Telefónica

Informe de **Transparencia** en las Comunicaciones **2020**

ÍNDICE

Introducción y alcance del Informe

En nuestro compromiso con los derechos fundamentales de privacidad y libertad de expresión, publicamos el quinto Informe de Transparencia de las telecomunicaciones, 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, la Inteligencia Artificial y el protagonismo de los datos a escala global.

Tal y como ocurre en otras empresas de nuestro sector, en Telefónica recibimos solicitudes (ver definición en glosario) de información referidas a las comunicaciones de nuestros clientes o usuarios, solicitudes de bloqueo de acceso a ciertos sitios o contenidos o de filtrado de contenidos, o solicitudes con el objetivo de suspender temporalmente el servicio en determinadas zonas o determinadas cuentas. Dichas solicitudes están cursadas por los cuerpos y fuerzas de seguridad del Estado, organismos gubernamentales y/o juzgados, (en adelante: Autoridades Competentes, ver definición en glosario).

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.

En este ejercicio de transparencia, nuestro informe muestra:

i. nuestra gobernanza en derechos humanos y específicamente en la privacidad y libertad de expresión;

ii. nuestra debida diligencia en los derechos humanos;

iii. los compromisos, políticas y procesos que seguimos cuando respondemos a las solicitudes de las Autoridades Competentes;

iv. la información sobre el contexto legal que da potestad legal a las autoridades para hacer este tipo de solicitudes[1];

v. las autoridades que tienen potestad según la legislación local para cada uno de los indicadores que reportamos;

vi. el número total de solicitudes 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;

vii. y además, y cuando técnicamente es posible, reportamos el número de solicitudes que rechazamos, los accesos que son afectados por cada indicador y las url´s y/o IPs afectadas en el caso de bloqueo y restricción de contenidos.

1 El marco legal específico de cada país señala también limitaciones de cara a facilitar la información sobre los requerimientos 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.

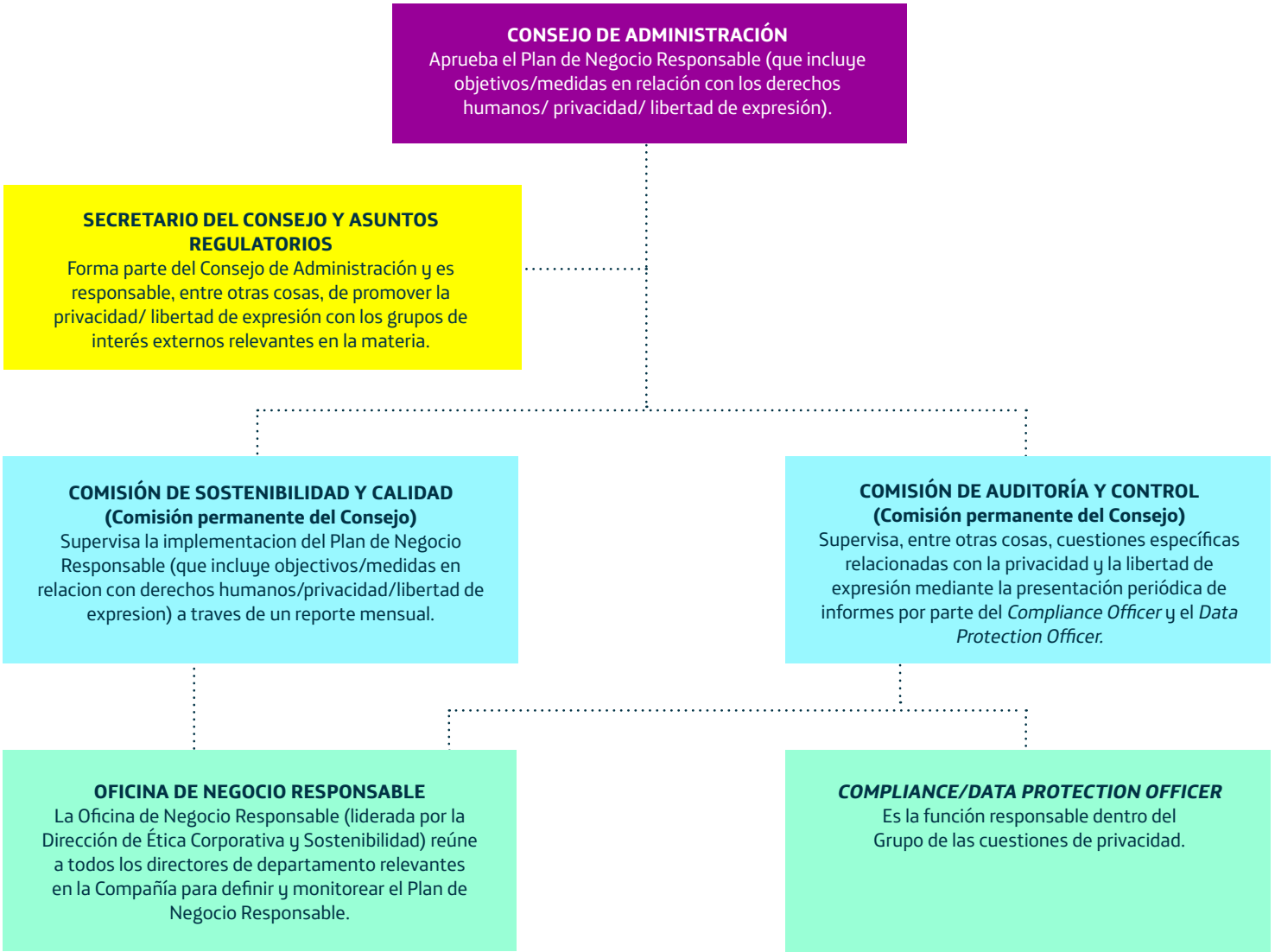
Nuestra gobernanza

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.

Nuestras actividades en materia de derechos humanos se definen e implementan a través del Plan de Negocio Responsable, que establece la estrategia y los objetivos de sostenibilidad de la empresa, y que es aprobado y supervisado por el Consejo de Administración y el Comité de Sostenibilidad y Calidad (uno de los comités permanentes).

Nuestra Política de Derechos y Humanos y nuestra debida diligencia que se basan, entre otras cosas, en los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas y los principios de la Global Network Initiative (GNI), forman parte integral del Plan de Negocio Responsable.

Este modelo de gobernanza, encabezado por el Consejo de Administración y la Oficina de Negocio Responsable en la que participan todos los departamentos pertinentes, tiene como objetivo garantizar que nuestro compromiso con los derechos humanos se incorpore a todas las actividades y niveles de la empresa.



Asimismo, 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.

Para los asuntos de Privacidad y Libertad de Expresión relacionados con los requerimientos de las autoridades contamos con el Comité de Transparencia integrado por los responsables de las áreas globales de Secretaría General, Cumplimiento, Auditoría Interna y Ética Corporativa y Sostenibilidad, quienes analizan los datos reportados de este informe, y pueden realizar las observaciones que consideren pertinentes, con carácter general o específicamente en relación con la información facilitada por las operadoras, con el objetivo de 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 solicitudes que por sus características y excepcionalidad así lo requieren, son analizadas por los máximos responsables de cada área responsable, mediante la adecuada ponderación de todos los intereses potencialmente comprometidos, incluidos 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.

En caso de crisis, se sigue un procedimiento establecido en el Sistema Global de Gestión de Crisis, en cuya taxonomía de incidentes críticos que pueden dar lugar a una crisis se enumeran las solicitudes de las autoridades que tienen un impacto en la libertad de expresión y la privacidad, así como "legislaciones con un posible alto impacto negativo en los derechos humanos (libertad de expresión, etc.)". El Sistema Global de Gestión de Crisis prevé que, en caso de una crisis relacionada con la cuestiones de libertad de expresión, el Presidente del Comité de Crisis puede convocar la denominada "Mesa Redonda de Derechos Humanos" (integrada por los departamentos pertinentes) para analizar la situación y diseñar y aplicar una estrategia de respuesta, informar al Comité Ejecutivo y realizar un análisis posterior con el fin de evitar un riesgo en el futuro.

Nuestra debida diligencia en derechos humanos

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.

De acuerdo con nuestra Política Global de Derechos Humanos contamos con una debida diligencia para identificar, prevenir, mitigar y remediar los impactos (potenciales y reales) en los derechos humanos. Una parte integral de nuestra debida diligencia son las evaluaciones de impacto, que se llevan a cabo cada cuatro/cinco años a nivel global con la ayuda de expertos externos en derechos humanos y en estrecha consulta con nuestros grupos de interés. El objetivo de estas evaluaciones de impacto es averiguar cómo nuestras actividades/relaciones comerciales y productos/servicios impactan en los derechos humanos existentes (ver asuntos de derechos humanos analizados en evaluaciones en impacto en gráfica) y, sobre esta base, identificar los asuntos de derechos humanos más relevantes para nuestra actividad empresarial. Se llevan a cabo evaluaciones adicionales y específicas sobre cual-

Foco: Privacidad y Libertad de Expresión dentro de la Debida Diligencia en Derechos Humanos

quier tema relevante en el que en la evaluación de impacto se haya detectado especial preocupación. Además, se llevan a cabo evaluaciones de impacto locales en los países en los que operamos para integrar el contexto local en la evaluación general. Además, contamos con un mecanismo de reclamación y remedio, nuestro Canal de Negocio Responsable, que permite a los grupos de interés, de forma confidencial y anónima, plantear quejas o consultas (en varios idiomas) sobre cualquier aspecto relacionado con los Principios de Negocio Responsable, explícitamente también sobre derechos humanos en general y privacidad y/o libertad de expresión en particular. Contamos con un procedimiento que garantiza el adecuado funcionamiento del Canal.

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 2019 actualizamos nuestra matriz de impacto con una nueva evaluación de la mano de *Business & Human Rights* (BHR) 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 otra vez identificados como relevantes (ver nuestra web sobre derechos humanos para obtener más información sobre la última evaluación de impacto a nivel global). Una vez concluido el análisis, se identificaron varias actividades y temáticas que merecían una evaluación específica como han sido la evaluación de impacto en el proceso de despliegue de red, en 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.

El conjunto de todo este proceso en torno a las evaluaciones de impacto forma la base para adaptar nuestras políticas/ procesos internos con vistas a prevenir, mitigar y/o remediar los posibles impactos sobre los derechos humanos en general y sobre la privacidad y libertad de expresión en particular. A continuación, destacamos las políticas/ procesos internos más importantes en materia de privacidad y libertad de expresión que se han adaptado a raíz de las ultimas evaluaciones de impacto.

Políticas y procesos de aplicación

Hemos impulsado y revisado diferentes políticas y procedimientos para asegurar la protección de los derechos de privacidad y libertad de expresión, el acceso a la información y la no-discriminación.

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 (Confianza Digital).

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 sobre 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.

Bajo el principio de transparencia garantizamos que a los interesados se les facilite de forma accesible e inteligible información sobre los datos personales que recogemos (tales como, a título de ejemplo, nombre, apellidos, dirección, cuenta bancaria, preferencias personales etc..), cómo los recogemos, la finalidad (prestación del servicio, etc..).

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:** Encargada 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 encargada de 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, a través de los Responsables de Cumplimiento, al objeto de 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 ante Peticiones por parte de las Autoridades Competentes:
En el 2019 se aprobó el Reglamento para reforzar el procedimiento ya existente desde 2016, con el objetivo de alinearlo con otras Políticas existentes y nuestros compromiso por 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/OB 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 solicitudes. Contamos con interlocutores fijos como ventanilla única en nuestra relación con las Autoridades Competentes, de manera que rechazamos cualquier solicitud que no viene por este conducto reglamentario.

Política Global de Seguridad:

Actualizada en el 2019 e inspirada en los principios de 'honestidad y confianza', 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 2019 -2020 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:

Aprobada en octubre del 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. En nuestra comunicación hacia clientes y a través de la publicidad prohibimos ciertas conductas que van en contra de nuestros Principios de Negocio Responsable. Así, en nuestros mensajes y nuestros patrocinios no toleramos que se abuse de la buena fe del consumidor, que atenten contra la dignidad de las personas, que fomenten el consumo del alcohol, el tabaco, las drogas, los trastornos alimenticios o el terrorismo, que inciten al odio, a la violencia o a la discriminación, a la comisión de comportamientos ilegales y puedan abusar de la ingenuidad del menor.

Principios de Inteligencia Artificial:

Aprobados por el Comité Ejecutivo en octubre del 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: 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.

Durante el 2019, hemos estado trabajando en la implementación de estos principios en todas nuestras operaciones, centrándonos en tres pilares interrelacionados:

- **Formación para empleados:** contamos con un curso de formación sobre Ética e Inteligencia Artificial para nuestros empleados, explicando a) cómo la Inteligencia Artificial, si se utiliza de forma inapropiada, puede tener un impacto negativo en los derechos humanos y b) qué pasos se deben tomar en la práctica para hacer frente a los posibles riesgos en materia de derechos humanos asociados con el uso de la Inteligencia Artificial.
- **Cuestionario de autoevaluación** para los jefes de producto que compran, desarrollan y/o usan Inteligencia Artificial. Así,para cada uno de los principios se elaboran preguntas relacionadas con los algoritmos utilizados y pueden identificar los riesgos asociados a los principios y las recomendaciones para prevenirlos o evitar esos riesgos.
- **Gobernanza:** Contamos con un modelo de gobernanza para la implementación efectiva de los Principios

Formación en derechos humanos:

A finales del 2019 empezamos a trabajar a nivel global la formación en derechos humanos. Así, profundizamos durante el 2020 y habrá una sección más ampliada sobre derechos humanos dentro del curso obligatorio de los Principios de Negocio Responsable y talleres específicos para empleados cuyo trabajo puede tener un impacto mayor en los derechos humanos. Las áreas a las que se impartirán estos talleres serán:

- **Jurídica y Cumplimiento:** Para los asuntos de Privacidad y Libertad de Expresión desde una perspectiva de derechos humanos, haciendo hincapié en los principios del GNI y de los requerimientos de las Autoridades Competentes y sobre los derechos humanos a tener en cuenta en los acuerdos de fusión, adquisición y desinversión.
- **Asuntos Públicos y Relaciones Institucionales:** Para promover la privacidad y la libertad de expresión a través de un *advocacy* proactivo con los grupos de interés externos (por ejemplo gobiernos, organizaciones internacionales, ONGs).
- **Gestores de producto y desarrolladores:** Para la integración de los derechos humanos desde el diseño y haciendo foco en los productos y servicios que incorporan nuevas tecnologías o Inteligencia Artificial.

Riesgo básico de derechos humanos:

Los riesgos relacionados con impactos en derechos humanos 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 derechos humanos.

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 en los países 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.

Derechos humanos por diseño:

Evaluamos los posibles impactos en los derechos humanos de nuevos productos y servicios a través del enfoque 'derechos humanos desde el diseño', es decir, desde el inicio del diseño y/o comercialización de productos y servicios. Concretamente, los jefes de producto deben llevar a cabo una autoevaluación de nuevos productos y servicios a través de una herramienta en línea en la fase de diseño con el fin de identificar y abordar los posibles impactos en los derechos humanos ya en la fase de diseño. Los derechos humanos abordados en este cuestionario son, por ejemplo, privacidad, libertad de expresión, no- discriminación, Inteligencia Artificial, impacto en grupos vulnerables como los menores, etcétera. Si se identifican riesgos en materia de derechos humanos una vez finalizada la autoevaluación, el producto/servicio en cuestión se somete a un análisis más detallado con la ayuda de expertos en derechos humanos de la empresa, a fin de abordar los posibles efectos adversos sobre los derechos humanos en el desarrollo del producto/servicio en el futuro.

Iniciativas de Transparencia:

Uno de los retos y elementos clave en la privacidad es garantizar la transparencia y en Telefónica hemos apostado por llevarlo a la práctica incluyéndolo como uno de los Principios de la Política Global de Privacidad y desarrollando diferentes iniciativas que implementan este Principio como son, como son el Centro de Privacidad Global y los Centros de Privacidad de las operadoras. Además, Telefónica comienza a disponibilizar a clientes el acceso a los datos que generan durante el uso de nuestros servicios, datos que son recogidos en el denominado "Personal Data Space". Durante el 2020 se lanzará el Centro de Transparencia en España, que hace realidad la consulta y gestión de los datos recogidos en el Personal Data Space. A través de la sección "Permisos" los clientes pueden gestionar sus consentimientos sobre el uso de datos para determinados propósitos. Y desde la sección de "Consulta y Descarga" se ofrecen útiles visualizaciones de diferentes tipos de datos, con una experiencia amigable y respetando los criterios de privacidad, con la opción de descargar un documento con mayor nivel de detalle de esos conjuntos de datos.

La experiencia del Centro de Transparencia se ha diseñado centrada en el usuario, evitando emplear un lenguaje legal complejo, donde Aura, la Inteligencia Artificial de Telefónica, acompaña y aporta en cada visualización una explicación sobre el propósito y la naturaleza de esos datos dentro de Telefónica, ofreciendo claridad, transparencia, y reforzando la confianza.

Con el Centro de Transparencia empoderamos a nuestros clientes con funciones de control y transparencia sobre sus datos.

Aplicación efectiva de las políticas y procesos:

De acuerdo con nuestra Política de Elaboración y Organización del Marco normativo, corresponde a la dirección de Auditoría Interna la coordinación del Marco Normativo del Grupo Telefónica, a través de la supervisión del proceso de definición de las normas Internas; promoviendo, a su vez, acciones que favorezcan la actualización y comunicación de las mismas. Adicionalmente detecta las necesidades y oportunidades de mejora, modificación o actualización de las Normas Internas existentes, proponiendo líneas de actuación a los Responsables de las Normas Internas, y proporcionar apoyo y asesoramiento al Responsable de la Norma Interna en relación con su redacción e implantación.

La observancia y cumplimiento de la normativa (p. ej. las políticas de privacidad, seguridad etc. mencionadas) son objeto de revisión y supervisión por parte de los responsables de las Normas Internas que lideran la propuesta, creación, difusión e implantación de la Norma interna y realizan su seguimiento, evaluación y actualización, quien está facultada para realizar las supervisiones muestrales de los controles siempre que lo considere conveniente.

GNI (Global Network Initiative) y RDR (Ranking Digital Rights)

Como muestra de nuestro compromiso con los derechos fundamentales de la libertad de expresión y la privacidad, 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. El GNI es una organización de escala global e 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 asumimos el compromiso de su implementación y rendición de cuentas mediante evaluaciones de cumplimiento por parte de asesores independientes. Así en el 2019, hemos pasado con éxito nuestro primer proceso de evaluación independiente del GNI. El Consejo de Administración del GNI, integrado por múltiples grupos de interés, determinó que Telefónica está realizando esfuerzos de buena fe para implementar los principios del GNI sobre la libertad de expresión y privacidad con mejoras a lo largo del tiempo. La evaluación positiva del GNI se basó en un informe de un asesor externo independiente (Deloitte) que evaluó las políticas, los procesos, y el modelo de gobernanza de Telefónica para salvaguardar la libertad de expresión y la privacidad de sus clientes.

Además, quedamos primeros entre todas las empresas de telecomunicaciones en la edición 2019 del Ranking *Digital Rights*, que evalúa los compromisos, políticas y prácticas de las empresas que afectan a la libertad de expresión y a la privacidad de los clientes, incluidos los mecanismos de gobernanza y supervisión.

Indicadores de este Informe

En los apartados siguientes reportamos el número de solicitudes que recibimos por parte de las autoridades nacionales competentes en los países donde operamos.

Cualquier solicitud que se pueda recibir por parte de una autoridad competente 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 Reglamento ante Peticiones por parte de las Autoridades Competentes. En Telefónica **no atendemos solicitudes privadas,** solo se tramitan las solicitudes que provienen de autoridades determinadas por ley. Dicho esto y como única excepción, en la lucha proactiva contra los contenidos de imágenes de abusos sexuales a menores de edad en la Red, Telefónica procede al bloqueo de estos materiales siguiendo las pautas y las listas proporcionadas por la Internet Watch Foundation.

Los indicadores que reportamos son:

- **Interceptaciones legales:** 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.
  Este año hemos incorporado el desglose de Interceptaciones siempre y cuando sea técnicamente y/o legalmente posible, por:
  - **Altas:** Solicitudes de una nueva interceptación.
  - **Prórrogas:** Solicitudes para prorrogar una interceptación ya existente.
  - **Bajas:** Solicitudes para desconectar a una interceptación existente.
- **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.).
  Este año hemos incorporado el desglose por tipo de bloqueo, cuando las herramientas y la legislación lo permiten.
- **Suspensiones geográficas o temporales de servicio:** Aquellas solicitudes requerimiento de las Autoridades Competentes para limitar temporal y/o geográficamente la prestación de un servicio. Estos requerimientos 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:

- **Solicitudes rechazadas o atendidas parcialmente:** número de veces que hemos rechazado una solicitud o que solo hemos proporcionado información parcial o ninguna información en respuesta a una solicitud por alguna de las siguientes razones:
  - Por no ajustarse a la legislación local para ese tipo de requerimiento.
  - Por no contener todos los elementos necesarios que posibilita la ejecución (firmas necesarias, autoridad competente, descripción técnica del requerimientos etc...)
  - Porque técnicamente es imposible ejecutar el requerimiento.

- **Accesos afectados:** número de accesos que se ven afectados por cada solicitud. Para bloqueo y restricción de contenidos contabilizamos Url's 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 solicitudes con potencial impacto relevante sobre el derecho a la libertad de expresión y derecho a la privacidad en las telecomunicaciones. Identificamos dicha solicitud y demandas como *major events.*

A este respecto cabe destacar en España la Modificación de la Ley 9/2014, General de Telecomunicaciones, en virtud de lo establecido en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Dicha ley y los artículos que afectan a Interceptación legal se detallan en el contexto legal del Informe de España.

También debemos destacar la situación de excepcionalidad en la que continúa 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.

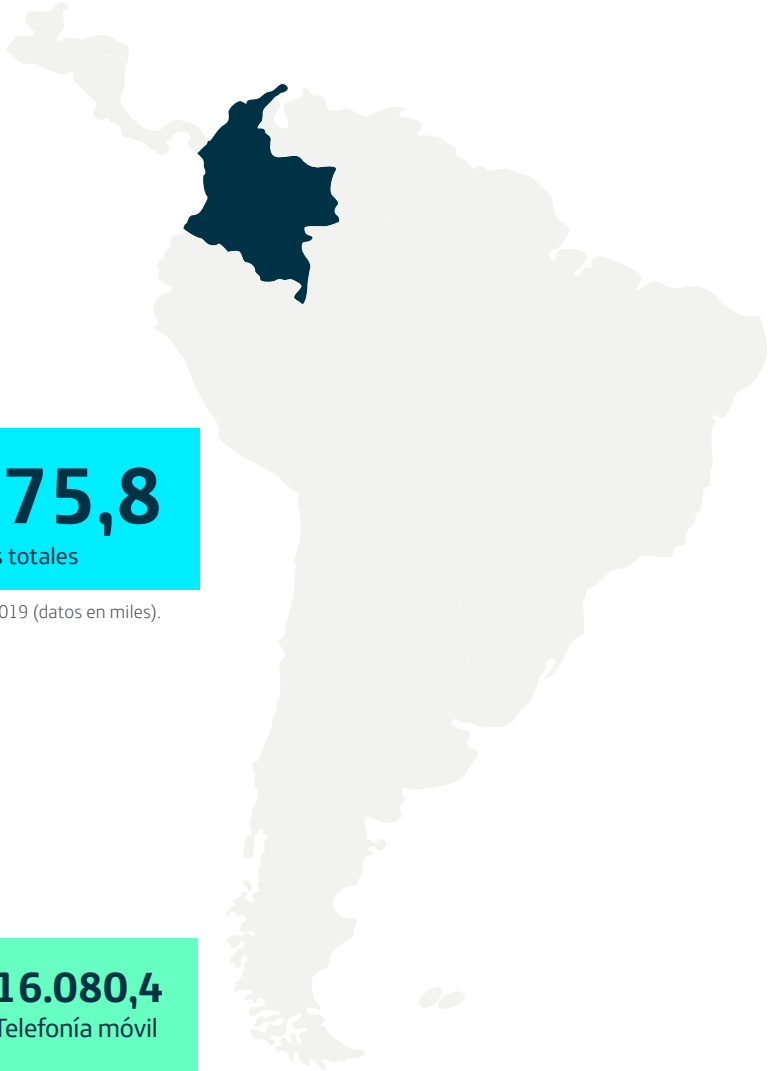
Colombia

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 19,2 millones de accesos a cierre de 2019.

Los ingresos de Telefónica en Colombia alcanzaron 1.410 millones de euros y el OIBDA sumó 558 millones de euros.



19.275,8
Accesos totales

Accesos a cierre de 2019 (datos en miles).

Accesos

1.487,7 Telefonía fija	**16.080,4** Telefonía móvil
1.179,2 Datos e Internet	**528,1** TV de pago

Accesos a cierre de 2019 (datos en miles).

INTERCEPTACIÓN LEGAL

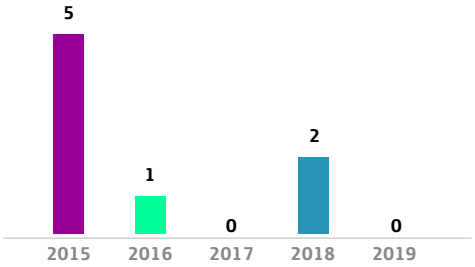
Contexto legal

- 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. Art. 44.
- Decreto 1704 de 2012. Artículo 1-8.
- Decreto 2044 de 2013. Art. 3.

Autoridades Competentes

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

Solicitudes*



*Solicitudes 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	0	Solicitudes rechazadas	0

METADATOS ASOCIADOS A LAS COMUNICACIONES

Contexto legal

- Constitución Colombiana: Artículo 250.
- Ley 906 de 2004. Art. 235.
- Ley 1621 de 2013. Ar. 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:

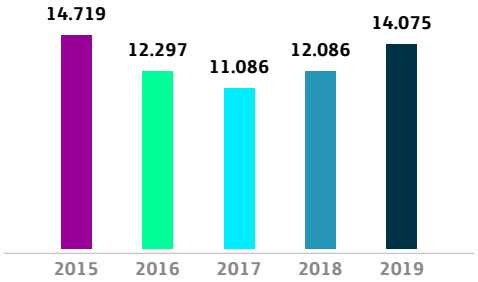
  - Fiscalía General de la Nación y todos sus servidores públicos que desempeñen funciones judiciales (Art. 249 CN y Art. 112, 113 CPP).
  - Policía Judicial: C.T.I., Policía Nacional y D.A.S., facultados por comisión de autoridad judicial competente y por mandato legal (Art. 311 a 320 CPP).
  - Grupos 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 (MINTIC, ANE, SIC y CRC).
  - 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 facultados las oficinas de control disciplinario interno.
- Policías con autorización del ministerio Público y orden de investigar.
- Juez de Sumario en Procedimiento penal inquisitivo. (Código Procedimiento Penal).
- Agencias de Inteligencia de Estado con autorización judicial previa.

Solicitudes



Accesos afectados	42.225	Solicitudes rechazadas	140

BLOQUEO Y RESTRICCIÓN DE CONTENIDOS

TOTAL URL AFECTADAS

URL afectadas	5.641	Solicitudes rechazadas	N/A*

*N/A por el sistema de bloqueo establecido por ley.

Material de abuso sexual infantil

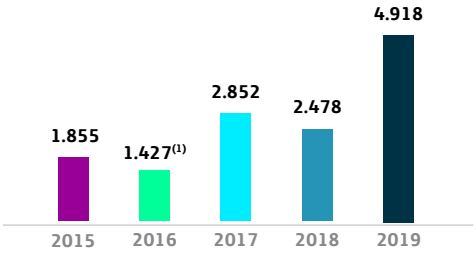
Contexto legal

- 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 URL*



(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 periodica por medio de la página web del Ministerio de las Tecnologías de la Información y las Comunicaciones.

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

Juegos Ilegales

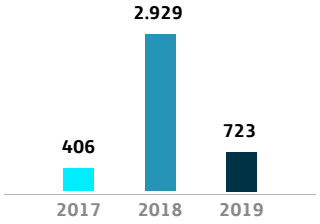
Contexto legal

- Ley 1753 de 2015: Artículo 93, parrágrafo 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 rentistico de los juegos de suerte y azar, en conjunto con la Policia 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 URL



Orden judicial

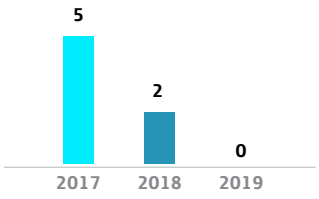
Contexto legal

- 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 Fiscalia General de la Nación y la Superintendencia de Industría 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 URL



SUSPENSIONES GEOGRÁFICAS O TEMPORALES DE SERVICIO

Contexto legal

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

Decreto 2434 de 2015, Resolución CRC 4972 de 2016 – Obliga a priorizar las llamadas entre autoridades para atender emergencias. Esta priorización implica terminar llamadas de usuarios que no están en el listado de números.

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.

Solicitudes

Accesos afectados	0	Solicitudes rechazadas	0

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 sialgún 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.

CONCEPTO	EXPLICACIÓN
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.
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.).

CONCEPTO	EXPLICACIÓN
***MAJOR EVENTS* (cont.)**	> 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.

CONCEPTO	EXPLICACIÓN
Solicitud	Una Petición es un requerimiento relacionado con la prestación de un servicio, en el ejercicio del deber de cooperación con las Autoridades Competentes. Una Petición puede contener una o varias solicitudes individualizadas, denominadas Solicitudes. Clases solicitudes: > Interceptaciones legales > Metadatos asociados a las comunicaciones: > Bloqueo y restricción de contenidos > Suspensiones geográficas o temporales de servicio
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 Locator* (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.