



Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos



Confianza digital

Queremos que nuestros clientes se sientan seguros usando nuestros servicios, que confíen en que protegemos sus comunicaciones y sus datos, y que contribuimos a que se haga un uso responsable de la tecnología.

Vivimos una parte cada vez más importante de nuestra vida a través de la conectividad y los servicios digitales, por eso, sabemos que la responsabilidad que asumimos en este ámbito condiciona el éxito a futuro. Así lo ven también nuestros grupos de interés, en particular inversores y analistas, que consideran que la seguridad y la privacidad es una de las temáticas más importantes en nuestro compromiso hacia el cliente (ver capítulo Materialidad).

La protección de los derechos de privacidad, seguridad de los datos y de la información, así como la protección del derecho a la libertad de expresión, junto con la protección de los derechos humanos en general, son temas que recaen bajo la supervisión del Consejo de Administración, a través de la Comisión de Regulación y Asuntos Institucionales. Esta Comisión se encarga de impulsar y seguir la implementación de nuestro Plan Global de Negocio Responsable, que incluye objetivos específicos en estas materias.

La confianza digital es un tema que, en los últimos años, ha despertado un interés creciente entre los reguladores, los grupos de interés especializados y los analistas. Existe además una creciente preocupación en la

sociedad sobre potenciales impactos negativos que podría conllevar un uso inadecuado o irresponsable de la tecnología. Ante esta situación, centramos nuestros esfuerzos en tres líneas de actuación:



■ **Cumplimiento de la ley:** Ante un entorno de presión regulatoria creciente, particularmente en Europa, ha sido muy importante nuestra interlocución con todos los actores europeos y nacionales necesarios para garantizar una correcta adaptación de todos nuestros procesos y actuaciones a la legislación aplicable.



■ **Transparencia:** Frente al cliente y otros grupos que representan sus intereses, hemos hecho un esfuerzo importante de aumentar la transparencia sobre cómo gestionamos la seguridad y la privacidad de su información, aumentando y simplificando la comunicación con el cliente. La confianza digital constituye un elemento importante de nuestra promesa cliente, y es importante que el cliente se de cuenta de la relevancia que le damos.



■ **Engagement y protección del menor:** La adopción y el uso por parte de la sociedad de los servicios digitales ha aumentado a una velocidad tan vertiginosa, que es importante que estemos en contacto continuo con clientes, expertos, otras empresas del sector y autoridades para detectar riesgos, analizar retos y proponer soluciones.

Desde el Canal de Negocio Responsable hemos recibido dos consultas/reclamaciones en temas de protección de datos de las cuales, una ha sido resuelta satisfactoriamente y la otra está pendiente de resolver. No hemos recibido ninguna consulta a través de este canal sobre seguridad y protección al menor.

No obstante, disponemos de canales específicos en privacidad y seguridad para que nuestros clientes puedan contactar con nosotros en las respectivas materias (ver apartado Privacidad y Seguridad).

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

PRIVACIDAD Estrategia

La búsqueda de confianza se está transformando en un reto empresarial y regulatorio, no solo para nosotros, sino también para los legisladores, reguladores y, en general, para todos los participantes en el ecosistema digital.

Cada vez son más los países que se han dado cuenta de que tienen que contar con nuevas regulaciones en protección de datos para adaptarse a la nueva economía digital.

Particularmente, en Europa, nos encontramos en plena implementación del Reglamento General de Protección de Datos (RGPD), con total aplicación a partir del 25 de mayo de 2018.

En Latinoamérica también se han fortalecido las normativas en protección de datos:

- **México:** El 26 de enero de 2017 se publicó el Decreto de expedición de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPD). La norma establece las bases, principios y procedimientos para garantizar el derecho a la protección de los datos personales.
- **Chile:** El 10 de marzo de 2017, el Gobierno de Chile firmó el proyecto de Ley de Protección de Datos Personales. Este proyecto busca modernizar la ley N° 19.628 sobre Protección a la Vida Privada de 1999 y actualizar el marco legal vigente, ante los avances de la tecnología y la necesidad de equilibrar los intereses de las personas con la libre circulación de la información.

Este contexto regulatorio es el reflejo de una realidad en la que la digitalización y el uso de los datos se ha convertido en la base de nuevos modelos de negocio, donde las reglas de juego no están escritas. La responsabilidad que asume cada compañía sobre cómo incorpora los valores y los derechos de las personas a sus propuestas de valor es crítica para que el cliente pueda seguir teniendo confianza en nosotros. No solo debemos incorporar en el diseño de todo servicio el respeto por los derechos de las personas, sino que también debemos ser cada vez más transparentes hacia el cliente sobre qué datos usamos, con qué fines, y cómo puede el propio cliente autorizar o modificar esta gestión.

Gobernanza

Como refuerzo al Gobierno Corporativo de la Compañía, el Consejo de Administración de Telefónica, S.A. dispone de Comisiones a las que encomienda el examen y seguimiento de áreas clave de especial relevancia. Así, la Comisión de Regulación y Asuntos Institucionales es la responsable de impulsar el desarrollo del Plan Global de Negocio Responsable, que incluye objetivos en aspectos de confianza digital (privacidad, seguridad y promoción del uso responsable de la tecnología).

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. a través de la Comisión de Auditoría y Control.

En Telefónica, S.A., sociedad matriz del Grupo Telefónica, esta responsabilidad ha sido asignada a la Dirección de Cumplimiento (*compliance*) del Grupo, quien en esta materia cuenta con el apoyo de la Dirección Técnica de Protección de Datos y la Dirección de Coordinación de Cumplimiento y Datos, con un doble rol corporativo y global.

Contamos además con un *Chief Data Officer*, que forma parte del Comité Ejecutivo. Su principal objetivo es definir la estrategia global de la Compañía en materia de datos, es decir, los servicios de Inteligencia Artificial asociados al *Big Data*. Esta función estratégica nos garantiza que la privacidad y la seguridad de los datos sean un elemento prioritario a tener en cuenta en todos nuestros servicios, estemos donde estemos.

El Comité responsable de coordinar todas las actuaciones de cumplimiento en materia de protección de datos es el Comité de Privacidad, que será reformulado por la aprobación de un modelo de gobierno de Protección de Datos a nivel global durante 2018.



Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Políticas

Nuestro compromiso con la privacidad está recogido en el principio de "Respeto a los Derechos de Privacidad y de Libertad de Expresión", que forma parte de nuestros Principios de Negocio Responsable. Se concreta en políticas y normativas internas que establecen pautas comunes para todas nuestras empresas:

- La **Política de Privacidad** global aprobada por el Consejo de Administración y que establece las directrices que todas las empresas del Grupo deben seguir para proteger la privacidad de sus clientes y de todos los grupos de interés que nos confían sus datos. Durante 2017, se ha estado trabajando para actualizar dicha política y adaptarla al nuevo contexto digital y a nuestra estrategia.

- Instrucción Protección de Datos de carácter personal.

Líneas de actuación

Durante el 2017, uno de nuestros principales objetivos ha sido mejorar la transparencia hacia nuestros grupos de interés. Así, en España se ha aprovechado el marco que ofrece el reglamento para, además de establecer las políticas y procedimientos adecuados para su cumplimiento, lanzar otros proyectos de cara a facilitar la transparencia hacia el cliente y ofrecer soluciones a inquietudes que estos puedan tener.

Un ejemplo de esto último son las siguientes iniciativas:

- **Focus Group con Clientes:** Se hizo con 8 grupos de discusión de 2 horas de duración y 8 participantes en cada grupo. En cada ciudad realizamos 2 grupos, uno de cliente Fusión y otro de cliente móvil.

En la muestra se incluyeron todos los clientes de Movistar Residencial de Fusión y Móvil, 4 segmentos de clientes según ciclo de vida (usuarios jóvenes de móvil, usuarios solo de móvil, clientes de Fusión, clientes de Fusión con hijos y el resto de clientes Fusión).

Los objetivos eran:

- Evaluar y conocer su percepción de la nueva normativa.
- Estudiar en qué medida creen que les afectará a su relación con las diferentes empresas de las que son clientes y cuál era su postura.
- Conocer cómo les gustaría que les comunicásemos e implementásemos estos cambios.
- Testar con ellos diversas propuestas en relación al consentimiento.

PRIVACIDAD DESDE EL DISEÑO



Trabajamos buscando la privacidad de nuestros clientes en el desarrollo de todos los productos y servicios, desde su idea inicial hasta su puesta en funcionamiento, aportando a los clientes seguridad, transparencia y control en el tratamiento de sus datos de carácter personal. Es lo que llamamos la privacidad por diseño, gracias a la cual tenemos en cuenta, no solo las garantías que ofrece la normativa aplicable en la materia, sino también las expectativas que los clientes tienen sobre su privacidad a la hora de usar nuestros productos y servicios.

Así, por ejemplo, en nuestra propuesta de Inteligencia Artificial, denominada Aura, los expertos en materia de protección de datos están involucrados con el equipo del producto desde el inicio en la definición de la experiencia digital de los clientes con la Compañía, en la definición de casos de uso y en las propuestas de gestión y control de sus datos. Se incorporan nuevos mecanismos más intuitivos, más cercanos y comprensibles de transparencia y consentimiento informado, promoviendo la generación de un espacio de confianza donde el cliente, de forma dialogada, pueda gestionar nuevas propuestas y casos de uso que le permitan enriquecer sus experiencias digitales.

■ Comunicación a Clientes:

- Pruebas pilotos en diferentes canales sobre recogida de consentimiento expreso para testar cuál es la mejor manera de informar y recogerlos.
- Comunicación del cambio de política con foco en el interés legítimo a través de nuestros diferentes canales (factura, web, TV...).

Carta del
PresidentePerfil y valores
de la Compañía1. Principales
magnitudes
20172. Contribución
al progreso e
impacto en las
comunidades3. Gobierno
corporativo4. Negocio
Responsable5. Modelo y
desarrollo de
negocio6. Compromiso
con el cliente7. Compromiso
con nuestro
equipo8. Compromiso
con la sociedad9. Compromiso
con el medio
ambiente

10. Anexos

- **Sistema de mediación voluntaria con AUTOCONTROL:** Operativo desde enero de 2018, para dar una respuesta ágil a las reclamaciones en materias como la suplantación de identidad y la recepción de publicidad no deseada. El procedimiento, desarrollado por la [Asociación para la Autorregulación de la Comunicación Comercial](#) (AUTOCONTROL), en colaboración con la [Agencia Española de Protección de Datos](#) (AEPD), cuenta junto a nuestra participación, con Orange y Vodafone y está abierto a otras entidades. Esta información se puede encontrar en el [Centro de Privacidad de Movistar](#).

En cada país disponemos de diversos canales de comunicación para los asuntos relacionados con la protección de datos, de acuerdo a cada legislación.

Durante el 2017, desde Telefónica España fuimos evaluados dentro del proyecto ¿Quién defiende tus datos? de [Éticas Foundation](#) y [Electronic Frontier Foundation \(EFF\)](#) y cuyo informe fue publicado en enero de 2018. El análisis tiene en cuenta la información pública de las organizaciones y webs sobre los siguientes aspectos: políticas de privacidad, lineamientos según la ley, notificación a los clientes de las demandas de datos gubernamentales, informes de transparencia y promoción de la privacidad de los usuarios.

Desde Movistar, lideramos el *ranking* de empresas analizadas en esta primera edición española con 6 estrellas y puntuación en 10 criterios, de un total de 12.

Procedimientos abiertos y sanciones

Durante 2017, en el total del Grupo reportamos 43 penalizaciones, un 22% menos respecto al 2016. Por otro lado, se abrieron 262 procedimientos por temas relacionados con protección de datos en el año. La cuantía total de las sanciones fue de 1.339.778,86 €. La mayoría de estos procedimientos se abrieron en España, donde la legislación es más estricta que en otros mercados.

Relación con instituciones y líderes de opinión

Para fomentar la cooperación internacional entre gobiernos y sector privado, y mejorar la transparencia en asuntos de seguridad nacional, derechos humanos y privacidad, somos miembros y participamos activamente en grupos de trabajo internacionales y regionales que promueven el respeto y la protección de la privacidad, seguridad y libertad de expresión. En 2017, las principales iniciativas han sido:

- **Center for Information Policy Leadership:** Somos miembros de este grupo, cuyo objetivo es la reflexión sobre política de privacidad y seguridad. Con sede en Washington DC, Bruselas y Londres, trabaja con líderes de la industria, autoridades reguladoras y responsables de políticas en todo el mundo para ayudar a contextualizar y promover la política de privacidad y ciberseguridad a escala global.
- **Rightscon:** Hemos participado en la edición de Rightscon en Bruselas del 29 al 31 de marzo, cuya temática son los derechos humanos digitales. Este evento reúne a grupos de interés a escala global.

Foro de Gobernanza de Internet en España:

Participando como ponentes y asistentes en distintas mesas redondas en el IGF España los días 28 y 29 de noviembre de 2017. Edición dedicada a los derechos digitales.

- **IGF:** Participación como ponentes y asistentes en el Foro de Gobernanza mundial celebrado en Ginebra del 18 al 21 de diciembre. Edición dedicada a los derechos digitales.

- **Eurodig:** Participación en mesas redondas en Tallin, el 6 y 7 de junio de 2017.

- **GSMA:** Tomando parte en sesiones de trabajo para la elaboración de los principios de responsabilidad del ecosistema móvil.

- **Consejo de Europa:** Firmamos un acuerdo entre empresas digitales y el Consejo de Europa para la promoción de derechos digitales, en Estrasburgo, el 8 de noviembre de 2017.

- **Data Transparency Lab:** Somos miembros de este laboratorio que trabaja para avanzar en la transparencia de los datos personales *online* a través de la investigación científica y el diseño.

- **Mapping Project:** Participamos en mesa redonda el 12 de septiembre en París, a través del proyecto europeo Mapping, liderado por el relator especial de Naciones Unidas para la Privacidad, Joe Canatacci.

43
penalizaciones, un
22%
menos respecto al 2016

Carta del Presidente

Perfil y valores de la Compañía

1. Principales magnitudes 2017

2. Contribución al progreso e impacto en las comunidades

3. Gobierno corporativo

4. Negocio Responsable

5. Modelo y desarrollo de negocio

6. Compromiso con el cliente

7. Compromiso con nuestro equipo

8. Compromiso con la sociedad

9. Compromiso con el medio ambiente

10. Anexos

SEGURIDAD Estrategia

El Plan Estratégico Global de Seguridad creado en 2017 y aprobado por el Comité Global de Seguridad en enero de 2018, cuenta con el apoyo del Comité de Dirección de la Compañía. Tiene un alcance de tres años y el objetivo de definir y establecer los objetivos de seguridad de nuestro Grupo durante su vigencia, a través de diferentes Planes de Acción (2017-2019).

En su elaboración se ha contado con la colaboración de las áreas globales, tales como Auditoría Interna, *Global Chief Technology Office*, *Global Innovation Office* y Recursos Humanos, para alinearnos con el resto de planes. Este plan es revisado anualmente para coordinarlo con la Estrategia Global y los Planes Estratégicos de la Compañía.

Este Plan complementa los esfuerzos realizados por los diferentes responsables para diseñar, desplegar, mantener y operar cada una de las 4 plataformas descritas en el capítulo 'Modelo de negocio', da soporte directo al negocio y aumenta el perímetro de seguridad, potenciando la prevención y control de amenazas, sin descuidar la reacción y contención ante incidencias. Está integrado por planes de acción, cada uno de ellos, coordinado por cada una de las distintas áreas de la Dirección Global de Seguridad.

Datos 4

Productos y Servicios 3

Sistemas y Tecnologías 2

Infraestructuras y Activos 1



Carta del Presidente

Perfil y valores de la Compañía

1. Principales magnitudes 2017

2. Contribución al progreso e impacto en las comunidades

3. Gobierno corporativo

4. Negocio Responsable

5. Modelo y desarrollo de negocio

6. Compromiso con el cliente

7. Compromiso con nuestro equipo

8. Compromiso con la sociedad

9. Compromiso con el medio ambiente

10. Anexos

Gobernanza

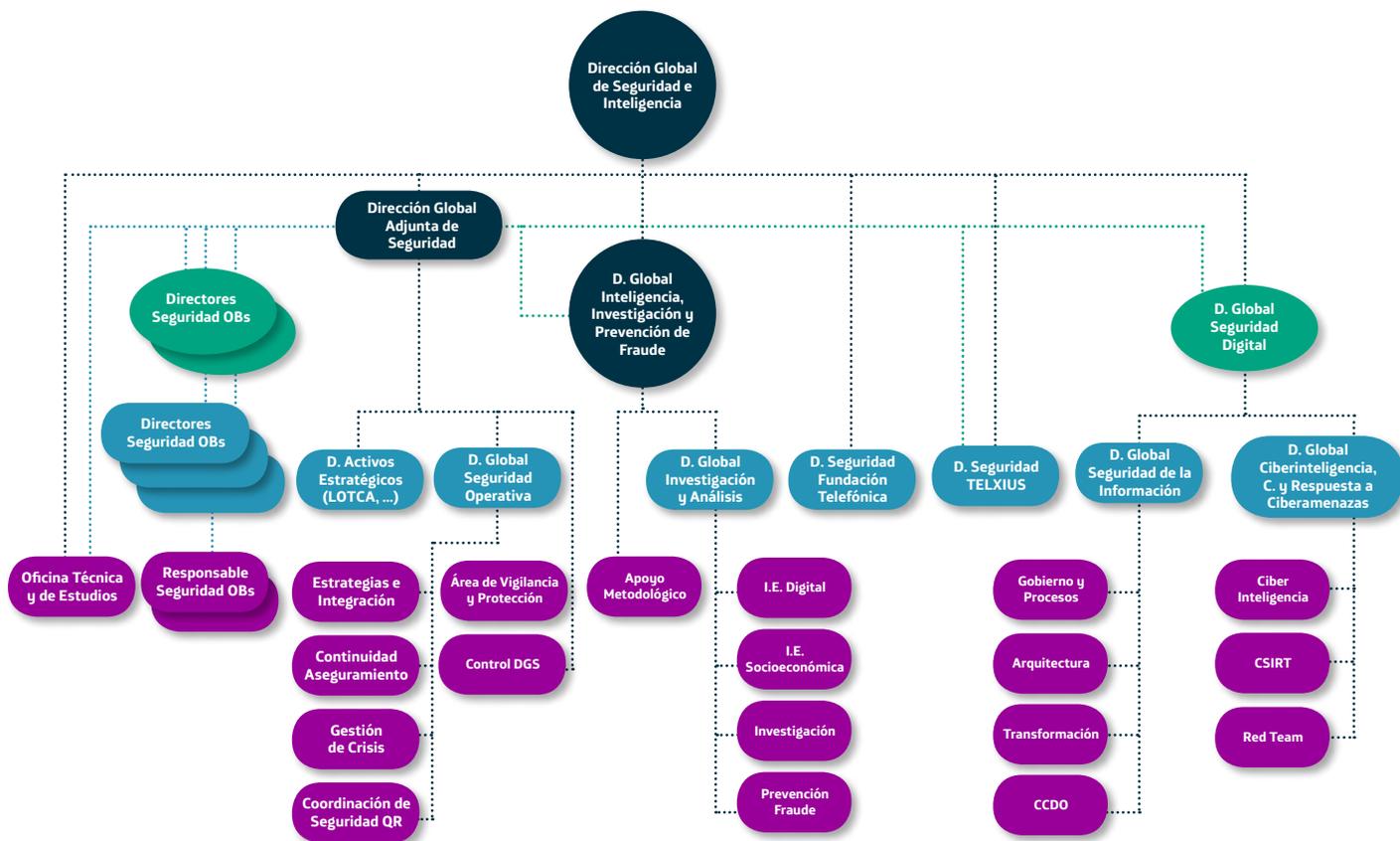
Nuestra Organización Global de Seguridad se construye tras la actualización de la Política Global de Seguridad en el 2016. La finalidad es preservar los activos de la Compañía y proteger los intereses y objetivos estratégicos, tanto en la organización vertical (incluyendo nuestras unidades de negocio) como en la dimensión transversal (aplicable a las tres plataformas):

- Infraestructura y Activos de Red
- Tecnologías de la Información
- Productos y Servicios

El Director Global de Seguridad es el representante máximo de la organización de seguridad en el Grupo Telefónica. Su misión es la protección eficaz y eficiente de nuestros

activos y está orientada a velar por la viabilidad del negocio.

Asimismo, existen responsables de seguridad, tanto a nivel global como local, cuyas obligaciones y responsabilidades están definidas y coordinadas por el Director Global de Seguridad. Cada empresa del Grupo tiene asignado uno de estos responsables, dependiendo de cuál sea la solución más eficiente y eficaz en cada caso.



Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Para garantizar la cohesión, la colaboración y la correcta gestión del Plan Estratégico y de los Planes de Acción, hemos definido un nuevo modelo basado en grupos de trabajo dentro del marco del Comité Global de Seguridad.

Este Comité, con un nuevo diseño y formato, es completamente ejecutivo y, por tanto, tiene la capacidad de elevar propuestas al Comité Ejecutivo de la Compañía.

Políticas

Para garantizar que los datos de nuestros clientes y servicios se mantienen a salvo y seguros, se ha desarrollado un trabajo de actualización y publicación de normativas y reglamentos de seguridad basados en las buenas prácticas del [Information Security Forum](#) [ISF], que dispone de varias normativas que fortalecen la seguridad global de la información.

Líneas de actuación Gestión de Calidad

Con el fin de alcanzar los objetivos de control determinados por la normativa de seguridad y el plan estratégico se han establecido un conjunto adecuado de controles. Estos se implementan, supervisan y revisan de forma continua para asegurar que se alcanzan los objetivos. En los reglamentos, instrucciones y manuales de seguridad se definen los criterios, requisitos, procedimientos y tecnologías que hay que tener en cuenta para establecer estos controles en cada entorno concreto.

| TEMAS | NORMAS |
|------------------------|---|
| Políticas y Normativas | Política Global de Seguridad Normativa Global de Seguridad Normativa de Auditoría |
| Reglamentos | Gestión de Incidentes y Emergencias Análisis de Riesgos de Seguridad Continuidad de Negocio Seguridad en Ciclo de Vida de Desarrollo Seguridad en la Infraestructura IT Seguridad en Redes y Comunicaciones Ciberseguridad Gestión de Cambios Clasificación y Tratamiento de la Información Gestión de Activos Control de Acceso Seguridad Física Seguridad en las Personas • Manual del Viajero Seguridad en la Cadena de Suministro Uso Servicios Internet |

Para realizar esta tarea se han puesto en marcha Sistemas de Gestión de la Seguridad de la Información (SGSI) basados en la norma ISO/IEC 27001.

Con independencia de lo anterior, siempre se debe tener un análisis de riesgos actualizado (ver capítulo 'Identificación y gestión de riesgos') y un plan de acción en el que se identifiquen y prioricen los proyectos y presupuestos orientados a implementar los controles de seguridad más adecuados que permitan conseguir los objetivos de control, así como reducir los riesgos de seguridad a un nivel aceptable para la organización.

Certificaciones y Estándares certificados o en proceso de certificación:

- Gestión de Servicios de Tecnologías de la Información: ISO 20000-1
- Gestión de Continuidad de Negocio: ISO 22301
- Gestión de Seguridad de la Información: ISO 27001
- Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago: PCI DSS (*Payment Card Industry Data Security Standard*)

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Seguridad de Red

Nuestro enfoque en redes y comunicaciones se basa en el adecuado conocimiento de nuestros activos y emplazamientos, sus características y su importancia para el negocio, de forma que las redes estén adecuadamente planificadas y ejecutadas, manteniendo siempre los requisitos de seguridad aplicables para minimizar el riesgo de indisponibilidad, acceso no autorizado o destrucción de las mismas.

La Normativa Global de Seguridad establece los objetivos de control necesarios para alcanzar un nivel de seguridad homogéneo y adecuado a las necesidades del negocio. Estos objetivos son:

1. Asegurar la protección de la información en las redes y los recursos de tratamiento.
2. Mantener la seguridad en la información que se transfiere dentro de la organización y con cualquier entidad externa.

Para asegurar el cumplimiento de dichos objetivos, se establecen los siguientes controles de seguridad:

■ Arquitectura de red y configuración de los dispositivos

Establecer una arquitectura de seguridad que permita administrar la complejidad de las redes y los diferentes dispositivos de la organización y proporcionar unos niveles de seguridad homogéneos en toda la organización.

Este control permite que los administradores de red y operadores de seguridad tomen decisiones más efectivas, ayudando a implementar una seguridad consistente y fácil de usar en las diferentes redes de la organización.

■ Gestión de la red física

Proteger nuestras redes internas (incluidas las redes de voz) mediante una documentación y un etiquetado exactos y actualizados, así como la aplicación de controles físicos para asegurar que todas las redes se configuren de forma precisa y segura, y proporcionar disciplinas de seguridad a los empleados.

■ Acceso inalámbrico

Asegurar que el acceso inalámbrico a nuestras redes y sistemas está sujeto a autorización, que los usuarios y los dispositivos informáticos sean autenticados y que el tráfico inalámbrico está cifrado. De esta manera, nos aseguramos de que solo las personas y los dispositivos informáticos autorizados obtengan acceso inalámbrico a las redes. También reducimos el riesgo de que las transmisiones inalámbricas sean monitorizadas, interceptadas o alteradas.

■ Acceso desde redes externas

Todas las conexiones desde redes externas a sistemas y redes de las empresas del Grupo Telefónica deben ser individualmente identificadas, verificadas, registradas y aprobadas por el propietario del sistema o la

red para evitar que usuarios no autorizados obtengan acceso a los sistemas y redes de la organización.

■ Dispositivos de protección de redes

Asegurar el tráfico de nuestras redes mediante el uso de dispositivos de protección como cortafuegos, IDS o IPS para evitar que tráfico no autorizado obtenga acceso a la red o salga de la misma.

■ Monitorización de redes y dispositivos de red

Monitorizar nuestras redes y los dispositivos de red que las soportan, para reducir la probabilidad de que un rendimiento degradado, una indisponibilidad temporal o una brecha de seguridad, tengan impacto en el negocio.

■ Conectividad de los puestos de trabajo

Disponer de medios seguros de conexión de los dispositivos utilizados por nuestros trabajadores (ordenadores portátiles, tablets y teléfonos inteligentes).

■ Telefonía, voz sobre IP y conferencias

Proteger nuestros recursos de telefonía y conferencias, mediante una combinación de controles físicos y lógicos, acceso restringido y concienciación de los usuarios para garantizar la disponibilidad de los recursos y proteger la confidencialidad e integridad de la información, así como prevenir y detectar el uso no autorizado o indebido de los recursos disponibles.

Carta del
PresidentePerfil y valores
de la Compañía1. Principales
magnitudes
20172. Contribución
al progreso e
impacto en las
comunidades3. Gobierno
corporativo4. Negocio
Responsable5. Modelo y
desarrollo de
negocio6. Compromiso
con el cliente7. Compromiso
con nuestro
equipo8. Compromiso
con la sociedad9. Compromiso
con el medio
ambiente

10. Anexos

■ Correo electrónico

Proteger el correo electrónico mediante una combinación de políticas, concienciación, procedimientos y controles técnicos de seguridad para garantizar su disponibilidad, proteger la confidencialidad e integridad de los mensajes y minimizar el riesgo de mal uso.

■ Mensajería instantánea

Proteger los servicios de mensajería instantánea, mediante la definición de políticas de gestión, la implementación de controles técnicos y la correcta configuración de los elementos de seguridad de su infraestructura.

Ciberseguridad, gestión de vulnerabilidades y brechas

Nuestro enfoque se basa en la proactividad, aplicar el conocimiento y la tecnología para alcanzar los niveles de protección requeridos, detectando rápidamente las infracciones o ataques en activo y construyendo las capacidades técnicas y humanas necesarias para responder con eficacia y rapidez ante cualquier brecha o incidente. Nuestro objetivo es minimizar la ventana de ataques y las consecuencias de los mismos.

La función global de Control y Respuesta a Ciberamenazas, que depende del Director Global de Seguridad, tiene la responsabilidad de definir, impulsar y coordinar los procesos y las capacidades humanas y tecnológicas necesarias en las empresas del Grupo.

Las funciones locales están coordinadas y siguen las líneas marcadas por la función global, dependiendo de los Responsables de Seguridad locales correspondientes.

Los responsables de seguridad locales, a su vez, pueden nombrar a un responsable a cargo de un equipo de ciberseguridad, para el ejercicio de esta función.

Contamos con una red de Centros de Respuesta a Incidentes (CSIRT), a nivel global, que trabajan de forma coordinada para conocer y analizar los riesgos de las potenciales ciberamenazas; monitorizar las vulnerabilidades graves existentes en los activos tecnológicos más críticos; establecer las relaciones con otros CSIRTs/ CERTs nacionales e internacionales tanto del sector público como privado; detectar los potenciales incidentes de seguridad que están afectando a los activos tecnológicos de la organización y responder ante los incidentes de seguridad que afectan a la organización.

Contamos con un buzón público, a nivel global y a disposición de cualquier usuario, con el fin de reportar alguna vulnerabilidad o amenaza que pudiera afectar a nuestra infraestructura tecnológica. Este buzón se encuentra en el [Centro de Privacidad Global/Seguridad](#).

Cuando el impacto o las consecuencias de un incidente y/o vulnerabilidad amenazan la continuidad de uno o varios procesos o servicios críticos o a la reputación de la

organización, contamos con un Plan de Continuidad de Negocio y un Sistema Global de Gestión de Crisis. Esto nos permite estar preparados para afrontar estas situaciones, facilitando la coordinación, la comunicación y colaboración de todas las áreas implicadas hasta recuperar la normalidad operativa en el menor tiempo y menor impacto posible.

Además, en el período 2014-2017 tuvimos varios programas de seguros, tanto a nivel local como global, para casos de incidentes. Nuestro reto en el 2018 es consolidar esta información para poder notificarla a nivel mundial. A nivel corporativo, tenemos una cobertura de ciberseguridad en caso de incidentes que ocasionen una pérdida de ingresos, gastos adicionales o recuperación de activos digitales, entre otros, y una cobertura de *'Technological Professional Indemnity'* en caso de reclamaciones de terceros, basado en los mejores estándares del mercado de seguros en términos de límites, sublímites y coberturas.

Durante 2017, se han gestionado 6 incidentes de seguridad, que han tenido un impacto mínimo gracias a los protocolos existentes de respuesta a incidentes. En uno de ellos ha estado involucrado un número muy limitado de datos de carácter personal sin consecuencias reseñables. Prueba de esto es que no hemos tenido multas relacionadas con brechas de seguridad.

 Más información, en el capítulo 'Emergencias'

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Servicios de seguridad

Gracias a nuestra unidad de servicios de ciberseguridad, ElevenPaths, este 2018 cumplimos 5 años ofreciendo innovación disruptiva para aportar confianza y privacidad a nuestra vida digital y la de nuestros clientes.

Hoy en día, estamos expuestos a sufrir ataques cada vez más frecuentes y sofisticados que ponen en peligro no solo los negocios, sino también nuestra reputación, privacidad y confianza. Por eso, necesitamos ser cada vez más receptivos a las medidas de ciberseguridad y redefinir nuestra estrategia hacia la ciber-resiliencia. Con este objetivo, dedicamos toda nuestra experiencia y esfuerzo a la creación de productos innovadores, logrando estar siempre un paso por delante de nuestros atacantes. Durante los cinco años de vida de la unidad, hemos combinado el desarrollo de tecnologías innovadoras patentadas con las tecnologías de los principales actores del mercado (*partners*) para proporcionar soluciones únicas. Queremos lograr un futuro más seguro para las personas y las empresas, y por ello, elegimos ser el proveedor de servicios de seguridad inteligente del mercado (*Intelligent MSSP*).

Nuestros servicios de ciberseguridad globales están diseñados para mejorar continuamente la eficacia de la infraestructura de seguridad.

Trabajamos para desarrollar nuevos servicios y capacidades de seguridad que ayuden a proteger los negocios y a las personas de las amenazas y vulnerabilidades, presentes en los entornos en los que operan. Colaboramos e intercambiamos información sobre amenazas, en tiempo real, con los principales organismos y entidades como la Comisión Europea, [Cyber Threat Alliance](#) (CTA), [ECSO](#), [EuroPol](#), [Incibe](#) y la [OEA](#).

Además, disponemos de diez centros de operaciones de seguridad (SOC) y un nuevo Centro Global Avanzado (*Telefónica Advanced Global SOC-TAGS*) que nos permiten afrontar las amenazas y problemas de seguridad con un enfoque global, pero sin distanciarnos de nuestros clientes.

En ElevenPaths impulsamos el espíritu emprendedor a través de la inversión en *startups* de ciberseguridad como [CounterCraft](#), [4iQ](#), [BlueLive](#), [LogTrust](#), [IMBox](#) y [Alise Devices](#). Gracias a estas colaboraciones, alianzas y nuestra propia experiencia, podemos ofrecer un portfolio de soluciones de seguridad integral para Internet de las cosas (IoT), identidad y privacidad, antifraude, ciberseguridad industrial, movilidad segura, exposición digital, gestión del riesgo y cumplimiento normativo con el objetivo de entregar a nuestros clientes una solución adaptada a sus necesidades específicas.

Wannacry

El 12 mayo de 2017 se produjo un ciberataque *ransomware* internacional que afectó a más de 150 países e innumerables empresas y organismos públicos. En el caso de Telefónica, esto no afectó ni comprometió en modo alguno la Red de telecomunicaciones, los servicios asociados o los datos personales de nuestros clientes.

Sin embargo, durante las primeras horas, nuestros sistemas internos de sensores bot detectaron que algunos PC ubicados en ciertos lugares de trabajo, en España, estaban potencialmente en riesgo de ser contaminadas por dicho *ransomware* y por esta razón,

implementamos inmediatamente la detección y protocolos de respuesta para este tipo de incidente de seguridad. Estos funcionaron robusta y continuamente desde el comienzo del ataque y durante sus momentos más críticos.

Nuestros valores guiaron todas y cada una de las decisiones tomadas desde el principio, conscientes de lo que somos, junto con nuestro compromiso inquebrantable con el servicio al cliente y nuestra obligación social ineludible de responsabilidad cívica. Por esta razón, fuimos los primeros en dar la alarma y colaboramos con agencias gubernamentales y organismos públicos.

Carta del Presidente

Perfil y valores de la Compañía

1. Principales magnitudes 2017

2. Contribución al progreso e impacto en las comunidades

3. Gobierno corporativo

4. Negocio Responsable

5. Modelo y desarrollo de negocio

6. Compromiso con el cliente

7. Compromiso con nuestro equipo

8. Compromiso con la sociedad

9. Compromiso con el medio ambiente

10. Anexos

TRANSPARENCIA

Conscientes de la importancia de merecer la plena confianza de nuestros clientes y usuarios, durante el 2017, hemos trabajado para mejorar el Centro de Privacidad Global e implementar centros locales en las webs comerciales de los países donde operamos. Hasta la fecha se han creado cuatro centros de privacidad en España, Brasil, Argentina y Colombia.

El objetivo de estos centros es que nuestros usuarios puedan encontrar toda la información sobre privacidad, seguridad y uso responsable de la tecnología de forma fácil y comprensible.

Aprovechamos estos centros para acercar nuestras políticas y procesos a un lenguaje más comprensible hacia el cliente, así, por ejemplo, en Brasil incorporamos un vídeo sobre el centro de privacidad y en Colombia una infografía explicativa de las condiciones de privacidad.

Además, hemos publicado nuestro segundo Informe de Transparencia de las Telecomunicaciones, como ejercicio de transparencia imprescindible en un mundo en el que se comparten espacios de responsabilidad a la hora de preservar y garantizar los derechos de las personas, de una parte, por las empresas y de otra por los Estados (ver capítulo de Derechos Humanos).

Colombia

Política de Colombia Telecomunicaciones S.A. ESP. para el tratamiento de datos personales

Como parte de nuestro compromiso con la transparencia y la privacidad a continuación podrás conocer la Política de Colombia Telecomunicaciones S.A. ESP. para el tratamiento de datos personales, en la cual se explican los condiciones a las que están sometidos los datos personales recolectados en ejercicio de las actividades comerciales y legales.

¿Qué tratamiento se hace de los datos personales recolectados?
El tratamiento al cual son sometidos los datos personales recolectados en ejercicio de las actividades comerciales y legales de Colombia Telecomunicaciones son:

- Actualizar
- Usar
- Conservar
- Suprimir
- Compartir
- Circular

A terceros

¿Para qué fines se usa la información?

- El suministro de información relativa al cumplimiento de las obligaciones de los titulares de los datos.
- El cálculo de riesgo económico o crediticio.
- La publicación de directorios telefónicos.
- La prevención y control de fraudes.
- Para beneficio propio o de terceros con los que Colombia Telecomunicaciones haya celebrado convenio para envío y recepción de cualquier tipo de información, con fines comerciales o publicitarios en Colombia y en el exterior.

¿Cuáles son los derechos de los usuarios y cómo se pueden ejercer?
Los titulares de los datos recogidos en las bases de datos de la empresa tienen derecho a:

conocer actualizar rectificar suprimir revocar

sus datos personales mediante comunicación dirigida a la Gerencia Gestión y Soporte de Colombia Telecomunicaciones y/o a través de la página web www.movistar.co por medio del enlace o correo electrónico "contáctenos".

¿A quién se le pueden presentar peticiones, consultas y reclamos?
Colombia Telecomunicaciones, a través de la Gerencia Gestión y Soporte, atenderá las peticiones, consultas y reclamos relacionados con datos personales que formulen los titulares de los datos.

¿Por cuánto tiempo se conservan los datos personales?
Las bases de datos de Colombia Telecomunicaciones tienen vigencia indefinida. Los datos personales recolectados se conservarán por el tiempo que dure la relación existente entre la empresa y el titular de los datos, y por el tiempo necesario para el cumplimiento de los deberes legales o contractuales que Colombia Telecomunicaciones deba observar. Las bases de datos de Colombia Telecomunicaciones tienen vigencia indefinida.

Cambios de esta política
Colombia Telecomunicaciones podrá modificar en cualquier momento la Política de Tratamiento de Datos Personales. Cualquier cambio sustancial en la Política será comunicado antes de su implementación a través de la página web de la empresa.

UNA MARCA DE **Telefónica**

Argentina

movistar Televisión - Tienda - Atención al cliente - Acceso MI Movistar

Centro de privacidad Movistar

En Movistar consideramos que nuestra actividad debe basarse en el respeto absoluto a la confidencialidad y privacidad de tus datos personales, de tal forma que puedas saber en todo momento como hacer uso de ellos. En el Centro de Privacidad podrás encontrar las Condiciones de Privacidad de nuestra web y nuestros productos y servicios así como los mecanismos de los que disponemos para que puedas gestionar tu Privacidad.

Áreas de privacidad

- Portal
- Condiciones de privacidad
- Política de cookies
- Contratos
- Fusión
- Telefonía Fija
- Móvil
- Internet
- Televisión
- Aplicaciones y Servicios
- Garantía de venta de equipos
- Cómo gestionar mi privacidad

Condiciones de privacidad

Como parte de nuestro compromiso con la privacidad reflejado en la Política Global de Privacidad de Telefónica, las presentes condiciones aplican cómo recogemos, utilizamos y protegemos tus datos de carácter personal cuando accedes a Movistar.es, con el fin de que puedas decidir si deseas facilitar tus datos personales a través de los formularios habilitados al efecto.

ALCANCE DE LA POLÍTICA

Cuando accedes y usas Movistar.es te comprometes a aceptar estas condiciones de Privacidad, así como las disposiciones contenidas en el Aviso Legal, la Política de Cookies y, en su caso, las Condiciones Generales de Contratación que puedes encontrar en la sección de Contratos de movistar.es

En Movistar.es te proporcionamos información para que, con carácter previo a la cumplimentación de tus datos personales, puedas acceder a las Condiciones de Privacidad y a cualquier otra información relevante en materia de Protección de Datos.

Estas condiciones son válidas únicamente para los datos de carácter personal que se obtienen en movistar.es, y no son aplicables a aquella información recabada por terceros en otras páginas web, incluso si éstas se encuentran enlazadas en Movistar.es.

Brasil

vivo MEU VIVO

Centro de Privacidade

A confiança é a chave para as pessoas poderem tirar o máximo da tecnologia.

Em um mundo cada vez mais digital e interativo, as pessoas precisam ter certeza de que os seus dados, informações pessoais e seguras, sendo geridos de um jeito transparente.

Entenda o Centro de Privacidade

- Entenda o Centro de Privacidade
- Informações coletadas
- Políticas de Segurança
- Direito de Acesso, Retificação, Oposição e Cancelamento
- Menores de Idade

A Vivo quer garantir a sua privacidade e promover a transparência nos seus direitos de usar os nossos produtos e serviços. Tudo isso em um ambiente de segurança e desde...

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

CONTROL INTERNO

Para atender las disposiciones legales de cada país, relacionadas con la Política de Privacidad de Datos, en el Plan Anual de Auditoría de 2017, se realizan proyectos específicos para verificar su cumplimiento, así como la identificación de las mejores prácticas en temas de protección de datos.

En 2017 dimos continuidad a las revisiones de protección de datos de carácter personal, ejecutando un total de 19 auditorías internas en esta materia en todo el Grupo.

Los aspectos más importantes que revisamos han sido: aplicación de las medidas de seguridad en el tratamiento de los datos personales; control de acceso lógico a los mismos; asegurar la integridad de la información; calidad de la información; consentimiento para el tratamiento de los datos y posibilidad de que los usuarios puedan ejercitar sus derechos de acceso, rectificación, cancelación y oposición de la información relacionada con ellos.

19

auditorías internas
revisiones de *protección
de datos* de carácter
personal

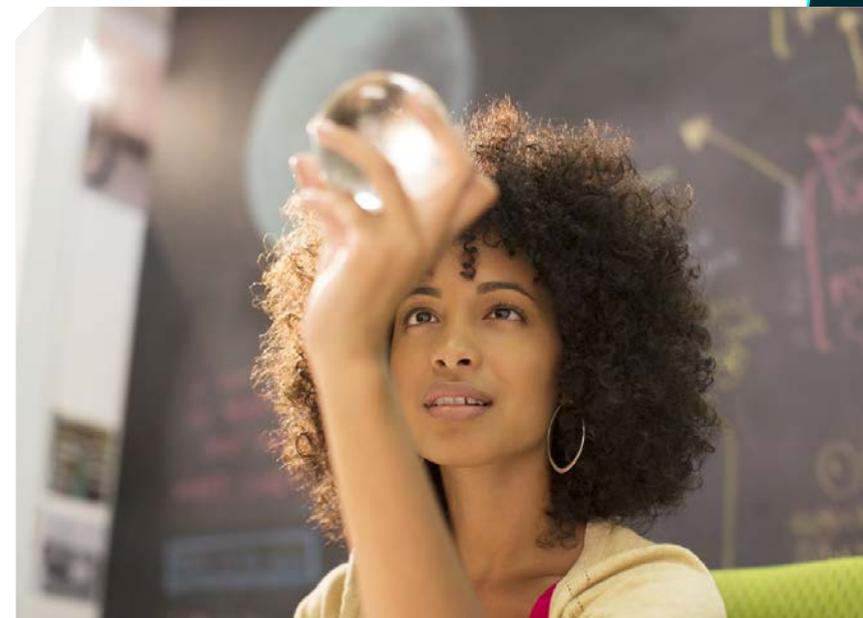
En 2017
47.278 profesionales
completaron la formación
global en materia de
protección
de datos

Además, dentro de nuestro Plan Anual de Auditoría Interna ponemos foco en temas relacionados con la Ciberseguridad y Seguridad en Redes y Sistemas de Tecnología de la Información, como base fundamental para proteger el acceso y la integridad de dichos elementos, verificando que la seguridad de acceso lógico es la adecuada. Estas auditorías se basan en la realización de trabajos técnicos que abarcan, entre otros aspectos, la seguridad lógica de redes y sistemas de tecnología de la información, ciberseguridad, gestión de incidentes, así como la revisión de controles de seguridad perimetral. A dicho respecto, durante el año 2017 se han llevado a cabo un total de 51 auditorías que dan cobertura a las materias anteriormente mencionadas.

FORMACIÓN Y SENSIBILIZACIÓN

Durante 2017, continuamos con el plan de formación global en materia de protección de datos. Un total de 47.278 profesionales la han completado este año, un 85% más respecto al 2016. Esto supone el 34% de los empleados totales del Grupo.

A nivel corporativo llevamos a cabo diferentes iniciativas de concienciación, entre las que cabe destacar la publicación, tutoriales y consejos de seguridad a través de correos, la Intranet y Yammer a todos los empleados del Grupo.



Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

PROTECCIÓN AL MENOR Y USO RESPONSABLE DE LA TECNOLOGÍA

La familiaridad de los más pequeños de la casa con las herramientas conectadas no es ajena a nadie. Ellos, son el ejemplo más claro de cómo ha cambiado nuestra manera de vivir, interactuar, aprender, etc. Esto se hace extensivo también a la forma de vivir de los adultos, nuestra manera de trabajar, de compartir información o de consumir ocio.

Con el objetivo de fomentar un entorno seguro en Internet y concienciar a la sociedad sobre la importancia de aprender a sacar el máximo provecho de las herramientas digitales en nuestro día a día, hemos definido una estrategia global basada en la promoción del uso responsable e inteligente de la tecnología en todos los ámbitos de nuestra vida, pero haciendo especial hincapié en la protección de un colectivo más vulnerable como lo son los niños y jóvenes.

Nuestras líneas de actuación y compromisos con la protección al menor en la Red y la promoción del uso responsable de la tecnología se recogen en 6 líneas clave de trabajo:

- Alianzas con grupos de interés
- Bloqueo de contenidos
- Entorno audiovisual
- Productos y servicios
- Trabajo con proveedores
- Educación y sensibilización

Alianzas con grupos de interés

Velar por una Red más segura es una tarea que no podemos abordar en solitario, es

por ello que, en Telefónica, trabajamos de manera conjunta con aliados sectoriales y de la sociedad civil con el objetivo de que niños y jóvenes sean conscientes de que Internet es una ventana abierta llena de oportunidades, pero que es importante también saber que existen riesgos que hay que aprender a gestionar.

En este sentido, podemos destacar nuestra colaboración con:

- Fuerzas y Cuerpos de Seguridad del Estado, así como el apoyo a las diferentes líneas de denuncia nacionales (Equipo Niños, ASI, Seguros

en Internet, Safernet, Te Protejo, *Centre for Child Protection on the Internet*, entre otras).

- ONGs, asociaciones nacionales (Pantallas Amigas, Safernet, UNICEF, Faro Digital, NSPCC, RedPapaz, Argentina Cibersegura, entre otras).
- Acciones con grupos de interés clave en la protección al menor *online* (Inhope, Insafe, ANATEL, RCPI, CONNA, UNODC, Red de Aliados por la Niñez, Zentrum, für Kinderschutz im Internet, INAI, ITAIPUE, Red Contra la Pornografía Infantil, Gobiernos, entre otras).

GUATEMALA

Desde Telefónica Guatemala participamos en el grupo de trabajo Seguridad en línea para niños y adolescentes, con el objetivo de implementar medidas para la protección *online* de los más jóvenes.

EL SALVADOR

En El Salvador formamos parte del grupo de trabajo del Consejo Nacional de Protección de la Niñez y Adolescencia (CONNA) para habilitar una línea de denuncia para que niños y niñas denuncien sus derechos.

Además, desde 2015, firmamos la carta de compromiso con UNICEF y la GSMA para impulsar acciones para la protección de los menores en le mundo *online*, además de participar activamente en el comité que da seguimiento a lo acordado en dicha carta.

PANAMÁ

A través de Telefónica Panamá formamos parte de la Red de Aliados por la Niñez. Las organizaciones participantes han asumido el cumplimiento de 10 compromisos con el fin de trabajar en favor de los derechos de los menores.

PERÚ

Desde Telefónica Perú formamos parte del grupo de trabajo Riesgos en Internet para Niños, Niñas y Adolescentes, en la que también participan UNODC, Ministerio del Interior, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, UNICEF e InfoTrata.

NICARAGUA

En Nicaragua formamos parte de la Mesa de Trabajo Nacional del Uso Seguro de Internet, liderada por la Vicepresidencia de la República, a través del Consejo Nicaragüense de Ciencia y Tecnología, en la que, además, participan el Ministerio de Educación, la Cámara Nicaragüense de Telecomunicaciones e Internet, empresas privadas, universidades y ONGs.

COLOMBIA

Formamos parte del Grupo de trabajo Te Protejo, mesa de trabajo que tiene por objetivo promover iniciativas sobre protección de niños y jóvenes en la Red.

Carta del
PresidentePerfil y valores
de la Compañía1. Principales
magnitudes
20172. Contribución
al progreso e
impacto en las
comunidades3. Gobierno
corporativo4. Negocio
Responsable5. Modelo y
desarrollo de
negocio6. Compromiso
con el cliente7. Compromiso
con nuestro
equipo8. Compromiso
con la sociedad9. Compromiso
con el medio
ambiente

10. Anexos

Asimismo, participamos en las siguientes alianzas con el objetivo de promover a nivel global el intercambio de buenas prácticas y el impulso de acciones concretas alrededor del buen uso de Internet:

- Alianza con la GSMA para la lucha contra los contenidos de abusos sexuales a menores.
- *ICT Coalition*.
- Alianza para proteger mejor a los menores *online*.

A nivel local, también participamos en numerosos grupos de trabajo que fomentan el uso responsable e inteligente de la tecnología entre los más jóvenes.

Bloqueo de contenidos

Para luchar de manera proactiva contra los contenidos e imágenes de abusos sexuales a menores en la Red, en Telefónica procedemos al bloqueo de estos materiales siguiendo las pautas y las listas proporcionadas por la [Internet Watch Foundation](#) en los siguientes países: Chile, Costa Rica, Ecuador, El Salvador, España, Guatemala, Nicaragua, México, Panamá, Perú, Reino Unido, Uruguay y Venezuela. Desde Telefónica Colombia, hacemos lo propio a través de MINTIC y la DIJIN.

Entorno audiovisual

Los niños y adolescentes hacen cada vez un uso más intensivo de nuestros productos y servicios en general y de los contenidos audiovisuales en particular. Las pantallas, además, constituyen una parte fundamental en su desarrollo personal,

La **tecnoadicción** es una realidad que afecta a las nuevas generaciones, por lo que es especialmente necesario informar a familias, educadores y a los propios menores de la importancia de hacer un **uso sano y responsable de Internet y la tecnología**

social y cívico, razón por la que desde Movistar + creemos fundamental:

- Asegurar que nuestra programación proteja a la infancia ante contenidos potencialmente inadecuados.
- Establecer las herramientas necesarias para hacer un buen uso de la televisión, garantizando que los padres dispongan de medios técnicos eficaces que les permitan ejercer su responsabilidad sobre los contenidos televisivos que ven sus hijos.
- Fomentar la alfabetización digital entre los menores y sus familias para aprovechar el potencial de los medios audiovisuales y hacerles conscientes de la necesidad de un consumo y ocio responsable e inteligente.

En este sentido, en nuestras diferentes operaciones contamos con las siguientes iniciativas:

- Etiquetado de contenidos por edad o por tipo de contenido.
- Controles parentales, pin parental y pin de compra en el dispositivo que permiten al cliente la posibilidad de bloquear canales y contenidos bajo demanda para menores.
- El contenido específico para adultos se presenta en una sección separada de los demás contenidos y es necesario introducir un pin especial para poder acceder a ella.
- Información sobre uso responsable de la TV o sobre los contenidos audiovisuales en la propia televisión y en la web comercial.
- Actividades de sensibilización sobre el uso responsable de las pantallas.



Carta del
PresidentePerfil y valores
de la Compañía1. Principales
magnitudes
20172. Contribución
al progreso e
impacto en las
comunidades3. Gobierno
corporativo4. Negocio
Responsable5. Modelo y
desarrollo de
negocio6. Compromiso
con el cliente7. Compromiso
con nuestro
equipo8. Compromiso
con la sociedad9. Compromiso
con el medio
ambiente

10. Anexos

Productos y servicios

Aunque realmente pensamos que nada podrá sustituir a la labor mediadora de un adulto cuando hablamos de educar en el uso responsable de las herramientas digitales, cuando esto no es posible, siempre tendremos el apoyo de la tecnología. Para ello, apostamos por la promoción y el desarrollo de productos y servicios que promuevan el uso responsable y seguro de la Red y de los dispositivos conectados:

■ **Controles parentales:** [Movistar Protege](#) (España), [Vivo Filhos Online](#) (Brasil), [Parental Control](#) (Reino Unido).

■ **Soluciones de seguridad con funcionalidad de control parental:** Escudo Movistar ([Colombia](#), [Ecuador](#), [El Salvador](#), [Perú](#), [Uruguay](#)), Seguridad Multidispositivo ([Argentina](#), [Chile](#)), Seguridad Total de Mcfee ([Argentina](#), [Chile](#), [Perú](#)) y Centro de Seguridad de Mcfee ([Colombia](#)).

■ **Otros servicios** (antivirus, packs personalizados...): Gurú, O2 Protect (Alemania), [Vivo Família Online](#) (Brasil).

Trabajo conjunto con nuestros proveedores

Examinamos junto a nuestros proveedores la posibilidad de implantación de los parámetros básicos de protección al menor, para asegurar el mejor desarrollo de los más pequeños. Algunas iniciativas en las que estamos trabajando:

■ **Seguridad desde el diseño:** desde el área de innovación en ecosistemas trabajamos estrechamente con los principales fabricantes de terminales, así como con los sistemas operativos para incluir funcionalidades de protección al menor que formen parte del propio sistema operativo.

■ **Seguridad desde los sistemas operativos:** Estamos totalmente comprometidos con la seguridad y la privacidad de nuestros clientes. Para ello, trabajamos con los principales "players" de la industria para mejorar el nivel de actualización de seguridad de los terminales que los clientes tienen en sus manos, así como en aumentar la transparencia sobre el tipo de datos que pueden estar compartiendo al hacer uso de sus terminales móviles.

■ **Colaboración en el desarrollo e implementación de iniciativas que promuevan el uso responsable de la tecnología y la protección del usuario:** mantenemos una comunicación fluida con los responsables de producto de los diferentes ecosistemas digitales para mejorar el uso de estos por parte de los clientes y para promover el buen uso de la tecnología.

Iniciativas de educación y sensibilización

El uso responsable e inteligente de Internet y la tecnología, se presenta hoy como un reto para todos, no solo para los más jóvenes. El mundo de las redes sociales, las aplicaciones móviles, los *smart devices*, o la realidad

virtual... evoluciona tan rápido que puede ser difícil mantenerse al día. Sin embargo, somos conscientes de esta realidad y por ello apostamos por el desarrollo de iniciativas formativas y de sensibilización para todos los públicos, que faciliten la convivencia en una sociedad cada vez más digital.

dialogando

El portal [dialogando.com](#) es una muestra de ello, y la iniciativa ha sido implantada ya en 15 países del Grupo Telefónica: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Guatemala, México, Nicaragua, Panamá, Perú, Uruguay y Venezuela.



En la web, un comité de expertos informa a través de artículos, vídeos, campañas de comunicación, entrevistas, etc. sobre los aspectos que más preocupan hoy en día a la sociedad, para conseguir desenvolverse sin miedos y de manera exitosa como buenos ciudadanos digitales.

Carta del
PresidentePerfil y valores
de la Compañía1. Principales
magnitudes
20172. Contribución
al progreso e
impacto en las
comunidades3. Gobierno
corporativo4. Negocio
Responsable5. Modelo y
desarrollo de
negocio6. Compromiso
con el cliente7. Compromiso
con nuestro
equipo8. Compromiso
con la sociedad9. Compromiso
con el medio
ambiente

10. Anexos

Además, hemos llevado a cabo diversas iniciativas entre las que destacan:

Jornada Acoso Escolar LGTBfóbico:

Organizada desde Dialogando en la Telefónica FlagShipStore Madrid, su objetivo fue sensibilizar a la sociedad sobre las nuevas formas de acoso que están en auge. En ella participaron profesionales de distintos ámbitos que luchan contra el *ciberbullying* y se explicó a los asistentes las claves para comprenderlo y abordarlo, así como el impacto que puede tener el uso de las tecnologías de la información y la comunicación sobre la convivencia escolar.

Impulso a la comunicación de la iniciativa

de **Movistar #RodamosJuntos**: Campaña de concienciación con el objetivo de recordar la importancia del respeto mutuo entre ciclistas y conductores en la carretera y que Dialogando apoyó con contenidos de sensibilización sobre el uso responsable del teléfono móvil al volante y al usar la bicicleta.

Publicación cuento infantil "WhatsApps, videojuegos y cabezas mutantes. A ti también te puede ocurrir":

Dirigido a niños de 4 a 8 años. Desde Dialogando buscamos fomentar una buena educación en el uso de las tecnologías conectadas, tan importantes son las normas y los límites como el acompañamiento y la supervisión de las actividades digitales de los niños por parte de los adultos. Un acompañamiento que, además, es deseado por los menores que buscan la complicidad de sus padres en el uso de los dispositivos digitales. Esto supone una oportunidad para fortalecer la relación y la comunicación entre padres e hijos.



Campaña de sensibilización

#ContraseñaSegura - 8 claves para proteger la entrada a tu vida digital:

En colaboración con [Pantallas Amigas](#). La acción, que forma parte del programa educativo "Pilar y su celular", ofrece a los más jóvenes las pautas básicas a la hora de definir una clave de acceso robusta a los servicios de Internet.

Proyecto Ciberexpert@:

Su objetivo es aportar una mayor educación digital a las familias y aportar una visión positiva del uso seguro y responsable de Internet mediante diferentes actividades de sensibilización y charlas en colegios, además de visualizar de manera real los riesgos y problemas que los menores se pueden encontrar en la Red. Creado por la Unidad de

Participación Ciudadana de la Policía Nacional, cuenta con el apoyo de Telefónica y Fundación Cibervoluntarios.

Hitos 2017

- Centros de Privacidad locales en 4 países. 
- Sistema de mediación voluntaria para Reclamaciones sobre Protección de Datos en Telefonica España. 
- 85% más de formados en Privacidad y Seguridad respecto a 2016. 
- Implantación de Dialogando en 15 países. 

Objetivos 2018

- Ampliación de los Centros de Privacidad locales.
- Actualización de la Política Global de Privacidad.
- Campañas de sensibilización de uso responsable con proveedores.
- Desarrollo de herramientas para fomentar un buen uso de los contenidos audiovisuales por parte de los menores.

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Buenas prácticas

BRASIL

Llevamos a cabo las "Jornadas Semana de Internet Segura", cuyo objetivo era doble. Por un lado, queríamos concienciar sobre uso responsable de la tecnología, dando a conocer el portal Dialogando y, por otro, abordar la importancia de utilizar Internet de manera más consciente y positiva, resaltando la responsabilidad que cada usuario tiene cuando publica un comentario, un post o da un "me gusta" en alguna red social.

Además, el Día de Internet Segura el equipo de Vivo Brasil participó en un evento organizado por SaferNet en el que grandes empresas contaron las iniciativas en las que están trabajando alrededor del uso responsable de la tecnología. Asimismo, a lo largo de la semana se realizaron debates con empleados sobre los temas de mayor interés en el uso de la Red por niños y adolescentes, con el apoyo de Safernet Brasil.

ALEMANIA

En Telefónica Alemania publicamos una guía de Internet segura para la infancia con motivo del "Día del Niño", con la colaboración de Deutschen Kinderhilfswerk, FSM (Freiwillige Selbstkontrolle Multimedia Dienstanbieter) y FragFINN e.V.

Esta guía ofrece a los menores y a sus padres asistencia para una mejor alfabetización mediática

y una mayor seguridad en el mundo digital. Asimismo, el folleto proporciona información útil sobre cómo los niños pueden beneficiarse de Internet y lo que deben tener en cuenta en el caso de recibir correo no deseado, publicidad o virus. Además, la Guía de Internet contiene consejos para el uso correcto de su propio teléfono inteligente.

ARGENTINA

Desde Movistar Argentina lanzamos durante 2017 el programa de uso seguro y responsable de la tecnología "Elegí Cuidarte" y la plataforma web "Dialogando", un espacio de información y reflexión sobre el uso de las TIC. La inauguración del portal fue apoyado por el lanzamiento de la campaña de seguridad vial "Elegí Cuidarte a vos, como cuidas tu celular", que buscó concienciar sobre los riesgos de hablar, mandar mensajes o chatear mientras se conduce. Dicha campaña recibió la distinción de la organización Luchemos por la vida.

Durante la segunda parte del año se trabajó en una campaña sobre prevención del Grooming o acoso sexual a menores a través de Internet "Love Story" impulsada junto con la Asociación Civil Faro Digital, que registró más de 5 millones de visualizaciones en su spot central y recibió un premio otorgado por Argentina CiberSegura. Esta iniciativa se complementó con charlas presenciales para empleados de la compañía y a través de la Fundación Telefónica para el público general y escuelas.

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Buenas prácticas

NICARAGUA

El dúo musical Nina y Sebastián acompañó a Fundación Telefónica en la presentación del sitio web Dialogando, con el objetivo de sensibilizar a niños y jóvenes con mensajes sobre el buen uso de Internet. Su participación fue compartida con gran éxito en las redes sociales. Asimismo, los músicos promovían el uso positivo de la tecnología en sus conciertos lanzando mensajes entre canciones e invitando a los jóvenes a disfrutar de Internet de manera sana y responsable.

ESPAÑA

Llevamos a cabo una jornada sobre uso responsable de la tecnología "#DialogandoConectados ¿EPIC FAIL O EPIC WIN?", que junto con el apoyo de Fundación Telefónica se organizó en Madrid con el objetivo de discutir y analizar con numerosos expertos de ámbitos las cuestiones que más preocupan a la sociedad alrededor del uso que estamos haciendo de Internet y los dispositivos conectados en nuestro día a día: ¿sabemos aprovechar todo el potencial que nos

ofrece la tecnología?, ¿somos capaces de trasladar las normas básicas de educación y respeto al mundo digital? ¿cómo podemos prevenir los casos de ciberviolencia de género o ciberacoso escolar?

Asimismo, Dialogando presentó el estudio "Los 10 epic fails de los españoles", con el objetivo de constatar que son necesarios educación y conocimiento profundo de las redes para sacar partido a Internet sin riesgos.

ECUADOR

Desde Telefónica Ecuador hemos organizado espacios de diálogo en colegios y universidades con motivo del lanzamiento de la plataforma de uso responsable de la tecnología Dialogando. Entre las sesiones impartidas se trataban, entre otros temas:

- Campaña Intercolegial de Reciclaje de teléfonos móviles: Charla e-waste.

- Formación ambiental en material de residuos eléctricos y electrónicos.
- Formación en el uso responsable de la tecnología: aprendizaje en la correcta gestión de la identidad digital, privacidad, redes sociales...
- Smart cities y cambio climático.

COLOMBIA

En Colombia participamos "Conectados para protegerlos", un encuentro organizado como parte de las actividades de la red de socios del canal de denuncia virtual Te Protejo, que sirvió como escenario para presentar en el país el modelo We Protect, contra la explotación sexual de niñas, niños y adolescentes, buscando además instalar un

compromiso entre el gobierno, las autoridades, empresas y ONG para su implementación inmediata en el país.

We Protect es una herramienta que permite respuestas coordinadas e integrales entre los países para prevenir, mitigar y combatir la explotación sexual en línea en niños, niñas y adolescentes.

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Buenas prácticas

MÉXICO

Lanzamos la campaña “*Love Story*”, que busca concienciar y prevenir que niños y adolescentes acepten a extraños en sus redes sociales, evitando que sean víctimas de abusos, tales como acoso, sexting o grooming. Esta campaña ha obtenido además el reconocimiento “Sol de Plata” en la categoría de TV y Cine de Electrónica de Consumo, durante la edición número 32 del Festival Iberoamericano de la Comunicación Publicitaria.

También durante 2017, desde Telefónica México presentamos el videojuego “*Privacy Adventure*”, disponible de manera gratuita para dispositivos Android e iOS, promueve aspectos de privacidad y seguridad para el uso de tabletas y teléfonos móviles, tales como el bloqueo, etiquetado, mensajería instantánea, descargas, geolocalización, bluetooth y wifi, subiendo en cada nivel la complejidad para que niños y adultos adopten buenos hábitos sobre el uso responsable de la tecnología.

GUATEMALA

Por medio de la campaña de comunicación “*Elegí Cuidarte*”, en Movistar Guatemala buscamos sensibilizar a nuestros clientes sobre la necesidad de hacer un uso adecuado de Internet y las redes sociales. La campaña está basada en el vídeo “*Love Story*”, en la cual dos jóvenes se conocen a través de las redes sociales y cuyo principal objetivo es prevenir que niños y jóvenes no acepten solicitudes de extraños en Internet y eviten caer en las redes del grooming.

PERÚ

Lanzamos el cuento “Whatsapp, videojuegos y cabezas mutantes” junto a influencers y líderes digitales.

Con el objetivo de fomentar el uso responsable y seguro del Internet para niños y niñas, desde Telefónica Perú presentamos este cuento, en el marco de las acciones de la compañía para el uso adecuado de las tecnologías de información y comunicación. Durante la presentación, los niños y sus padres disfrutaron de una representación teatral del cuento, que dio a conocer los efectos que ocasiona el uso no responsable de dispositivos como tablets, ordenadores o teléfonos móviles.

PANAMÁ

Desde Telefónica Panamá lanzamos la campaña #YoElijo sobre el uso responsable del teléfono móvil, orientada a promover una cultura de uso responsable.

Esta campaña invita a reflexionar sobre las pequeñas cosas que podemos hacer para evitar riesgos y ayudar a construir una mejor sociedad. La campaña se basó en 4 consejos fundamentales:

1. #YoElijo no aceptar extraños en redes sociales.
2. #YoElijo no chatear mientras manejo el auto.
3. #YoElijo no hacer cyberbullying.
4. #YoElijo no compartir imágenes crudas.

Carta del
Presidente

Perfil y valores
de la Compañía

1. Principales
magnitudes
2017

2. Contribución
al progreso e
impacto en las
comunidades

3. Gobierno
corporativo

4. Negocio
Responsable

5. Modelo y
desarrollo de
negocio

6. Compromiso
con el cliente

7. Compromiso
con nuestro
equipo

8. Compromiso
con la sociedad

9. Compromiso
con el medio
ambiente

10. Anexos

Buenas prácticas

VENEZUELA

Organizamos talleres sobre huella digital y ciberacoso. En ellos, buscamos crear espacios presenciales con estudiantes (niños, niñas y adolescentes), maestros y padres para transmitir contenidos y consejos prácticos sobre el buen uso de la tecnología. Lo interesante de estos talleres es que se debate sobre situaciones reales y cómo impactan en los profesionales, jóvenes y familiares.

URUGUAY

Lanzamos una campaña sobre el uso responsable del teléfono móvil en el coche. Así, publicamos en revistas y diarios, así como en redes sociales varias piezas gráficas con el siguiente "claim": Un mensaje de voz también puede provocar un siniestro. No uses el celular mientras manejas. La gráfica fue premiada como el mejor anuncio en prensa del año en el Festival de Campanas de Publicidad.

REINO UNIDO

Desde O2 Reino Unido colaboramos con la principal organización benéfica para niños del país, NSPCC, con el objetivo de ayudar a los padres a entender la vida online de sus hijos y cómo mantenerlos a salvo. El proyecto, visible a través de una sección de la web comercial, incluye iniciativas de sensibilización, asesoramiento y formación así como la web [Net Aware](#), un site en el que poder encontrar consejos y recomendaciones sobre el uso responsable de la tecnología. Además, O2 Reino Unido ofrece una línea gratuita de ayuda de seguridad en línea (0808 800 5002) y un chat específico para resolver dudas sobre uso responsable, que brinda a los padres acceso a expertos en seguridad en línea a los que se podrá solicitar ayuda sobre consejos alrededor de las redes sociales, configuración de privacidad y control parental, los siete días de la semana.

Asimismo, las familias que lo deseen, podrán suscribirse a un servicio de correo electrónico para obtener información, consejos y actividades, enviadas directamente a su bandeja de entrada, que les ayudará a mantener conversaciones regulares con sus hijos sobre cómo mantenerse seguros en la Red.