We want our customers to feel confident using our services, that they trust that we protect their communications and data, and that we contribute towards the responsible use of technology.

We live an increasingly important part of our lives through connectivity and digital services; we therefore know that the responsibility we assume in this field conditions future success. This is how our stakeholders, specifically investors and analysts, also see it, considering that security and privacy is one of the most important issues in our commitment towards the customer (see chapter on ‘Materiality’).

The protection of privacy rights, data security and information security, as well as the protection of the right to freedom of expression, together with the protection of human rights in general, are issues that fall under the supervision of the Board of Directors through the Regulations and Institutional Affairs Committee. This Committee is in charge of driving and supervising the implementation of our Global Responsible Business Plan, which includes specific goals on these matters.

Digital trust is an issue that, in recent years, has created a growing interest among regulators, specialised stakeholders and analysts. There is also a growing concern in society concerning potential negative impacts that could lead to an inappropriate or irresponsible use of technology. Considering this situation, we focus our efforts on three lines of action:

- **Compliance with the law:** In an environment of increasing regulatory pressure, especially in Europe, our dialogue with the national and European actors needed to guarantee a correct adaptation of all our processes and actions to the applicable legislation has been very important.

- **Transparency:** With regard to customers and other groups that represent their interests, we have made a significant effort to increase the transparency of how we manage the security and privacy of their information, increasing and simplifying the communication with the customer. Digital trust constitutes an important element of our customer promise, and it is important that the customer can see the importance that we give to this subject.

- **Engagement and protection of minors:** The adoption and use by society of digital services has increased at a speed that is so dizzying that it is important that we are in continuous contact with customers, experts, other sector companies and the authorities to detect risks, analyse challenges and propose solutions.

From the Responsible Business Channel we have received two queries/claims on data protection issues, one of which has been satisfactorily resolved and the other has yet to be solved. We have not received any query on security and the protection of minors via this channel.

However, we have specific channels for privacy and security so that our customers can contact us regarding the respective subjects (see section on Privacy and Security).
PRIVACY
Strategy
The search for trust is turning into a business and regulatory challenge not only for us, but also for legislators, regulators, and, in general, for all the participants in the digital ecosystem.

Increasingly more countries have realised that they have to have new regulations on data protection to adapt to the new digital economy.

Specifically in Europe, we find ourselves in the complete implementation of the General Data Protection Regulations (GDPR), with total application as of 25 May 2018.

Regulations for the protection of data have also been strengthened in Latin America:

- **Mexico:** On 26 January 2017 the Decree of Issuance of the General Law of Protection of Personal Data in Possession of the Mandatory Subjects (LGPD for its Spanish original) was published. The standard establishes the bases, principles and procedures for guaranteeing the right to the protection of personal data.

- **Chile:** On 10 March 2017, the Government of Chile signed the Personal Data Protection Law project. This project seeks to modernise law No. 19,628 of 1999 regarding the Protection of Private Life, and update the current legal framework considering the advances in technology and the need to balance the interests of people with the free flow of information.

This regulatory context is the reflection of a reality in which digitalisation and the use of data has become the basis of new business models, where the rules of the game aren’t written. The responsibility assumed by each company regarding how they incorporate the values and rights of people to their value proposals is critical so that the customer can continue to have confidence in us. Not only must we incorporate in the design of the entire service the respect for the rights of people, but we must also be increasingly transparent towards the customer about what data we use, to what purpose, and how the customer itself can authorise or modify this management.

Governance
To strengthen the Corporate Governance of the Company, the Telefónica S.A. Board of Directors has Committees to which it entrusts the study and monitoring of areas of particular relevance. Thus, the Regulations and Institutional Affairs Committee is responsible for promoting the development of the Global Responsible Business Plan, which includes goals regarding aspects of digital trust (privacy, security and promotion of the responsible use of technology).

The head of the personal data protection function is the Data Protection Officer (DPO), who reports directly to the Board of Directors of Telefónica, S.A. through the Audit and Control Committee.

At Telefónica, S.A., parent company of the Telefónica Group, this responsibility was assigned to the Group’s Compliance Directorate, who in this matter has the support of the Data Protection Technical Directorate and the Data and Compliance Coordination Directorate, with a double corporate and global role.

We also have a Chief Data Officer who is part of the Executive Committee. Their principal objective is to define the Company’s global strategy on data. In other words, the cognitive intelligence services associated with Big Data. This strategic function guarantees that the privacy and security of the data are priority elements to keep in mind in all our services, wherever we are.

The Committee responsible for coordinating all the actions in terms of data protection compliance is the Privacy Committee, which will be reformulated by the approval of a Data Protection governance model on a global level during 2018.
Policies
Our commitment to privacy is reflected in the principle of “Respect for the Rights of Privacy and Freedom of Expression”, which is part of our Responsible Business Principles. It is embodied in internal policies and regulations which establish common guidelines for all our companies:

- The global Privacy Policy approved by the Board of Directors establishes the guidelines that all Group companies must follow in order to protect the privacy of our customers and that of all the stakeholders that entrust us with their data. During 2017, work was done to update the policy and adapt it to the new digital context and our strategy.

- Instructions for the Protection of Personal Private Data.

Lines of action
During 2017, one of our main objectives was to improve transparency towards our stakeholders. Thus, in Spain the framework offered by the regulation was used for launching other projects in order to facilitate transparency towards the customer and offer solutions to concerns that they may have, as well as to establish the adequate policies and procedures for its compliance.

An example of the latter are the following initiatives:

- **Customer Focus Group**: Done with 8 discussion groups over 2-hour long sessions, with 8 participants in each group. In had 2 groups in each city: one of Fusion customers, and the other of mobile customers.

- The sample included all Movistar Residential Fusion and Mobile customers, 4 segments of customers according to life cycle (young mobile users, only mobile users, Fusion customers, Fusion customers with children and the rest of Fusion customers).

The objectives were:

- To assess and understand their perception of the new regulations.
- To study to what extent they believe that it will affect their relationship with the different companies of which they are customers, and what was their position.
- To learn about how they would like these changes to be communicated to them and how they would like them to be implemented.
- To test with them different proposals regarding consent.

PRIVACY BY DESIGN
We work on including the privacy of our customers in the development of all our products and services, from the initial idea to its final implementation, providing customers with security, transparency and control over how they treat their personal data. This is what we call privacy by design, as a result of which we take into account not only the guarantees provided by the applicable legislation on the matter but also the customer’s expectations with regard to their privacy when using our products and services.

Thus, for example, in our Artificial Intelligence proposal called Aura, the experts on matters of data protection are involved with the product team from the start, with the definition of the digital experience of customers with the Company, with the definition of cases of use, and with proposals for the management and control of their data. New, more intuitive, closer, and understandable transparency and informed consent mechanisms are incorporated, promoting the generation of a space of trust where the customer, in a conversational manner, can manage new proposals and cases of use that allow them to enrich their digital experiences.

- **Communication to Customers**: 
  - Pilot tests on different channels regarding the collection of express consent to test which is the best way to inform and collect them.
  - Communication of the change in policy through our different channels (invoice, web, TV...) with focus on legitimate interests.
Voluntary mediation system with AUTOCONTROL: In operation since January 2018 to give a quick answer to claims in matters such as identity theft and the receipt of unwanted advertising. The procedure, developed by the Association for the Self-regulation of Commercial Communications (AUTOCONTROL), in collaboration with the Spanish Data Protection Agency (AEPD for its Spanish original), includes the participation of Orange and Vodafone as well as our own, and is open to other entities. This information can be found in the Movistar Privacy Centre.

We have different communications channels in every country for issues related to the protection of data, in accordance with each legislation.

During 2017, at Telefónica Spain we were assessed within the Ethical Foundation and Electronic Frontier Foundation (EFF). Who defends your data project, and whose report was published in January 2018. The analysis takes into account the public information of organisations and websites on the following aspects: privacy policies, guidelines according to the law, notification to customers of the demands of governmental data, reports of transparency, and the promotion of user privacy.

Movistar leads the ranking of companies analysed in this first Spanish Edition, with 6 stars and a score of 10 criteria out of a total of 12.

Open procedures and sanctions
During 2017, we reported 43 penalties in the entire Group, 22% less than in 2016. Furthermore, 262 procedures related to topics on data protection were opened during the year. The total sum of penalties was €1,339,778.86. Most of these procedures were initiated in Spain, where legislation is stricter than in other markets.

Relationship with institutions and opinion leaders
In order to contribute to international cooperation between governments and the private sector, and to improve transparency in issues affecting national security, human rights and privacy, we are members and active participants in international and regional working groups that promote respect and protection of privacy, security and freedom of expression. In 2017, the principal initiatives were:

Centre for Information Policy Leadership: We are members of this group whose goal is the reflection on privacy and security policy. With offices in Washington DC, Brussels and London, it works with industry leaders, regulatory authorities and policy-makers around the world to help contextualise and promote privacy and cybersecurity policy on a global scale.

Rightscon: We participated in the Rightscon edition in Brussels from 29 to 31 March, the theme of which was digital human rights. This event brings together stakeholders on a global scale.

Internet Governance Forum in Spain: Participation as speakers and attendees in different round tables in the IGF Spain on 28 and 29 November 2017. Edition dedicated to digital rights.

IGF: Participation as speakers and attendees in the Global Governance Forum held in Geneva from 18 to 21 December. Edition dedicated to digital rights.

Eurodig: Participation in round tables in Tallin, on 6 and 7 June 2017.

GSMA: Taking part in work sessions for the elaboration of the mobile ecosystem responsibility principles.

European Council: We signed an agreement between digital companies and the European Council for the promotion of digital rights in Strasbourg, on 8 November 2017.

Data Transparency Lab: We are members of this laboratory that works to move forward in the transparency of online personal data through scientific research and design.

Mapping project: We participated in the round table on 12 September in Paris through the European Mapping project led by the United Nations Special Rapporteur on Privacy, Joe Canatacci.
SECURITY

Strategy

The Global Strategic Security Plan, created in 2017 and approved by the Global Security Committee in January 2018, has the support of the Company’s Management Committee. It has a three-year scope and the goal is to define and establish our Group’s security objectives during its period of validity through different Action Plans (2017-2019).

It was prepared in collaboration with global areas, such as Internal Audit, the Global Chief Technology Office, the Global Innovation Office and Human Resources, to align ourselves with the rest of the plans. This plan is reviewed annually to coordinate it with the Company’s Global Strategy and Strategic Plans.

This Plan complements the efforts made by the different parties responsible for designing, deploying, maintaining and operating each of the four platforms described in the ‘Business Model’ chapter, provides direct support to the business, and increases the security perimeter, strengthening the prevention and control of threats without neglecting the reaction to, and containment of, incidents. It is made up of action plans, each of them coordinated by each of the different areas of the Global Security Directorate.
Governance
Our Global Security Organisation was built after the updating of the Global Security Policy in 2016. The purpose is to preserve the Company's assets, and to protect the strategic interests and objectives both in the vertical organisation (including our business units), and in the transversal dimension (applicable to the three platforms):

- Network Infrastructure and Assets
- Information Technologies
- Products and Services

The Global Security Director is the maximum representative of the security Organisation in the Telefónica Group. Its mission is the efficient and effective protection of our assets and is aimed at ensuring the viability of the business.

Within the security Organisation there are Security Officers both on the global and local levels. Their obligations and responsibilities are defined and coordinated by the Global Security Director. Each Telefónica Group company will have one of these Security Officers assigned to it, depending on what is the most efficient and effective solution in each case.
In order to guarantee the cohesion, collaboration and correct management of the Strategic Plan and Action Plans, we have defined a new model based on working groups within the framework of the Global Security Committee.

This Committee, with a new design and format, is completely executive and will therefore have the capacity to submit proposals to the Company’s Executive Committee.

**Policies**

Work has been done to update and publish standards and safety regulations based on best practices of the Information Security Forum (ISF), which has several regulations that strengthen the global security of information, and has been developed to guarantee that the data of our customers and services is kept safe and sound.

**Lines of action**

**Quality management**

An adequate set of controls has been established for the purpose of achieving the control objectives established by the security regulations and the strategic plan. These are continuously implemented, supervised and reviewed to ensure that these objectives are reached. The regulations, instructions and security manuals define the criteria, requirements, procedures and technologies that must be taken into account to establish these controls for each specific setting.

To perform this task, Information Security Management Systems (ISMSs) based on the ISO/IEC 27001 standard have been implemented.

Regardless of the aforementioned, an updated analysis of risks must be considered, as well as an action plan (see chapter on ‘Identification and management of risks’) in which the projects and budgets aimed at implementing the most adequate security controls that allow for fulfilment of the control objectives are identified and prioritised, as well as reduction of security risks to a level acceptable to the organisation.

**Certifications and Standards that are certified or in the process of certification:**

- Management of Information Technology Services: ISO 20000-1
- Business Continuity Management: ISO 22301
- Managing Information Security: ISO 27001
- Data Security Standard for the Prepaid Card Industry: PCI DSS (Payment Card Industry Data Security Standard)
Network security
Our focus on networks and communications is based on the adequate knowledge of our assets and sites, their characteristics and their importance for the business, in such a way that the networks are properly planned and executed, always maintaining the applicable security requirements to minimise the risk of unavailability, unauthorised access, and the destruction of said networks.

The Global Security Regulation establishes the control objectives needed to reach a homogeneous level of security and meet business needs. These objectives are:

1. To ensure protection of the information in the networks and the processing resources.
2. To maintain the security of the information transferred within one organisation and to any external entity.

The following security controls are established to ensure the compliance of said objectives:

- **Network architecture and configuration of devices**
  Establishment of a security architecture that makes it possible to manage the complexity of the networks and different devices of the organisation, and provide homogeneous security levels throughout the organisation. This control allows network administrators and security operators to make more effective decisions, helping to implement consistent and easy-to-use security in the different networks of the organisation.

- **Management of the physical network**
  Protection of our internal networks (including voice networks) through exact and updated documentation and labelling, as well as the application of physical controls to ensure that all the networks are accurately and securely configured, and provide security disciplines to employees.

- **Wireless access**
  Assurance that wireless access to our networks and systems is subject to authorisation, that users and computer devices are authenticated, and that the wireless traffic is encrypted. In this way, we ensure that only authorised people and computer devices obtain wireless access to the networks. We also reduce the risk of wireless transmissions being monitored, intercepted, or altered.

- **Access from external networks**
  All connections from external networks to Telefónica Group company systems and networks must be individually identified, verified, registered and approved by the owner of the system or network to prevent unauthorised users from gaining access to the systems and networks of the organisation.

- **Network protection devices**
  Ensure the secure traffic of our networks through the use of protection devices such as firewalls, IDS or IPS, to avoid unauthorised traffic gaining access to or from the network.

- **Monitoring of networks and network devices**
  Monitoring of our networks and the network devices that support them to reduce the probability that a degraded performance, temporary unavailability, or a security breach have an impact on the business.

- **Workstation connectivity**
  Provision of secure connection measures for the devices used by our workers (laptops, tablets and smartphones).

- **Telephony, voice over IP and conferencing**
  Protection of our telephony and conferencing resources through a combination of physical and logical controls, restricted access and awareness of the users, to guarantee the availability of resources, and protect the confidentiality and integrity of the information, as well as preventing and detecting the unauthorised or improper use of the available resources.

- **Email**
  Protection of emails through a combination of policies, sensitisation, and technical security procedures, and controls to guarantee their availability, protect the confidentiality and integrity of the messages and minimise the risk of incorrect use.
**Instant messaging**

Protection of the instant messaging services through the definition of management policies, the implementation of technical controls and the correct configuration of the security elements of their infrastructure.

**Cybersecurity, management of vulnerabilities, and breaches**

Our approach is based on proactivity, applying the knowledge and technology to achieve the required levels of protection, quickly detecting infractions or active attacks, and building the technical and human capabilities necessary for effectively and quickly responding to any breach or incident. Our goal is to minimise the window for attacks and the consequences of such attacks.

The global function of Cyberthreat Control and Response, which reports to the Global Security Director, is responsible for defining, promoting and coordinating the human and technological processes and capacities necessary in the companies of the Group.

The local functions are coordinated and follow the lines set forth by the global function, depending on the corresponding local Security Officers.

The local Security Officers, in turn, may appoint a person in charge of a cybersecurity team for the exercise of this function.

We have a network of Response to Incidents Centres (CSIIRT for its Spanish original), at a global level, which work in a coordinated way to understand and analyse the risks of potential cyberthreats; to monitor the serious vulnerabilities that exist in the most critical technological assets; to establish the relationships with other national and international CSIRTs/CERTs in both the public and private sector; to detect the potential security incidents that are affecting the organisation’s technological assets; and to respond to the security incidents that affect the organisation.

We have a public inbox at a global level that is available to any user, for the purpose of reporting any vulnerability or threat that could affect our technological infrastructure. This inbox is located in the Global/Security Privacy Centre.

When the impact or consequences of an incident and/or vulnerability threaten the continuity of one or several processes or critical services, or the reputation of the organisation, we turn to our Business Continuity Plan and a Global Crisis Management System. This allows us to be prepared to face these situations, facilitating the coordination, communication and collaboration of all the areas involved until operational normality is recovered in the shortest possible time and with the least possible impact.

In addition, in the 2014-2017 period we had several insurance programmes, both at a local and global level, for cases of incidents. Our challenge in 2018 is to consolidate this information to be able to notify it a global level.

At a corporate level, we have cybersecurity coverage in the event of incidents that cause a loss of revenue, additional expenses, or the recovery of digital assets, among others, and 'Technological Professional Indemnity' coverage in case of third party claims, based on the highest standards of the insurance market in terms of limits, sub-limits and coverages.

During 2017, six security incidents that had a minimal impact thanks to the existing incident response protocols, were managed. In one of them, a very limited number of personal information was involved without notable consequences. Proof of this is that we have not had any fines related to security breaches.
Security services
Thanks to our cybersecurity services unit, ElevenPaths, in 2018 we are celebrating five years of offering disruptive innovation to provide confidence and privacy to our digital lives and that of our customers.

Nowadays, we are exposed to increasingly frequent and sophisticated attacks that threaten not only the business, but also our reputation, privacy and trust. For this reason, we need to be increasingly receptive to cybersecurity measures and redefine our strategy towards cyber-resilience. With this goal, we dedicate all our experience and effort to the creation of innovative products, always managing to be one step ahead of our attackers. During the unit’s five year lifespan, we have combined the development of innovative patented technologies with the technologies of the main players in the market (partners) to provide unique solutions. We want to achieve a more secure future for people and companies, and therefore chose to be the provider of smart security services of the market (Intelligent MSSP).

Our global security services are designed to continuously improve the efficiency of our security infrastructure.

We are working to develop new security services and capabilities that help to protect businesses and people from threats and vulnerabilities present in the environments in which they operate. We collaborate and exchange information in real time about threats with the main bodies and entities such as the European Commission, the Cyber Threat Alliance (CTA), ECSO, EuroPol, Incibe, and the OAS.

In addition, we have ten security operations centres (SoCs) and a new Advanced Global Centre (Telefónica Advanced Global SOC-TAGS) that make it possible for us to face the threats and security problems with a global approach, but without distancing ourselves from our customers. At ElevenPaths we promote the entrepreneurial spirit through the investment in cybersecurity start-ups such as CounterCraft, 4IQ, BlueLive, LogTrust, IMBox, and Aise Devices. Thanks to these collaborations, partnerships and our own experience, we can offer a portfolio of comprehensive security solutions for the Internet of Things (IoT), identity and privacy, anti-fraud, industrial cybersecurity, safe mobility, digital exposure, risks management and regulatory compliance, with the goal of providing our customers with a solution adapted to their specific needs.

Wannacry
On 12 May 2017 an international ransomware cyberattack occurred, affecting more than 150 countries and countless companies and public bodies. In the case of Telefónica, this did not affect or compromise the telecommunications Network, the associated services, or the personal data of our customers in any way whatsoever.

However, during the initial hours, our internal systems of sensor bots detected that some PCs located in certain work places in Spain were potentially at risk of being contaminated by said ransomware and, for this reason, we immediately implemented the detection and response protocols for this type of security incident. These functioned in a robust and continuous manner from the beginning of the attack and during its most critical moments.

Our values guided each and every one of the decisions taken from the beginning, aware of what we are, together with our unwavering commitment to customer service and our inescapable social obligation of civic responsibility. For this reason, we were the first to raise the alarm and collaborated with government agencies and public bodies.
TRANSPARENCY

Aware of the importance of earning the complete confidence of our customers and users, during 2017 we worked to improve the Global Privacy Centre and implement local centres in the commercial web of the countries where we operate. To date, four privacy centres have been created in Spain, Brazil, Argentina and Colombia.

The goal of these centres is for our users to be able to find all the information about privacy, security, and the responsible use of technology in a simple and understandable manner.

We take advantage of these centres to bring our policies and processes closer to a more understandable language towards the customer; thus, for example, in Brazil we incorporated a video about the privacy centre, and in Colombia an explanatory infographic of the conditions of privacy.

In addition, we have published our second Report on Telecommunications Transparency as an exercise of essential transparency in a world where spaces of responsibility are shared when it comes to preserving and guaranteeing the rights of people, by companies, on the one hand, and by States, on the other (see chapter on ‘Human Rights’).
INTERNAL CONTROL
In order to meet the legal provisions of each country regarding Data Privacy, in our Annual Audit Plan of 2017 we carry out specific projects to ensure that these provisions are met, and to identify best practices in data protection.

In 2017, we continued with the personal information protection reviews, performing a total of 19 internal audits on this subject in the entire Group.

The most important aspects that have been reviewed are: the application of security measures in the processing of personal data; logical access control to them; assurance of the integrity of the information; the quality of the information; consent for the processing of the data; and the ability of the users to exercise their rights of access, rectification, cancellation and opposition of the information related to them.

TRAINING AND AWARENESS
In 2017, we continued with our global training plan on data protection. A total of 47,278 professionals completed the training this year, 85% more than in 2016. This represents 34% of all Group employees.

At a corporate level, we carried out different awareness initiatives, among which the publication, tutorials and security tips can be highlighted through emails, the Intranet and Yammer to all Group employees.

In addition, within our Annual Internal Audit Plan we focus on issues related to Cybersecurity and the Security on Information Technology Networks and Systems as a fundamental basis to protect the access and integrity of said elements, verifying that the logical access security is the correct one. These audits are based on the execution of technical work that encompasses, among other aspects, the logical security of information technology networks and systems, cybersecurity, the management of incidents, as well as the review of perimeter security controls. In this regard, during 2017 a total of 51 audits that provide coverage to the aforementioned subjects were performed.
At Telefónica Guatemala we participated in the online Security working group for children and adolescents with the goal of implementing measures for the online protection of children.

GUATEMALA
At Telefónica Guatemala we participated in the online Security working group for children and adolescents with the goal of implementing measures for the online protection of children.

PANAMA
At Telefónica Panama we are part of the Network of Allies for Childhood. The participating organisations have assumed compliance of ten commitments with the goal of working in favour of the rights of children.

PERU
At Telefónica Peru we are part of the Risks on the Internet for Boys, Girls, and Adolescents working group, in which UNODC, the Interior Ministry, the High Technology Crimes Division of the National Police of Peru, UNICEF, and InfoTrata also participate.

PROTECTION OF MINORS AND RESPONSIBLE USE OF TECHNOLOGY
The familiarity of the youngest at home with connected tools is nothing new. They are the clear example of how our way of living, interacting, learning, etc. has changed. This also extends to the way adults live, our way of working, sharing information, or consuming entertainment.

With the aim of promoting a safe environment on the Internet and raising awareness in society about the importance of learning to take full advantage of the digital tools in our day-to-day lives, we have defined a global strategy based on the promotion of the responsible and smart use of technology in all areas of our lives, but with special emphasis on the protection of a more vulnerable group such as children and young people.

Our lines of action and commitments to the protection of minors on the Network, and the promotion of the responsible use of technology, can be grouped into six key lines of work:

- **Alliances with stakeholders**
- **Content blocking**
- **The audiovisual environment**
- **Products and services**
- **Work with providers**
- **Education and awareness**

**Alliances with stakeholders**
Ensuring a more secure Network is a task that we cannot address alone, and that is why at Telefónica, we work together with sectoral and civil society allies with the goal of making sure that children and young people are aware that the Internet is an open window full of opportunities, but that it is also important to know that there are risks that they must learn to manage.

Along these lines, we would like to underline our collaboration with:

- **State Security Forces and Bodies**, as well as the support for different national lines of crime reporting (Children’s Team, ASI, Safe on the Internet, Safernet, Te Protejo, Centre for Child Protection on the Internet, among others).

In Nicaragua we are part of the National Working Council for the Safe Use of the Internet led by the Vice-president of the Republic through the Nicaraguan Council of Science and Technology, in which the Ministry of Education, the Nicaraguan Chamber of Telecommunications and the Internet, private companies, universities, and NGOs also participate.

**EL SALVADOR**
In El Salvador we are part of the National Council for the Protection of Childhood and Adolescence (CONNA for its Spanish original) working group to enable a complaints line for boys and girls to report violations of their rights.

In addition, since 2015, we signed the Charter of Commitment with UNICEF and the GSMA to promote actions for the protection of minors in the online world, as well as actively participating in the committee that monitors what is agreed in said letter.

**NICARAGUA**
In Nicaragua we are part of the National Working Council for the Safe Use of the Internet led by the Vice-president of the Republic through the Nicaraguan Council of Science and Technology, in which the Ministry of Education, the Nicaraguan Chamber of Telecommunications and the Internet, private companies, universities, and NGOs also participate.

**COLOMBIA**
We are part of the Te Protejo working group, a working council whose goal is to promote initiatives regarding the protection of children and young people in the Network.
Furthermore, we participate in the following alliances with the goal of globally promoting the exchange of best practices and the promotion of specific actions regarding the correct use of the Internet:

- Alliance with the GSMA to fight against content involving sexual abuse of minors.
- ICT Coalition.
- Alliance for the better protection of minors online.

At a local level, we also participate in numerous working groups that promote the responsible and smart use of technology among children.

**Content blocking**

To proactively fight against the contents and images of sexual abuse of minors on the Network, at Telefónica we proceed to block these materials following the guidelines and lists provided by the Internet Watch Foundation in the following countries: Chile, Costa Rica, Ecuador, El Salvador, Spain, Guatemala, Nicaragua, Mexico, Panama, Peru, the United Kingdom, Uruguay and Venezuela. In Telefónica Colombia, we do the same thing through the MINTIC and the DIJIN.

**The audiovisual environment**

Children and adolescents increasingly use our products and services in general, and the specific audiovisual contents, in a more intensive manner. Screens also constitute an essential part of their personal, social and civic development, which is why at Movistar+ we believe the following to be fundamental:

- Ensuring that our programming protects children from potentially inappropriate content.
- Establishing the tools needed to make good use of television, guaranteeing that parents have effective technical means of exercising their responsibility over the programmes their children watch.
- The promotion of digital literacy among minors and their families to take advantage of the potential of audiovisual media and make them aware of the need for a responsible and smart consumption and leisurely use.

In this sense, in our different operations we have the following initiatives:

- Labelling of content by age or type of content.
- Parental controls, parental pin and purchase pin in the device that allow the customer to block channels and content to minors on demand.
- The specific content for adults is presented in a section that is separate from the other contents, and it is necessary to introduce a special pin to enable them.
- Information about the responsible use of TV or audiovisual content on TV itself and on the commercial web.
- Awareness-raising activities on the responsible use of screens.

**Techno-addiction** is a reality that affects the new generations, and it is therefore especially necessary to inform families, educators and minors themselves of the importance of using the Internet and technology in a healthy and responsible manner.
**Products and services**

Although we really think that nothing can replace the mediating job of an adult when talking about education in the responsible use of digital tools, we will always have the support of technology when this is not possible. As a result, we wager on promoting and developing products and services that promote the responsible and safe use of the Network and connected devices:

- **Parental controls:** Movistar Protege (Spain), Vivo Filhos Online (Brazil), Parental Control (United Kingdom).
- **Security solutions with parental control functionality:** Movistar Shield (Colombia, Ecuador, El Salvador, Peru, Uruguay), Multi-device Security (Argentina, Chile), Mcfee Total Security (Argentina, Chile, Peru), and Mcfee Security Centre (Colombia).
- **Other services** (anti-viruses, personalised packs...): Gurú, O2 Protect (Germany), Vivo Familia Online (Brazil).

**Working together with our providers**

Together with our providers, we study the possibility of promoting basic protection parameters for minors to ensure the best possible development in children. Some of the initiatives we are working on are:

- **Security from the design:** from the area of innovation in ecosystems we work closely with the main manufacturers of handsets, as well as with the operating systems, to include functionalities for the protection of minors that are part of the operating system itself.
- **Safety through operating systems:** We are fully committed to our customers’ security and privacy. As a result, we work with the principal players in the industry to improve the level of security updates in the handsets our customers use, as well as to improve transparency on the type of data that can be shared through mobile handsets.
- **Collaboration in the development and implementation of initiatives that promote the responsible use of technology and the protection of the user:** we maintain fluid communication with the responsible parties of products of the different digital ecosystems to improve the use of these by customers and to promote the correct use of technology.

**Education and awareness initiatives**

The responsible and smart use of the Internet and technology is present today as a challenge for everyone, and not only for children. The world of social networks, mobile applications, smart devices and virtual reality... evolves so fast that it can be difficult to keep up to speed. However, we are aware of this reality and therefore are committed to the development of training and awareness initiatives for everyone - initiatives that promote coexistence in an increasingly digital society.

The [dialogando.com](http://dialogando.com) portal is an example of this, and the initiative has already been implemented in 15 countries of the Telefónica Group: Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Spain, Guatemala, Mexico, Nicaragua, Panama, Peru, Uruguay and Venezuela.

On the web, a committee of experts reports through articles, videos, campaigns, interviews, etc. on the aspects that currently worry society the most in order to grow successfully and without fear as good digital citizens.
In addition, we have carried out different initiatives, among which the following stand out:

**LGTBfóbico School Bullying Workshop:** Organised by Dialogando in the Telefónica FlagShipStore Madrid, its goal was to raise awareness in society about the new forms of bullying that are on the rise. Professionals from different areas who are fighting against cyberbullying participated, and attendees were informed about the keys to understand it and deal with it, as well as the impact that the use of information and communications technologies can have on school co-existence.

**The Movistar #RodamosJuntos initiative communications drive:** An awareness campaign with the goal of reminding us of the importance of mutual respect between cyclists and drivers on the road, which Dialogando supported with sensitisation content on the responsible use of mobile phones while driving and when riding a bicycle.

**Publication of the “WhatsApps, video games, and mutants heads” children’s story. It can also happen to you”:** Aimed at children between the ages of 4 and 8. At Dialogando we seek to promote a good education in the use of connected technologies; both the regulations and limits are as important as the accompaniment and monitoring of the digital activities of children by adults. An accompaniment which is also desired by minors seeking the complicity of their parents in the use of digital devices. This is an opportunity to strengthen the relationship and communication between parents and children.

**#ContraseñaSegura awareness campaign - 8 keys to guard the entrance into your digital life:** In collaboration with Pantallas Amigas (Friendly Screens). The activity, which is part of the “Pilar and her cell phone” educational programme, offers children basic guidelines for defining a robust password for Internet services.

**Ciberexpert@ project:** Its goal is to provide a higher digital education for families and to provide a positive vision of the safe and responsible use of the Internet through different awareness activities and talks in schools, in addition to a view of the risks and problems that minors can face on the Network in a real manner. Created by the Citizen Participation Unit of the National Police, it has the support of Telefónica and the Cybervolunteers Foundation.

---

**2017 Milestones**

- Local Privacy Centres in 4 countries.
- Voluntary mediation system for Claims regarding the Data Protection in Telefónica Spain.
- 85% more trained individuals in Privacy and Security compared with 2016.
- Implementation of Dialogando in 15 countries.

---

**2018 Targets**

- To extend the local Privacy Centres.
- To update the Global Privacy Policy.
- To organise awareness campaigns on responsible use with providers.
- To develop tools to promote the proper use of audiovisual content by minors.
Good practices

At Movistar Argentina, during 2017 we launched the safe and responsible use technology programme, “Choose to take care of yourself”, and the “Dialogando” web platform, a space of information and reflection on the use of ICTs. The inauguration of the portal was supported by the launch of the “Choose to take care of yourself like you take care of your mobile phone” road safety campaign which sought to raise awareness about the risks of talking, sending messages, or chatting while driving. Said campaign received the award from the Let’s Strive For Life organisation.

During the second part of the year, work was done on a campaign for the prevention of Grooming or sexual harassment to minors through the Internet, the “Love Story” campaign, driven together with the Digital Lighthouse Civil Association, which registered more than five million visualisations in its central spot, and received an award from Argentina CyberSafe. This initiative was complemented by face-to-face talks for Company employees, through the Telefónica Foundation for the general public and schools.

At Telefónica Germany we published a secure Internet guide for children on the occasion of “Children’s Day”, with the collaboration of Deutschen Kinderhilfswerk, FSM (Freiwillige Selbstkontrolle Multimedia Dienstanbieter) and FragFINN e.V. This guide offers minors and their parents assistance with better media literacy and greater security in the digital world. Furthermore, the brochure provides useful information on how children can benefit from the Internet, and what they have to take into account in the event of receiving unwanted emails, advertising, or viruses. In addition, the Internet Guide contains tips for the correct use of their smartphone.

We carried out “Safe Internet Week Workshops”, with a double objective. On the one hand, we wanted to raise awareness about the responsible use of technology by presenting the Dialogando portal, and, on the other hand, to address the importance of using the Internet in a more conscious and positive manner, highlighting the responsibility that each user has when he/she publishes a comment, a post, or gives a ‘like’ on any social network.

In addition, on Safe Internet Day, Vivo Brazil participated in an event organised by SaferNet in which large companies presented the initiatives that they are working on regarding the responsible use of technology. Similarly, throughout the week debates were held with employees on the topics of greatest interest in the use of the Network by children and adolescents, with the support of Safernet Brazil.

In Argentina, we launched the safe and responsible use technology programme, “Choose to take care of yourself”, and the “Dialogando” web platform, a space of information and reflection on the use of ICTs. The inauguration of the portal was supported by the launch of the “Choose to take care of yourself like you take care of your mobile phone” road safety campaign which sought to raise awareness about the risks of talking, sending messages, or chatting while driving. Said campaign received the award from the Let’s Strive For Life organisation.
Good practices

NICARAGUA

The musical duet Nina and Sebastian accompanied the Telefónica Foundation in the presentation of the Dialogando website with the goal of sensitising children and young people with messages on the correct use of the Internet. Their participation was shared with great success on social networks. Similarly, the musicians promoted the positive use of technology in their concerts, launching messages between songs and inviting the young people to enjoy the Internet in a healthy and responsible way.

ECUADOR

At Telefónica Ecuador we have organised spaces for dialogue in schools and universities on the occasion of the launch of the responsible use platform of the Dialogando technology. In the workshops, the following subjects were addressed, among others:

- Inter-school Recycling of mobile telephones campaign: E-waste lecture.
- Environmental training in electrical and electronic waste material.
- Training in the responsible use of technology: correctly learning the management of the digital identity, privacy, social networks...
- Smart cities and climate change.

SPAIN

We carried out a workshop on the responsible use of the “#DialogandoConectados EPIC WIN or EPIC FAIL?” technology which, together with the support of the Telefónica Foundation, was organised in Madrid with the goal of discussing and analysing with experts from many areas the issues that most worry society about the use we are giving to the Internet and connected devices in our day-to-day lives: do we know how to take advantage of the full potential offered by technology? Are we capable of transferring the basic rules of education and respect to the digital world? How can we prevent cases of gender cyberviolence or school cyberbullying?

Furthermore, Dialogando also presented the “Ten epic fails of the Spanish” study with the goal of confirming that education and a deep knowledge of the networks are necessary to be able to take advantage of the Internet without risks.

COLOMBIA

In Colombia, we participated in “Connected to Protect Them”, an encounter organised as part of the activities of the Te Protejo partners network’s virtual complaint channel, which served as backdrop for presenting the We Protect model against the sexual exploitation of boys, girls and adolescents in the country, also seeking to install a commitment between the government, the authorities, companies and NGOs for its immediate implementation in the country.

We Protect is a tool that enables comprehensive and coordinated responses among the countries to prevent, mitigate and fight the online sexual exploitation of boys, girls and adolescents.
We launched the “Love Story” campaign which seeks to raise awareness and prevent children and adolescents from accepting strangers in their social networks, preventing them from being victims of abuse such as bullying, sexting, or grooming. This campaign also won the “Silver Sun” award in the TV and Consumer Electronics Film category during the 32nd edition of the Ibero-American Festival of Advertising Communication.

Also during 2017, at Telefónica Mexico, we presented the “Privacy Adventure” video game, available free of charge for Android and iOS devices, which promotes matters of privacy and security for the use of tablets and mobile phones, such as blocking, labelling, instant messaging, downloads, geolocation, Bluetooth, and wifi, raising the complexity in each level so that children and adults adopt good habits regarding the responsible use of technology.

At Telefónica Panama, we launched the #YoElijo (I Choose) campaign on the responsible use of mobile phones, aimed at promoting a culture of responsible use. This campaign invites us to reflect on the small things that we can do to avoid risks and help build a better society. The campaign was based on four key tips:
1. #YoElijo not to accept strangers on social networks.
2. #YoElijo not to chat while driving.
3. #YoElijo not to perform acts of cyberbullying.
4. #YoElijo not to share crude images.
At O2 United Kingdom we collaborated with the leading charity organisation for children in the country, the NSPCC, with the goal of helping parents to understand the online lives of their children and how to keep them safe. The project, visible through a section of the commercial website, includes initiatives for raising awareness, counselling and training as well as the NET AWARE web, a site on which advice and recommendations on the responsible use of technology can be found. In addition, O2 United Kingdom offers a toll-free online security helpline (0808 800 5002), and a specific chat to answer questions on responsible use, which gives parents access to online security experts to whom advice about social networks, and the configuration of privacy and parental control can be requested seven days a week.

Furthermore, families who wish to can subscribe to an email service for obtaining information, advice and activities sent directly to their inboxes, which will help them to maintain regular conversations with their children about how to stay safe on the Internet.

We organised workshops on our digital footprint and cyberbullying. In them, we sought to create on-site spaces with students (children and adolescents), teachers and parents to transmit practical contents and tips on the proper use of technology. The interesting thing about these workshops is that debates are held about real situations and how they affect professionals, young people and relatives.

We launched a campaign on the responsible use of mobile phones in the car. Thus, we published in magazines and newspapers, as well as on social networks, several graphic pieces with the following "claim": A voice message can also cause an accident. Don't use your mobile phone while driving. The graphics were awarded as the best advertisement in the press of the year at the Advertising Campaigns Festival.