6

Commitment to the customer

- Commitment to our customers
- Digital trust

Commitment to our customers _

"We're expanding the relationship with our customers, seeking to increase their satisfaction, and opening up new possibilities to them so that they can enrich their digital lives with us"

José María Álvarez-Pallete
Chairman & CEO

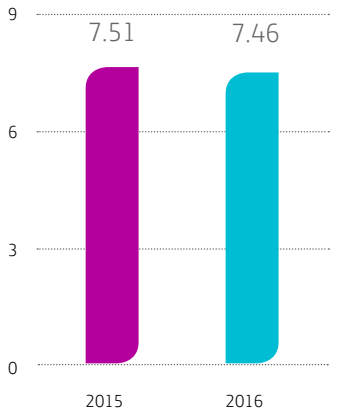
Today any company will state that their strategy is focused on listening and responding to the demands of their customers. When it comes to the connectivity service and other value-added digital services, the focus on the customer is not optional, it is a necessity. The markets in which Telefónica operates are highly competitive, and in the digital field, our customers' expectations have multiplied. We adapt our customer strategy to the markets, but we are aware of the importance of maintaining common standards aligned with the values of integrity, commitment and transparency which characterise our company culture.

HOW DOES IT WORK?

Customer experience is affected by a combination of factors and activities within the Company, and thus becomes one of the most important objectives across the whole organisation. Taking just the case of the mobile service for example, customer experience is influenced by elements as diverse as Network coverage, the quality and speed of the connection, the digitisation of the experience, the simplicity and the transparency with which we continuously communicate the terms and conditions of our service, the friendliness and efficiency of our call centres, effective management on the part of our suppliers, etc. All this requires a holistic management of what the customer expects from us and some shared incentives.

At Telefónica, each operator uses multiple indicators to measure the customer experience (Churn, NPS, customer care satisfaction surveys, response times, etc.). However, there is one that influences the remuneration of all of the Company's employees and that reflects therefore the significant and transversal nature of customer experience for the Group.

OUR CSI



In 2015 it was established that *50% of the variable remuneration* of Group employees would be directly linked to customer satisfaction levels

We are currently in the number 1 position for our sector according to the Customer Satisfaction Index (CSI) in 10 of our 17 markets.

Governance

The quality or customer experience plans are strategic for all operators within the Group and they are reported to the highest level in the executive committees of each company.

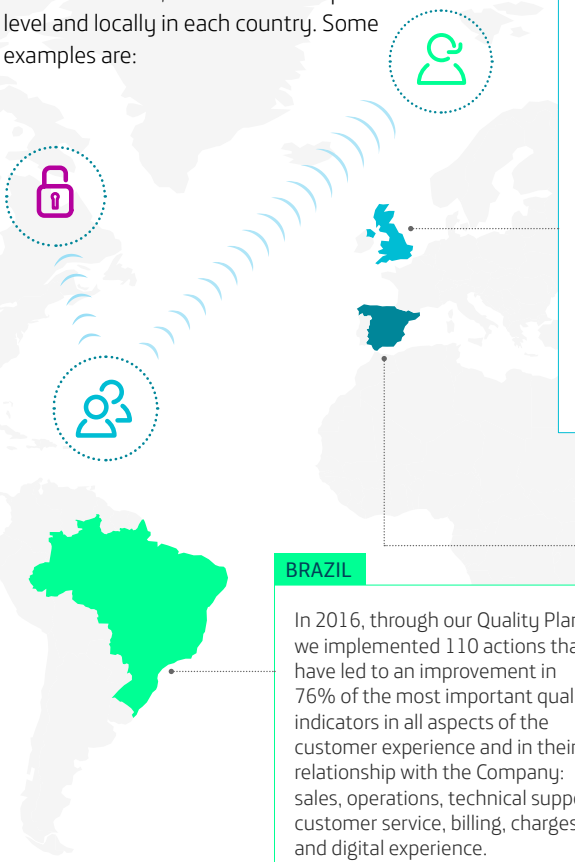
In addition, at Group level, the Board of Directors has a specific Committee dedicated to Quality which meets quarterly to review the development of the different countries' plans and the CSI globally.

Finally, Telefónica incorporates into its customer strategy a firm commitment to the right to privacy and control of personal data. This strategy is led by the Chief Data Officer, at global level, who forms part of the Group's Executive Committee.

G4-PR5

Initiatives

In 2016, multiple initiatives aimed at improving the customer experience were carried out, both at the Group level and locally in each country. Some examples are:



UNITED KINGDOM

At Telefónica UK we are in a continuous process of innovation. Through digitisation and personalisation, we ensure that our customers are more satisfied and loyal; we reduce Churn, which enables us to increase value for our customers. Our omni-channel is the best in the mobile sector in the country. By way of example, in 2016 we implemented a new development that allows us to deliver orders placed before midnight the following day. In addition, we are building a customer experience engine based on data, which will lead to even greater personalisation.

In 2016, Telefónica UK received several acknowledgements thanks to our customer service and operational experience:

- Branded Number 1 in Customer Service by the regulator Ofcom for the seventh consecutive year
- Web page of the year, for the third consecutive year
- Best "Pay As You Go Network" in the Switch Mobile Awards 2017
- UK Business Award for best customer-focused organisation
- Best retail network in the Mobile News 2016 Awards
- Best customer service in the Mobile Choice Consumer Awards 2016
- British Franchise Association Customer Focus Awards 2016

GLOBAL

E2E digitisation

As part of our commitment to our customers, we are implementing a global digitisation strategy through provision of a real time omni-channel experience, while at the same time adjusting our processes to comply with Lean methodology. This means that we are transforming all the processes and core systems that support the customer value chain (how we launch our products, how to sell and bill them, how we resolve requests and problems, how we consolidate them and even how we finalise the service), generating new digital skills.

The Full Stack and Satellite projects are being implemented in 15 markets simultaneously. 2017 is a key year for us as we have set ourselves the goal of migrating a significant number of our customers (from 13 to 42%) to these platforms and increasing our level of E2E digitisation of processes from 50% to 67%, almost doubling it by 2019.

BRAZIL

In 2016, through our Quality Plan, we implemented 110 actions that have led to an improvement in 76% of the most important quality indicators in all aspects of the customer experience and in their relationship with the Company: sales, operations, technical support, customer service, billing, charges and digital experience.

We have also expanded the digital channels available (our application has reached more than 40 million contacts in December 2016 and the virtual assistant, *Vivi*, is now capable of responding to more than 90% of questions thanks to artificial intelligence). We perform internal awareness actions such as awarding the Quality Value Trophy to recognise initiatives that have contributed to the transformation of customer experience. In 2016, the year in which we achieved a score of 7.27 (on a scale of 1 to 10) in the Customer Satisfaction Index (CSI), more than 250 projects were registered.

SPAIN

In Movistar Spain we have greatly improved understanding and accessibility of our privacy and security conditions, through the implementation of a Privacy Centre which explains Telefónica's policy. Here, the terms and conditions of the contracts we offer can be found, along with how data collected by the Company is used.

110

actions implemented in 2016, through our Quality Plan

MAJOR CUSTOMERS

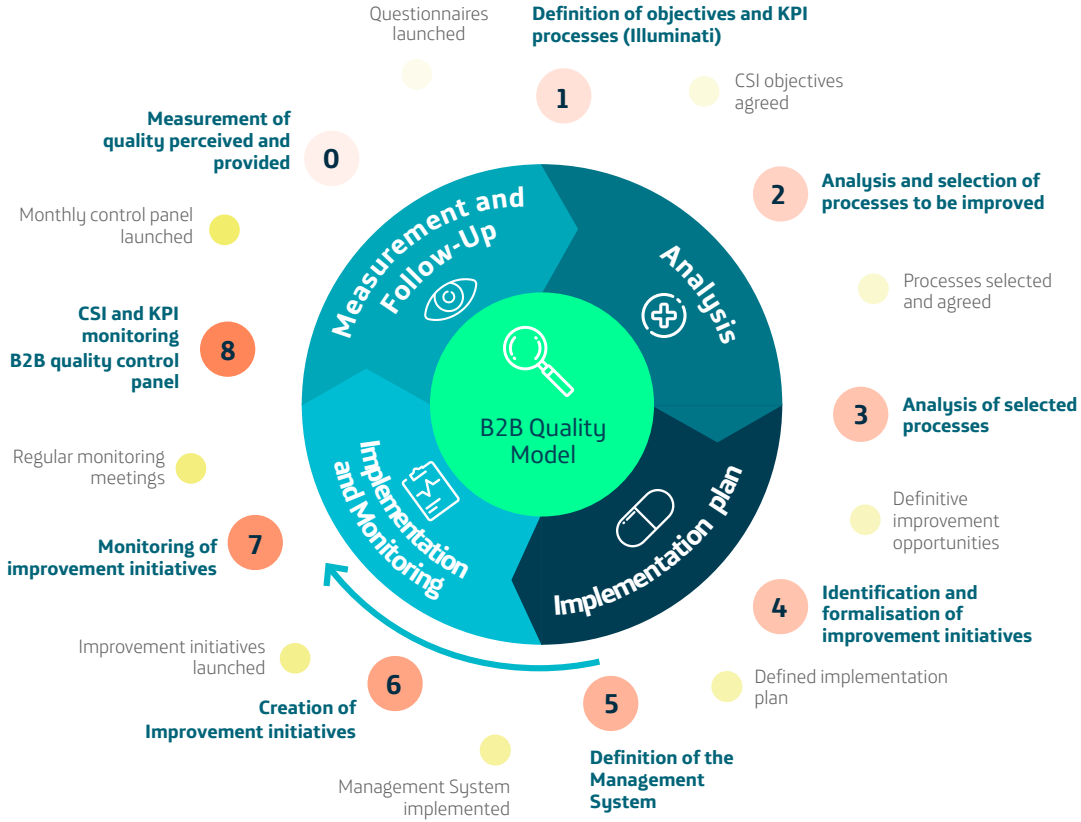
Our Telefónica Business Solutions division is responsible for providing comprehensive communication solutions for the B2B market and for managing commercial operations for businesses (multinationals, large companies and SMEs), wholesalers and Telefónica Group roaming.

CUSTOMER LIFE CYCLE

We support our customers in an agile, quick and efficient way. To do so, we offer experiences through an integrated operational improvement programme which is designed to encompass all the different types of interaction that a customer has with our Company throughout their life cycle.

With the objective of offering our customers a distinctive operating model where technology and the use of information make a difference, we are working on a complete transformation project aimed at developing the way we interact with our B2B customers, the products and services we offer and our internal departments.

This operating model is based on three pillars:



1. Optimisation of processes

We define and implement improvements in processes, systems, personnel, KPIs and the organisation itself. To do this, we have in place our own Quality Model that sustains the continuously improving procedure.

2. Optimum coordination of functional areas

We classify and map key interactions with our customers, allowing us to identify the relevant points of contact and, consequently, to work on improving them using the Lean methodology of redesigning processes.

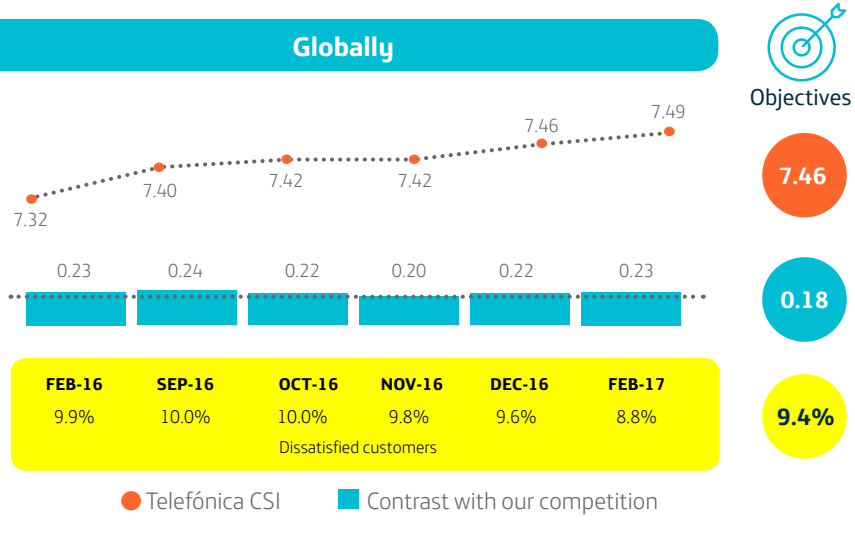
3. Digitising daily customer interactions

We incorporate intelligent automation of processes and provide intelligence to facilitate decision-making. In addition, we are working to integrate the customers' and the Company's points of view with the purpose of achieving an unbeatable experience.

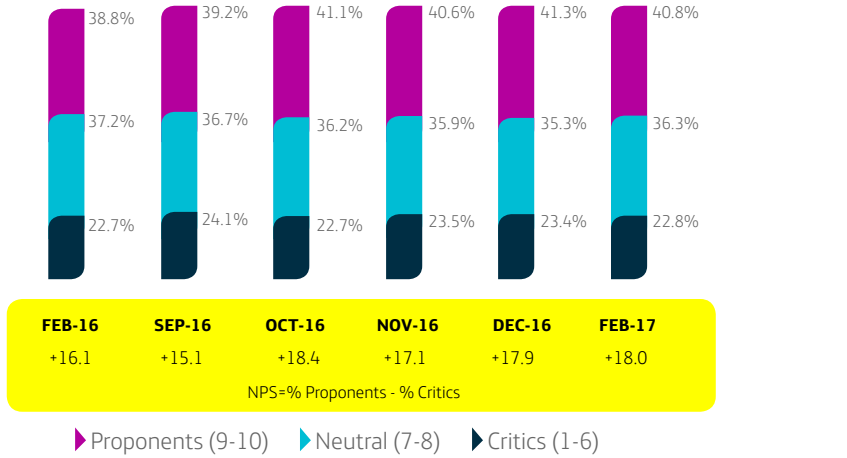
IN THE B2B SECTOR WE LEAD IN SATISFACTION AND IN NPS

In February 2017, we achieved a global B2B CSI of 7.49, the highest value achieved so far during the period measured. In addition, the NPS remains very positive, reaching a value of +18%, with 40.8% of our proponents in this sector.

CSI and the contrast with our competition



Distribution of proponents and critics



*** Based on a question of recommendation**

BEST PRACTICES

IN MULTINATIONAL COMPANIES AND WHOLESALERS THE VOICE OF THE CUSTOMER IS HEARD

With implementation of the Voice of the Customer (VoC) programme, the aim is to continuously improve interaction between multinational and wholesale customers and the services offered by Telefónica Business Solutions. Through the programme, efficient and effective responses can be provided according to customer needs and, thus, improve their experience with our Company.

We systematically document customer feedback at all levels, spreading the Voice of the Customer throughout the organisation so that it provides the main input for the content of improvement plans and it creates "customer records" when cross-referencing the information on quality provided with that on quality perceived.

The main objectives of this project are to optimise the product and services offered to customers, to improve customer satisfaction, reduce Churn and improve the working environment for employees.

BEST PRACTICES

OPERATIONAL CUSTOMER SERVICE MODEL

At the end of 2015, Brazil initiated transformation of its corporate sector Service Model with the aim of improving customer satisfaction and streamlining operations.

The Global Telefónica Business Solutions team has been supporting the Brazilian operator in this transformation ever since. It has created a more personalised Service Model, with greater E2E vision and integration of Corporate and Top VIP operations.

The results of the month of February 2017 reached a value of 7.47 (+0.32 p.p. YoY) and a reduction of customer service costs (-5%). The next challenges for 2017 are to work on fixed-mobile convergence of Post Sales customer service and on operational integration with Vivo2.

GLOBAL OPERATING SME TECHNICAL SUPPORT MODEL

A new Global Technical Support Model was defined in 2016 with the aim of transforming this process to suit SME customers.

The project started with implementation in the Spanish operation, which led to improvements in the front line of service of +0.72 p.p. in satisfaction and reduced the volume of dissatisfied customers by 60%. In addition, the improvements observed in the second line of service were +0.8 p.p in satisfaction and a reduction of 63.75% of dissatisfied customers. This experience was documented and is being replicated across all the convergent operators of the Group (Argentina, Brazil, Chile, Colombia and Peru).

63.75%
reduction in dissatisfied customers

BI_EN (SALESFORCE) PLATFORM

For the last two years, we have been working on the definition and implementation of an architectural system for the B2B sector, in all operators and global areas, in order to cover all the needs of our business. In this context, we have selected Salesforce as a tool for the management of the macro-processes of marketing, pre-sales and sales, integrating them with different transactional tools for the management of orders, provisioning and billing, and with various Fullstack projects and global digital service platforms.

With Salesforce we have developed what we call BI_EN (Business Intelligence for *empresas y negocios* - companies and businesses), constituting the first step of this transformation and including:

- 360º customer vision for all countries, products and channels.
- "Out of the box" processes by applying best practices and standardised processes (adapted to the reality of each operation)
- A unique catalogue with both a local and global vision
- Sharing of global data instantly through a homogeneous information structure
- Scalability and efficiency thanks to the features developed in unique effort for all countries and maintained by an internal global centre of excellence (in Global IT).
- Easy incorporation of new channels and areas: "opex based".
- Facility for establishing shared capabilities.

We have already implemented BI_EN in 12 countries and in the global B2B areas, reaching more than 5,000 users, 476,000 active customers, and reflecting 2,000 billion euros of opportunities gained in 2016.

476,000
active customers
on the BI_EN platform

Digital trust_

INTRODUCTION

We live in a world defined by connection and data. In turn, society is becoming increasingly concerned with how personal data is protected and kept safe. According to an Accenture survey from 2016 of 28,000 consumers in 28 countries on the use of technology, 47% of those surveyed expressed concern for privacy and security (Accenture's 2016 Digital Consumer Survey).

Regulations also reflect these concerns; in May 2018, a European law on privacy will come into effect - the European Regulation on the Protection of Personal Data. We feel that this is a significant step forward in the fundamental right to privacy, offering EU citizens greater control over their personal data. The goals of the GDPR match Telefónica's strategy to provide customers with privacy, transparency and control over their data.

In Latin America, regulators are also increasing measures to protect users. For example, in January 2017, the Peruvian Legislative Decree to create the National Authority on Transparency and Access to Public Information was published, strengthening the Personal Data Protection Regime and the regulation of the Management of Interests.

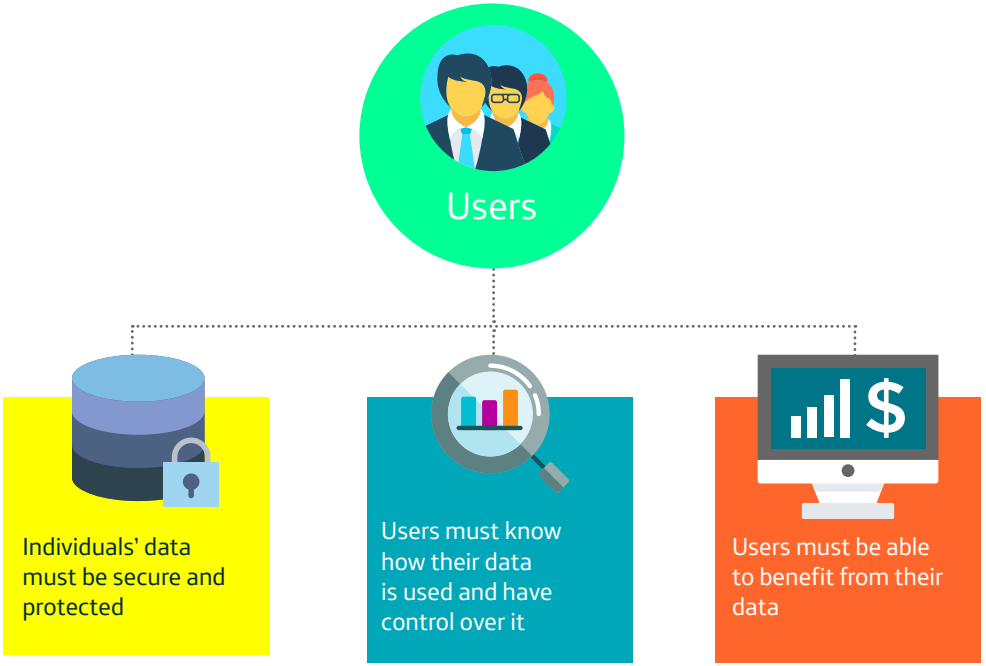
At Telefónica, we share this concern. We know that digital trust must be a key element of our promise to customers, and that we need to go beyond simply fulfilling current legislation. As a result, we are committed to a series of basic principles:

1. **Individuals' data mast be protected and secure:**
   Security and data privacy are the foundation of our business, and must be our principal concern when designing our services or collaborating with third parties.

2. **Users must know how their data is used and have control over it:**
   Customers must be able to easily access their data and understand how it is used. We need to provide simple tools that allow for data decision management. Transparency throughout the service life cycle is a basic principle that defines our relationships with customers and partners.

3. **Users must be able to benefit from their data:**
   With the consent of the customer, we will put their data to work to make our services simpler and more useful, with the goal of personalising their experiences or of offering them new services that fit their profile. We will innovate in our collaboration with other companies to offer services based on this data, and to generate value for them and for society.

In addition, privacy and cybersecurity are two of the aspects included in the Company risk management model. For further information, see the chapter on 'Identifying and managing risks'.



GOVERNANCE OF DIGITAL TRUST

Digital Trust (the protection of the right to privacy, data security and information, the protection of the right to freedom of expression), together with the protection of human rights in general, are issues which fall under the responsibility of the Board of Directors, through the Regulation 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.

At Telefónica, we also have a Chief Data Officer, who is part of the Executive Committee of the Group. Their principal objective is to define the Company's global strategy on data, or, in other words, on the cognitive intelligence services associated with Big Data. This strategic function ensures that data privacy and security are key elements considered in all our services, no matter where we are.

We also have a Chief Privacy Officer who ensures that the Privacy Policy is adhered to in any operation we are a part of. Furthermore, we have a Data Privacy Officer for each operation, who ensures that our actions on a local level comply with our internal and external regulations.
The Privacy Committee is the body in charge of coordinating all the actions to ensure data protection. In 2016, we held regional meetings where, among other issues, we discussed international transfers and adaptatation to the new Regulation 2016/679 on the protection of the treatment of personal data.

The Global Security Director is the head of the area of security for the Telefónica Group, answering directly to the CEO. The Director's area of responsibility includes protection of the Group's assets, both in vertical organisation (including business units) and in its transversal dimension (applicable across all three of its platforms): infrastructure and Network assets, information technologies and products and services.

Within the security organisation there are Security Officers at both global and local levels. Their obligations and responsibilities are defined and coordinated by the Global Security Director. Each company in the Telefónica Group has one of these Security Officers assigned to it, depending on what is the most efficient and effective solution in each case.

For coordination purposes, there is a Global Security Committee which meets every eight weeks and is presided over by the Global Security Director. Other participants include Security Officers from certain functions, companies, or territories, as well as those areas that are considered necessary at any given time. This Committee is responsible for supervising the Global Strategic Security Plan and the series of activities aimed at promoting specific action plans. Relevant security information for the Group, including both exterior and interior factors, is also discussed by the Committee,.

3 Committee meetings were held in 2016, in which a series of different issues were addressed, such as new challenges in data protection, the impact of the NIS directive, global management of physical security or criteria for security in the cloud.

PRIVACY BY DESIGN

We work on including customer privacy 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, through which we take into account not only the guarantees provided by the applicable legislation on the subject, but also the customers' expectations with regard to privacy when using our products and services.

So, for example, in our fourth platform, from the very beginning experts in data protection have worked on defining customers' experience with the Company and on proposals for controlling and managing data. They have incorporated new, more intuitive, easy-to-understand mechanisms for transparency and informed consent, promoting the generation of a safe space which is open to new proposals and where, for example, customers can decide if they want to share the knowledge generated using their data with others in order to enrich their digital experiences.

INTERNAL REGULATORY FRAMEWORK

Our commitment to privacy, security and freedom of expression are included in different sections of our Responsible Business Principles, which were re-formulated (among other things) to emphasise the importance that these rights have for us.

The principle of "Respect for the Right to Privacy and Freedom of Expression" included in our Responsible Business Principles is applied through policies and internal regulations that establish common guidelines for all of our companies.

In order to guarantee that our customers' data and services are as safe as they need to be, we are reviewing our regulatory framework, bringing it up to speed with the latest international standards so as to adapt to current challenges and needs in privacy and global security.

Transparency and fluid communication with our customers or users are priorities, enabling us to make sure that our customers feel comfortable using our services. We ensure that they have clear, simple information on how we use their data, and that they have the option of communicating with us directly and easily if they have any doubts.

Privacy

- **Global Privacy Policy**
  Approved by the Board of Directors, this Policy establishes the guidelines that all the companies in the Group must follow in order to protect the privacy of our customers and all the stakeholders that entrust us with their data. Soon, an online policy will be approved, which will be updated in accordance with Company strategy and centred on the trust we need to generate among users.

Freedom of Expression

- **Global Procedure for dealing with requests from the competent authorities**
  Defines the procedure for attending to requests by the authorities in the countries where we operate, guaranteeing a response that respects the privacy and security of these requests.

Information Technology

- **Regulations on Basic Controls for Information Technology**

Global Security

- **Global Security Policy**
  Updated in 2016. This new version, specifies the principles of legality, efficiency, co-responsibility, cooperation and coordination that structure the security activities within the Group. It also establishes the principal security roles within the organisation and establishes the basis of the normative framework.
- **Global Security Regulations (pending approval)**
  Currently being developed and/or updated, with specific regulations on:
  - Classification of Information
  - Incident Management
  - Business Continuity
  - Change Management
  - Risk Analysis
  - Supply Chain Security
  - Access Control
  - Security of the Platform
  - Security of People
  - Physical Security
  - Security of Communications
  - Asset Management
  - Security in the Development Cycle
  - Cybersecurity
  - Review and Compliance

Global Privacy Centre:
A public point of reference available on the different telefónica.com sites for all the countries where we operate, which describes our position and our way of showing respect for privacy and security. Stakeholders have expressed great acceptance of this Centre, with our page having received 8,889 visitors from the time of its launch, in August 2016, to February 2017.

Movistar Spain Privacy Centre: A public point of reference in which we offer easy-to-find information on issues related to privacy and security in Movistar, including options regarding how we collect, use and share users' information. The total number of visits received from December 2016 to March 2017 was 6,066. We are working to ensure that all of our markets apply the same measures for transparency and ease of access.

Responsible Business Channel: This channel, managed on a global level, establishes a stakeholder communication system that is directly associated with our Responsible Business Policy and, more specifically, our commitment to protect and promote human rights in our activities.

HOW WE INFORM OUR CUSTOMERS IN THE UNITED KINGDOM ABOUT PRIVACY

FURTHER INFORMATION

INTERNAL TRAINING

In 2016, we continued with our global training plan on data protection. More than 25,265 employees were trained in data protection, information security and awareness. The breakdown by region is:

- **Telefónica Europe**: 20,231 employees received training in privacy and data protection.
- **Telefónica Latin America:** 5,034 received either in-person or online training in privacy, data protection, security and confidentiality.

TABLE OF CERTIFICATIONS

Our Global Security Committee supervises the Group's Security Certifications in order to develop, implement and maintain the Company's system for managing certifications.

As an example, below are some of the certifications involving security processes held within our Group:

- ISO27001: Managing Information Security
- Systems for managing occupational health and safety
- PCI\DSS: Data Security Standard for the Prepaid Card Industry
- 22301: Business Continuity Regulation
- Data Centre TIER IV certification: GOLD certification for Operational Sustainability, Design and construction.

AUDITS

In order to meet each country's legal provisions on Data Privacy, our Annual Audit Plan encompasses specific projects that ensure compliance with these provisions, and identify best practices in data protection. In 2016 we continued to conduct reviews of personal data protection, performing a total of 21 internal audits on this subject.

The most important aspects to be reviewed were: the application of security measures in the processing of personal data, control of access thereto, the quality of the information, consent for the processing of data and the possibility for the affected parties to exercise their rights of access, rectification, cancellation and opposition.

In addition, within our Annual Audit Plan we focus on issues related to Cybersecurity, a fundamental basis for protecting the perimeter that guards access to and consistency of our customers' information and data. These audits are based on the carrying out of so-called penetration tests, applying "Black Box" and "White Box" techniques based on the OSSTMM, CVSS and OWASP standards.

These audits are performed every 18 months on all the public IP addresses of the Group's operators, as well as on specific products and services to improve their level of resistance to cyberattacks, if appropriate. In 2016 we conducted 84 cybersecurity audits on all our operators' Networks, Systems, Products and Services.

25,265 employees have been trained in data *protection*, information *security* and *raising awareness*

84 *Cybersecurity* audits

OPEN PROCEEDINGS AND SANCTIONS

In 2016 the Group reported 92 penalties and 105 proceedings initiated on data protection issues throughout the year. The total sum of sanctions was €2,300,445.01. Most of these proceedings were initiated in Spain, where legislation is stricter than in other markets.

FREEDOM OF EXPRESSION

We are a founding member of Telecom Industry Dialogue, a group of telecommunications operators and vendors that come together to address freedom of expression and right to privacy in the telecommunications sector, within the context of the Guiding Principles for Companies and Human Rights.

In this period, we have been particularly active in the area of privacy and freedom of expression, promoting the merger between Telecom Industry Dialogue and the Global Network Initiative (GNI), a multi-party organisation made up of Internet companies, academia, civil society organisations and investors. This step forward will result in more than 1,500 million people in over 120 countries in Africa, North America, Central America, South America, Europe, the Middle East and Asia-Pacific being covered by the standards and principles protecting users' rights to which all GNI members commit. We have already officially announced our desire to join the new organisation.

Furthermore, we participated in meetings on Network shutdowns, at which all the agents involved shared experiences and identified the negative effects of this practice, both in terms of human rights and from an economic and social point of view. In turn, the members of the GNI prepared a joint statement expressing their views on the matter.

We have also collaborated with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kayne. We provided our position and best practices to the public enquiry on Freedom of Expression in the Telecommunications and Internet Access Sector.

The progress we have made in the implementation of the 10 principles of Privacy and Freedom of Expression adopted by the TID in 2016 is described in the table on the following page.

We actively *collaborate* with the United Nations' Special Rapporteur on the *right to freedom* of *opinion* and *expression*

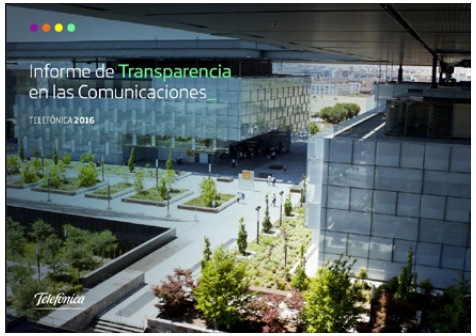
Transparency Report

In the interest of greater transparency for all of our stakeholders, in 2016 we published our Transparency Report for the first time. By doing so, we informed the public of the requests we can receive from the authorities regarding certain information.

At Telefónica we are subject to the legal environments in which we operate, which means that, in exceptional circumstances and always within the express provisions of national laws, we must respond to the requirements of the competent authorities concerning certain information on communications by our customers or the blocking of content. We must do so according to the legal framework applicable in each country, and with maximum respect for privacy, freedom of expression and the secrecy of users' communications.

In all of these cases, we implement a strict procedure which simultaneously guarantees compliance with our obligations to collaborate with the administration of justice and the protection of the rights of the affected parties.

We report that, in 18 countries for which we provide information on legal context, each jurisdiction allows the authorities to issue these types of requirements for four key indicators: legal interceptions, metadata associated with communications, blocking and filtering content and geographical or temporary suspension of service.



PRINCIPLES OF FREEDOM OF EXPRESSION

GUIDING PRINCIPLE	PROGRESS BY TELEFÓNICA
1 Create and/or maintain relevant policies, under the supervision of the Board of Directors or equivalent, highlighting the commitment to preventing, assessing and mitigating, to the extent of its capabilities, the risks for freedom of expression and privacy associated with the design, sale and operation of technology and telecommunications services.	Our Responsible Business Principles, revised in 2010, recognise the right to privacy as the basis for a relationship of trust with our stakeholders. Moreover, the Group has a Privacy Policy, approved by the Board in March 2013, which is binding in all the countries in which we operate. The Group includes the figure of the Chief Privacy Officer, the person responsible for the implementation and monitoring of the Policy, who is assisted by local Data Protection Officers. With regard to security management, the Group has in place the Corporate Information Security Policy (in addition to other regulations), which is based on international standards and updated in accordance with the growing international demands in matters of security. In addition to conducting specific training on the said Policies, all our employees have access to this via the Group Intranet.
2 Conduct regular impact assessments on human rights and use due diligence processes appropriate to the company for identifying, mitigating and managing risks for freedom of expression and privacy (in relation to technologies, products and services and specific countries), in accordance with the Guiding Principles for the application of the UN's "Protect, respect and remedy" framework.	As part of our due diligence process, in 2016 we began an update of our 2013 impact evaluation on human rights. We aim to understand the potential impacts of the Telefónica Group's strategies, of the Group's new activities, and the changing digital environment. As a starting point, we used the results from the previous evaluation and followed a methodological framework, the point of reference for which was the UN Guiding Principles on Companies and Human Rights. In this first phase, we have identified 23 human rights issues in which we find: Neutrality and respect for freedom of expression in publishing information online; offering sufficient, transparent information on mechanisms for collecting and treating information, and possible illegitimate or non-authorised uses of data. With this work, we manage to have an updated impact matrix that defines which issues are priorities for Telefónica, and which lines of action must be applied in order to ensure due diligence in the area of human rights.
3 Create and/or maintain operational processes and procedures for assessing and managing any governmental requests which might have an impact on freedom of expression and privacy.	At Telefónica, we are subject to the legal environments in which we operate, which means that, in exceptional circumstances and always within the express provisions of national laws, we must respond to the requirements of the competent authorities concerning certain information on customers' communications or the blocking of content. In doing so, besides adhering to the laws of each country, we always seek maximum respect for privacy, freedom of expression, and the secrecy of communications by users. At Telefónica, in all of these cases, we implement a strict procedure which simultaneously guarantees compliance with our obligations regarding collaboration with justice administrations and the protection of the rights of the affected parties. In 2016, we approved the Global Procedure establishing a single process for addressing these requests, in keeping with the legislation of the countries in which we operate on user information, the interception of communications, blocking access to certain websites and content, and suspending networks or services. We also specify the process for receiving and treating legal petitions, areas involved, responsibilities, treatment of communications, searches and internal control in order to guarantee legal compliance and respect for individuals' fundamental rights.
4 As far as possible, adopt strategies to anticipate, respond to and minimise any potential impact on freedom of expression and privacy in the event that an illegal governmental request or demand is received, or when the governments are deemed to be misusing products or technology for illegitimate purposes.	In addition to the formal processes indicated in the previous principle, the right to privacy, data security and information, protection of the right to freedom of expression are, together with the protection of human rights in general, issues which fall under the control of the Board of Directors, through the Regulation and Institutional Affairs Committee. This Committee is in charge of driving and supervising the implementation of Telefónica's Global Responsible Business Plan, which includes specific objectives in privacy, security and promoting the responsible use of technology. Telefónica also has a Chief Data Officer who is part of the Executive Committee of the Group. Their principal objective is to define the Company's global strategy on data or, in other words, the cognitive intelligence services associated with Big Data. This strategic function ensures that the privacy and security of data is a key element considered in our services, no matter where we are. We also have a Chief Privacy Officer who ensures that the Privacy Policy is followed in any operation we are a part of. Furthermore, we have a Data Privacy Officer for each operation, who ensures that our actions on a local level fulfil our internal and external regulations. The Privacy Committee is the body in charge of coordinating all the actions to ensure data protection. In addition, privacy and cybersecurity are two of the aspects included in our Company's risk management model (See chapter on 'Identifying and managing risks').

PRINCIPLES OF FREEDOM OF EXPRESSION

GUIDING PRINCIPLE	PROGRESS BY TELEFÓNICA
5 Always aim to guarantee the security and freedom of Company employees who may be exposed to situations of risk.	Our Global Management of Physical Security applies the security controls, processes and technologies meant for the personal protection, health and welfare of Company employees and collaborators. The information obtained by physical and logical access control allows for the management of efficient evacuation plans, managing emergency teams and affected personnel in real time, while mobilising the necessary resources to guarantee their integrity.
6 Raise awareness and train the employees involved in the relevant policies and processes.	The Telefónica Group has designed a specific plan to train and raise awareness among employees in the policies and processes that concern them. This continuous training programme is conducted both in person and online. In 2015, more than 25,265 employees were trained in Data Protection and Information Security. For further information, see details in the chapter on 'Digital Trust'.
7 Share knowledge and impressions, whenever relevant and appropriate, with all the interested parties involved in order to have a better understanding of the legal framework and the effectiveness of these principles in practice, and to provide support for their application and development.	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. Telefónica regularly participates in forums and inquiries on these issues. For further information, see details in the chapter on 'Digital Trust'.
8 Every year, and when circumstances so require, provide external information on the progress made in the application of the principles and, where appropriate, on the main events which occur in this respect.	This report summarises the progress made by the Telefónica Group in matters of privacy and freedom of expression. For further information, see the chapter on 'Digital Trust' in this Report. Seeking greater transparency for all our stakeholders, in 2016 we published our Report on the Transparency of Communication where we informed the public of the requests we may receive from the authorities in 18 countries in which we operate regarding legal interceptions, Metadata associated with communications, blocking and filtering of content and geographic or temporary suspensions of service. You may consult the Report on Transparency.
9 Assist in the development of policies and regulations promoting freedom of expression and privacy, either individually or in collaboration with other entities, seeking to mitigate the potential negative impacts arising from policies and regulations.	In this period, Telefónica has been particularly active in the area of privacy and freedom of expression, promoting the merger between Telecom Industry Dialogue and the Global Network Initiative (GNI). Furthermore, Telefónica participated in meetings on Network shutdowns, at which all the agents involved shared experiences and identified the negative effects of this practice, both in terms of human rights and from an economic and social point of view. Telefónica has also collaborated with the United Nations' Special Rapporteur on the right to freedom of opinion and of expression, David Kayne, providing the Company's opinion and best practices to the public enquiry on freedom of expression, the telecommunications sector and Internet access.
10 Examine the options for the implementation of the appropriate complaint mechanisms, as listed in Principle 31 of the UN's Guiding Principles on Business and Human Rights.	Questions regarding Telefónica's actions can be asked via the Responsible Business Channel, which is published on the Sustainability corporate web page. This channel was created in 2016 with the aim of establishing a system for communication with stakeholders, directly linked with the Responsible Business Policy and Telefónica's Commitment to Human Rights, in keeping with the principles of respect, confidentiality, rapid response and completeness.

SECURITY

Data security

We develop the concept of all-around global security for our Group. This covers the security of information through a number of control objectives that translate into a series of preventive and reactive measure on data and the technological systems processing them, in order to keep and protect information and guarantee its confidentiality, availability and integrity. For our customers, information security has a significant effect on privacy, and this takes on different dimensions depending on the country and culture.

Business continuity

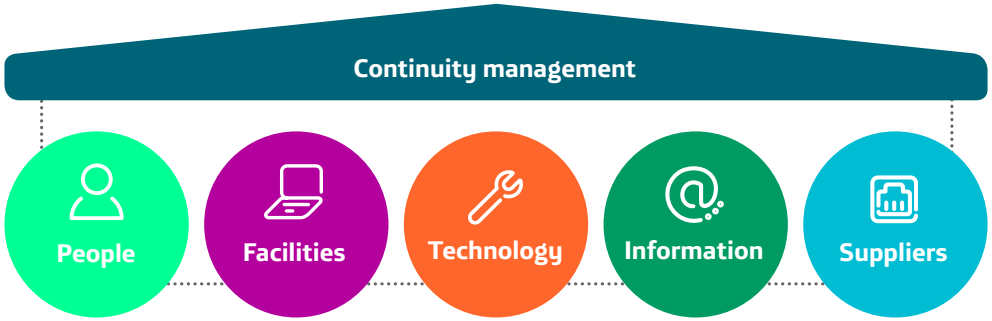
The growing competitiveness among business organisations, the ever-increasing demands of customers and shareholders, or the ever-stricter regulatory requirements are factors that force the organisation to demonstrate the resistance of its business activities when faced with any serious contingency.

A power outage, a flood, a fire or a robbery must be considered real threats that need to be treated preventively to ensure that, should any of these occur, losses are not serious enough to threaten the viability of the business. We need processes, mechanisms and techniques to mitigate the risks to which we are exposed and to guarantee high availability in the Company's operations.

The goal of our Global Continuity Plan is to preventively manage risks, ensuring the maximum possible resistance of fundamental business activities when faced with any sort of interruption to their systems.

Efficient distribution of investments in security according to our previous risk analysis process allows us to focus our efforts and budget for the most essential tasks. For more information, see the section on 'Emergencies'.

The reach of the continuity plan and of plans for recovering from disasters covers:



The continuity process is annual, and seeks constant improvement and expanded reach:

BEST PRACTICES

INVESTMENT IN CONTINUITY PLANS

When we speak of continuity, we are not referring to costs. We are speaking of an investment with very tangible returns in terms of reputation and Company image.

- Simplicity. The Business Continuity Plan is easy to understand, use and maintain.
- Limited reach. It covers the organisation's most critical operations.
- Responsibilities. It clearly states who is participating, and indicates their functions, responsibilities and authority.
- Activation of the Plan. The Business Continuity Plan is only activated in clearly defined crisis or emergency situations once the preventive security measures have failed.
- Real tests. As a result of Telefónica's large footprint, we have been able to test and improve our plans in real situations, gathering lessons learned and improvements that are unique in the sector.

Managing vulnerability and breaches

We have a network of Incident Response Centres (referred to as CSIRT in the world of cybersecurity) that work together to:

- Be aware of and analyse the risk of potential cyberthreats, as part of an intelligence process where the most relevant cyberthreats affecting the organisation are identified and understood, with the aim of predicting them and protecting the global organisation of the Group from their potentially damaging effects, and to mitigate any possible damage to a degree that is acceptable for the business.
- Monitor the serious vulnerabilities existing in the organisation's most critical technological activities, in order to minimise these assets' exposure time to the associated risks.

- Establish relationships with other national and international CSIRTs/CERTs in both the public and private sector for mutual support and the sharing of early warning information on cyberthreats and vulnerabilities.

- Detect potential security incidents affecting the organisation's technological assets by monitoring and analysing security events.

- Respond to and manage security incidents that affect the organisation by lessening their impact.

Security Services

With ElevenPaths, our cybersecurity unit, we offer disruptive innovation in cybersecurity to provide privacy and confidence to our digital lives.

We create innovative products capable of transforming the concept of cybersecurity, keeping a step ahead of the attackers who are a growing threat in our digital lives.

Eleven Paths
Telefónica CYBER SECURITY UNIT

FURTHER INFORMATION See the Eleven Paths website

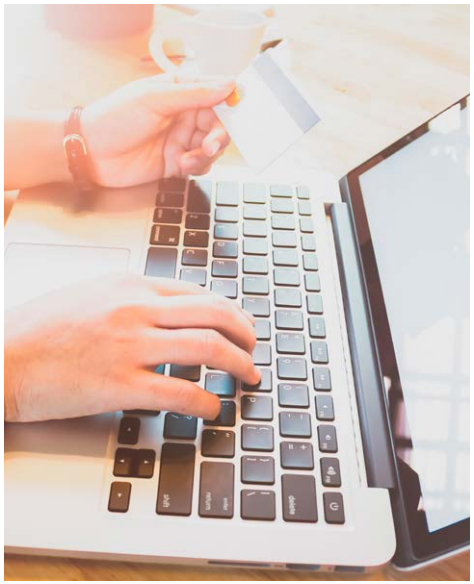
Over the past three years, we have combined the development of innovative patented technologies with the creation of alliances with the principal actors in the market. We choose to provide intelligent security services as our path towards a safer future.

Our global security services are designed to continuously improve the efficiency of our security infrastructure. Consequently, we are working to develop new services and security capabilities that can help to protect companies and their customers from the threats surrounding them. In 2016, we began a transformation process based on innovation through technology.

We collaborate with the foremost entities and organisations, such as the European Commission, CyberThreat Alliance, ECSO, EuroPol, Incibe and the OEA.

In addition, we have opened nine Security Operations Centres and a new Advanced Global Centre (Telefónica Advanced Global SOC -TAGS-). This broad network allows us to take on threats and security problems from a global point of view, but without having to distance ourselves from our customers.

Furthermore, with ElevenPaths we promote the entrepreneurial spirit by investing in security startups like Countercraft, 4IQ, BlueLive, LogTrust, IMBox and Alise Devices. Thanks to these collaborations, alliances and our experience, we can offer a portfolio of integral cybersecurity solutions for the world of IoT, identity and privacy, anti-fraud, document management, industrial cybersecurity, safe mobility and risk management, with the aim of providing our customers with solutions that are adapted to their specific needs.



STAKEHOLDERS, 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.

Telefónica regularly participates in forums and inquiries on these issues. In 2016, the principal initiatives were:

- **Centre for Information Policy Leadership:** We are members of the Centre for Information Policy Leadership, a discussion group on privacy and safety with offices in Washington DC, Brussels and London, which works with

We offer a portfolio of *integral cybersecurity* solutions with the aim of providing our customers with *solutions* that are *adapted* to fit their needs

leaders in the industry, regulatory authorities and policy leaders worldwide in order to contextualise and promote a policy of privacy and cybersecurity on a global scale.

In 2016, we worked together to elaborate a public position on data transparency.

- **Rightscon:** We participated in the edition of Rightscon Silicon Valley held from March 30 to April 1, 2016 in San Francisco, California. Rightscon is a debate forum on digital human rights that brings together stakeholders from around the world.

- **GSMA**: Working sessions for the elaboration of the Responsibility Principles for the Mobile Ecosystem.

- **Data Transparency Lab:** We are members of the Data Transparency Lab, a community of technology specialists, investigators, politicians and industry representatives that work to move forward in transparency of personal online data through scientific research and design.

PROTECTING MINORS AND PROMOTING THE RESPONSIBLE USE OF TECHNOLOGY

As part of our commitment to the responsible use of technology, we have defined a global strategy based on promoting proper Internet use by children and adolescents. Via implementation of this strategy, we seek to provide parents, tutors and everyone involved in educating society's youngest members with the tools and services they need to promote safe Internet surroundings, and to raise awareness in society in general of the importance of addressing these key issues to raise more responsible digital citizens.

Our lines of action and commitments to the protection of minors on the Web and to the responsible use of technology can be grouped into 5 working areas:

Alliances with stakeholders, self-regulation initiatives and content blocking

Looking out for security in the online environment is a challenge we cannot take on alone. Therefore, Telefónica will need to work together with allies in different sectors and in civil society to ensure that young people can take advantage of the potential of technology while minimising any risk they may encounter.

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

- State security forces and support for national crime reporting hotlines (Equipo Niños, ASI, Te Protejo, Safernet, Centre for Child Protection on the Internet, Seguros en Internet...).

- NGOs and national associations (Pantallas Amigas, Safernet, NSPCC, Childnet, Red Papaz, among others).

- Key stakeholders to deliver actions for the protection of minors online (Inhope, Insafe, ANATEL, Red de Aliados por la Niñez, Zentrum für Kinderschutz im Internet, RCPI, Governments, etc.).

As well as our participation in the following alliances:

- Alliance with the GSMA to fight against content involving sexual abuse of minors.

- We block content on the lists provided by the Internet Watch Foundation in the following countries: Argentina, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Spain, the UK and Venezuela. Telefónica Colombia also does their part through MINTIC.

- **ICT Coalition:** Principles of Safe Use of connected devices and online services for minors. At the end of 2016, each of the member companies submitted a report on our performance with regard to the commitments we took on for each of the actions in the ICT Principles. These documents are in the public domain, so that they can be reviewed by whoever would like to see them.

- **Alliance to better protect minors online:** We have participated in this initiative since its creation in September 2016. Its goal is to identify the risks children might encounter as they surf the Internet, to promote the exchange of best practices, and for members to commit themselves to realising specific actions, including a code of conduct, to protect minors in the digital world. Nevertheless, the Alliance is not starting from scratch. Rather, it takes advantage of the achievements and the lessons learned by the Coalition of CEOs to make the Internet a safer place.

On a local level, we also participate in several working groups, and we take part in national initiatives to promote responsible use of technology by young people, and the protection of minors in online environments:

GUATEMALA

Telefónica Guatemala signed, together with GSMA, UNICEF, CLARO and TIGO, a commitment letter for the protection of boys, girls and adolescents from online violence and sexual exploitation. In addition a committee was formed to ensure these commitments are fulfilled.

PANAMA

Through the Telefónica Foundation, the Company is part of the Red de Aliados para la Niñez (Network of allies for childhood), which brings together more than 23 organisations and/or foundations that work towards children's welfare.

MEXICO

We participate in the "Nos importa México" (We care about Mexico) programme promoted by the Agencia Nacional de Telecommunications (ANATEL), which aims to empower users and give them access to tools that allow them to enjoy mobile services in a safe and trustworthy environment.

GERMANY

O2 Germany is an active member of the Centre for the protection of minors on the Internet, which is currently working on developing a tool to report inappropriate and illegal content on the Internet in cooperation with the German ICT industry.

NICARAGUA

Since 2012, Telefónica Nicaragua has been a part of the Mesa de Trabajo Nacional del Uso Seguro del Internet (National Working Council for Safe Internet Use) led by the Vice President of the Republic through the Nicaraguan Council of Science and Technology, made up of the Ministry of Education, universities, private companies, the Cámara Nicaragüense de Telecomunicaciones e Internet (Nicaraguan Chamber on Telecommunications and the Internet) and NGOs.

ECUADOR

Telefónica Ecuador is part of a public-private technical council that aims to establish a reporting hotline in Ecuador for the protection of children and adolescents online.

COLOMBIA

Telefónica Colombia participates in the Mesa TIC (ICT Table), a multi-sector work group (involving the government, universities, civil society and private companies) that promotes initiatives for the protection of minors on the Internet. In addition, we collaborate with the Ministry of Information Technology, the Instituto Colombiano de Bienestar Familiar (Colombian Institute of Family Welfare, or ICBF), and the NGO RedPapaz as partners of the Te Protejo reporting hotline.

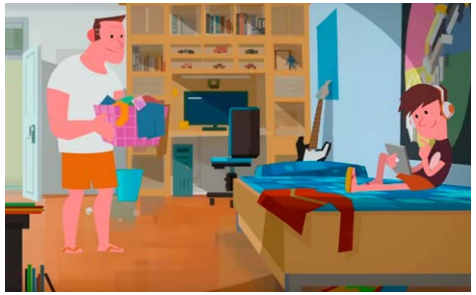
PERU

Seguros en Internet (Safe on the Internet) is an initiative driven by the Red Peruana Contra la Pornografía Infantil (Peruvian Network Against Child Pornography, RCPI) and Telefónica Peru, which seeks to promote safe use of the Internet by children. In order to achieve this, they operate the web portal www.seguroseninternet.org, which can be used by the public to report online content that is illegal or inappropriate for children, such as child pornography, grooming, or cyberbullying, among others.

URUGUAY

Through the Proyecto Emprender (telecommunications training and responsible use of social networks), the Telefónica Foundation is part of the Grupo de Gobernanza en Internet (Internet Governance Group).

FURTHER INFORMATION



THE AUDIOVISUAL ENVIRONMENT

Children and adolescents have made the use of ICT and the consumption of content part of their daily lives. This is an important part of their play time, their studies and their interactions with those around them. In addition, television is a fundamental element in their development, and therefore we at Movistar+ are committed to:

- 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.
- Encouraging digital literacy among young people and their families, persuading them to take advantage of the potential of audiovisual media.

Our aim is for the audiovisual experience to promote the *development* of *creative, social and civic* abilities in children

INITIATIVES IN SPAIN

- Labelling content: Movistar+ includes a permanent label that indicates the recommended age for audiovisual content being shown. In addition, these are visible on all Company promotions related to audiovisual content offered through the platform. This information can also be found through online programming guides.
- Technical protection: Parental controls, purchasing PINs and parental PINs, age verification tools... These security measures depend on the technology available to customers for accessing the service: IPTV, satellite TV or Internet, as well as the device used. In general, we offer our customers the ability to block channels by activating the parental PIN. In addition, with the IPTV platform, content can be blocked on demand for children under 7, 12, 16 and 18.

  Moreover, the specific content for adults is offered to customers in a section separate from other content. On some devices, this section may not even be available. In order to view this type of content, a PIN code is required.

PRODUCTS AND SERVICES

Together with family supervision, technology itself is the best tool to help parents and minors make effective use of technology. For this reason, we feel that promoting and developing products and services that facilitate responsible use of the Web and connected devices is key:

- **Parental controls:** Movistar Protege (Spain), Protección Familiar Movistar (Mexico), Escudo Movistar (Argentina, Uruguay, Colombia, Nicaragua), Qustodio (Peru), Vivo Filhos Online (Brazil), Parental Control (UK).

- **Safety measures aimed at protecting minors on the Web:** Online Protection Pack.

- **Technical security (antivirus, security packs, personalised care...):** Protección Multidispositivo (Mexico), Seguridad Total (Argentina), Gurú, O² protect (Germany), Safe Connection and Security Centre in devices.

SUPPLY CHAIN

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:

- **'Safety by design':** The Innovation in Ecosystems area works closely with the principal manufacturers of terminals, as well as with operating systems to include functionalities for protecting minors in 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 terminals our customers use, as well as to improve transparency on the type of data that can be shared through mobile terminals.

- **Collaboration in the development and implementation of initiatives that promote responsible use of technology and user protection:** We maintain fluid communication with product managers in different digital ecosystems to improve the use of the same by customers, and to promote proper use of technology.

EDUCATING AND RAISING AWARENESS:

We cannot ignore the importance of teaching children and youths to use the Internet and connected technologies creatively, responsibly and safely. The same can be said about the need for parents and educators to have the resources they need to successfully face this new challenge. For this reason, Telefónica supports the development of training and awareness-raising initiatives that promote coexistence in an increasingly digital society:

- **The Familia Digital and Dialogando portals are the principal lines of action for achieving all of these objectives:**

Familia Digital

In 2016, Familia Digital became the go-to website for advice on the responsible use of technology by minors in Movistar's Hispanic community, with the platform having been launched in 9 countries (Spain, Ecuador, Mexico, Costa Rica, El Salvador, Guatemala, Nicaragua, Panama and Venezuela).

dialogando

In November 2016, Movistar and Vivo presented Dialogando, a global initiative that has the aim of discussing our relationship with technology in each area of our lives, from our first steps in a digital environment to our personal relationships through ICT and responsible use of digital entertainment, among others.

This project has already been launched in Brazil, Spain, Venezuela, Colombia, Ecuador, Nicaragua, Panama, Guatemala and Uruguay, and in the coming months it will be launched in 6 of the Group's other operations to reach a total of 15 countries.

4 QUALITY EDUCATION

In addition, we have carried out several initiatives, including the launch of an educational programme for promoting the responsible use of smartphones “Pilar y su celular” (Pilar and her mobile phone): a series of animated videos and educational guides for children that address issues like privacy, managing one’s digital identity, caring for the environment through technology, downloading applications and integrated purchases, among other relevant subjects.

BEST PRACTICES

SPAIN

Last year in Madrid, we organised the 1st Encuentro de Familias Digitales (Digital Families Meeting) on the subject “Connected children, disconnected parents?”. At this Meeting we brought together experts, bloggers and minors to debate the importance of digital education in children, young people and adults in an increasingly connected environment, and sought solutions to the challenges we face regarding our digital diet and health.

The Ciberexpert@ program, a collaboration between Telefónica Spain and the Spanish National Police to help minors understand how to use connected devices through training in schools.

MEXICO

We launched the project “Caravana de Educación Vial Mapfre” (Mapfre Road Education Caravan), to promote responsible use of mobile phones behind the wheel; as well as the “Netiquétate” programme for training educators, parents and minors in collaboration with Pantallas Amigas (Friendly Screens).

NICARAGUA

Participation in the campaign “Por una comunidad educativa segura en Internet” (For a safe educational community on the Internet), by setting up a free advice reception service on responsible use of technology in mobile phones, which can be used by any interested customers.

BEST PRACTICES

COLOMBIA

We launched a social network communication campaign entitled #AprenderdeTIC, which provides information on safe use of smartphones, best Internet practices, privacy in social networks and how to responsibly choose video games, among other topics.

GERMANY

We created a Guide to raise awareness on safe, positive technology use among parents and children in collaboration with Deutsches Kinderhilfswerk e.V.,and have supported the development of school materials to teach minors and their teachers about developing digital skills.

UNITED KINGDOM

Through O2 United Kingdom, we initiated a broad strategy for protecting minors on the Internet in collaboration with the NSPCC organisation. The project, visible through a section of the commercial website, includes initiatives for raising awareness, offering advice and training as well as the development of programmes and products/services that help families make safe use of the online environment.

In addition, we have a free telephone help line aimed at addressing any doubts on the digital education of minors (how to install parental controls, how to report cases of cyberbullying...), as well as NET AWARE, a website developed together with NSPCC, which provides advice and recommendations on the responsible use of technology from O2 personnel, as well as other children and parents.

BRAZIL

We have published parental and school mediation Guides on the responsible use of technology among children and youths.

ECUADOR AND GUATEMALA

We organise talks in schools on proper Internet use, which are aimed at students, teachers and families.