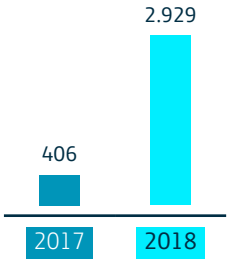
- Coljuegos, empresa industrial y comercial del Estado encargada de la administración del monopolio

Bloqueo y restricción de contenidos *(cont.)*

Juegos Ilegales *(cont.)*

rentístico de los juegos de suerte y azar, en conjunto con la Policía Nacional, identifican portales web en los que se comercializan juegos de suerte y azar no autorizados y le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI el listado de las URLs que deben bloquear.

Nº URLS



Orden judicial

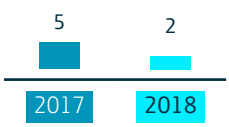
Contexto legal

- Ley 1273 de 2009, Artículo 269F.
- Ley 1340 de 2009, Artículo 18.
- Ley 1450 de 2011, Artículo 56.
- Resolución CRC 3502 de 2011.

Autoridades Competentes:

- La Fiscalía General de la Nación y la Superintendencia de Industria y Comercio dentro de las investigaciones que adelantan le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI las URLs que deben bloquear.

Nº URLS



URLs afectadas	2.931	Peticiones rechazadas	N/D[1]

(1) Por el sistema de bloqueo establecido por ley.

Suspensiones geográficas o temporales de servicio

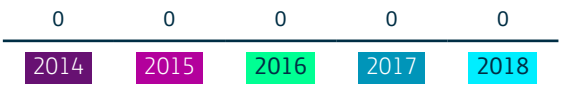
Contexto legal

- Ley 1341 de 2009, Art. 8. Casos de emergencia, conmoción o calamidad y prevención.

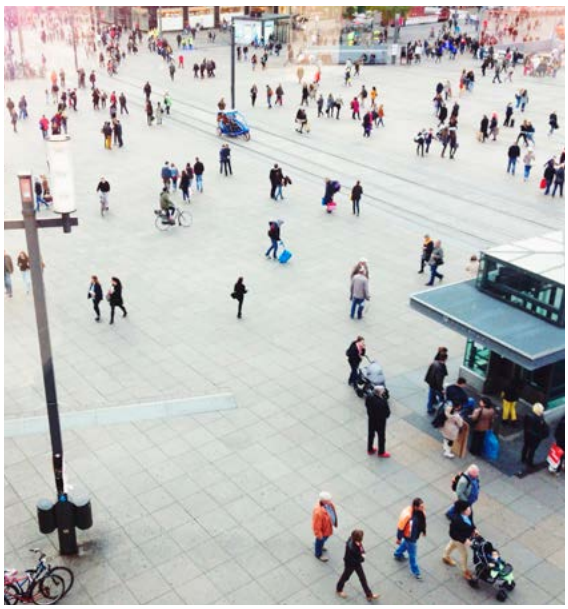
Autoridades Competentes

- Se darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.

PETICIONES



Accesos afectados	0	Peticiones rechazadas	0



Glosario

Autoridad competente
Datos personales
Datos de localización
Datos de tráfico
DPI
IMEI
IMSI
IOCCO
MAJOR EVENTS
PSI
SUTEL
TELCOR
URL

Glosario

CONCEPTO	EXPLICACIÓN
AUTORIDAD COMPETENTE	Jueces y Tribunales, Fuerzas y Cuerpos de Seguridad del Estado y demás administraciones u organismos gubernamentales a los que la ley faculta para realizar las peticiones objeto de este informe. Las Autoridades Competentes podrán variar en función del tipo de petición y de la legislación aplicable en cada uno de los países.
DATOS PERSONALES	Se entiende por datos personales cualquier información que se refiera a alguna persona identificada o identificable, como puede ser su nombre, domicilio, destinatarios de sus comunicaciones, localización, contenido de las comunicaciones, datos de tráfico (días, hora, destinatarios de las comunicaciones, etc.).
DATOS DE LOCALIZACIÓN	Los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de Red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada.
DATOS DE TRÁFICO	Cualquier dato tratado a efectos de la conducción de una comunicación a través de una Red de comunicaciones electrónicas o a efectos de su facturación.
DPI	Son las siglas en inglés de *Deep Packet Inspection* o inspección profunda de paquetes. DPI identifica situaciones de falta de cumplimiento de protocolos técnicos, virus, *spam*, o invasiones, aunque también puede usar criterios predefinidos diferentes a los anotados para decidir si algún paquete puede o no pasar, o requiere ser enrutado a un destino distinto, darle otra prioridad o asignación de ancho de banda, para tomar información con propósitos estadísticos o simplemente para eliminarlo.
IMEI	Son las siglas en inglés de *International Mobile Station Equipment Identity* o identidad internacional del equipamiento móvil. Se trata de un número de serie que identifica al terminal físicamente. El IMEI le sirve al operador para identificar terminales válidos y que, por tanto, pueden conectarse a la Red.
IMSI	Son las siglas en inglés de *International Mobile Subscriber Identity* o identidad internacional de abonado móvil. Es el identificador de la línea o servicio. Este número sirve para enrutar las llamadas y se puede obtener el país o la Red a la que pertenece.
IOCCO	Son las siglas en Inglés de *Interception of Communications Commissioner's Office* en Reino Unido. Es responsable de mantener bajo revisión la interceptación de comunicaciones, la adquisición y divulgación de datos de comunicaciones por agencias de inteligencia, fuerzas policiales y otras autoridades públicas. Presentan informes semestrales al Primer Ministro con respecto a la ejecución de las funciones del Comisionado de Interceptación de Comunicaciones.

CONCEPTO	EXPLICACIÓN
MAJOR EVENTS	Existen ciertas situaciones de fuerza mayor que pueden provocar las siguientes actuaciones: **1. Restricción o denegación del servicio.** (Incluyendo SMS, voz, correo electrónico, correo de voz, Internet u otros servicios) que supone limitar la libertad de expresión. Ejemplos: » Restricción o denegación del servicio a nivel nacional. » Restricción o denegación de acceso a un sitio web(s) por motivos políticos (por ejemplo, páginas de Facebook; web de noticias –Ej. bbc.co.uk–; sitios web del partido de la oposición en el período previo a las elecciones; sitios web de grupos de derechos humanos, etc.). » Desconexión específica de cualquier servicio de telecomunicaciones por motivos políticos. (Ej. en uno o un pequeño número de celdas). » Denegación de acceso a redes o a determinados servicios a ciertos clientes con el objetivo de limitar la libertad de expresión legítima de ese individuo. **2. Apagado de Red/control de acceso.** Ejemplos: » El cierre de toda la red a nivel nacional. » Control de acceso a la red en un área específica o en una región por motivos políticos. **3. La interceptación sin fundamento legal.** Situaciones en las que las autoridades interceptan comunicaciones sin tener una base legal por causas de fuerza mayor. **4. Comunicaciones impuestas por las autoridades.** Ejemplo: » Envío de mensajes/comunicaciones a nuestros clientes en nombre de un gobierno o agencia gubernamental por motivos políticos. **5. Cambios operacionales significativos.** Ejemplos: » Cambios, o propuestas de cambios, significativos operativos y técnicos respecto a los servicios de vigilancia (acceso a los datos, retención de datos e interceptación), que tienen como objetivo reducir el control por parte del operador para supervisar este tipo de actividades. (Ej. un cambio en el proceso para permitir el acceso directo por una agencia gubernamental/gobierno). » Un cambio en el proceso para establecer vigilancia masiva. **6. Cambios legales significativos.** (Ej. cambios significativos –o propuestas de cambios– de leyes que dan a las autoridades gubernamentales más poder para hacer peticiones a los operadores). Ejemplo: » Cambios en las leyes de interceptación de comunicación.
PSI	El Portal de Servicio Interno "PSI" es una aplicación de consulta, permite que los integrantes de la Policía Nacional de Colombia, como clientes internos de la organización, encuentren en un sitio web toda la información para trámites internos, con altos niveles de seguridad.
SUTEL	La SUTEL es un órgano de desconcentración máxima de Costa Rica, adscrito a la Autoridad Reguladora de los Servicios Públicos (Aresep); creada mediante la Ley 8.660, publicada el 13 de agosto de 2008. A la SUTEL le corresponde la aplicación de la regulación al sector de telecomunicaciones y asegurar la eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura e información, así como mejores alternativas en la prestación de los servicios de telecomunicaciones.
TELCOR	El Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR) es el "Ente Regulador" de los Servicios de Telecomunicaciones y Servicios Postales, una institución estatal, la cual tiene como funciones la normación, regulación, planificación técnica, supervisión, aplicación y el control del cumplimiento de las Leyes y Normas que rigen la instalación, interconexión, operación y prestación de los Servicios de Telecomunicaciones y Servicios Postales.
URL	Son las siglas en inglés de *Uniform Resource Locato*r (en español, localizador uniforme de recursos), que sirve para nombrar recursos en Internet. Esta denominación tiene un formato estándar y su propósito es asignar una dirección única a cada uno de los recursos disponibles en Internet, como por ejemplo páginas, imágenes, vídeos, etc.


Telefonica