2.4. Digital Trust

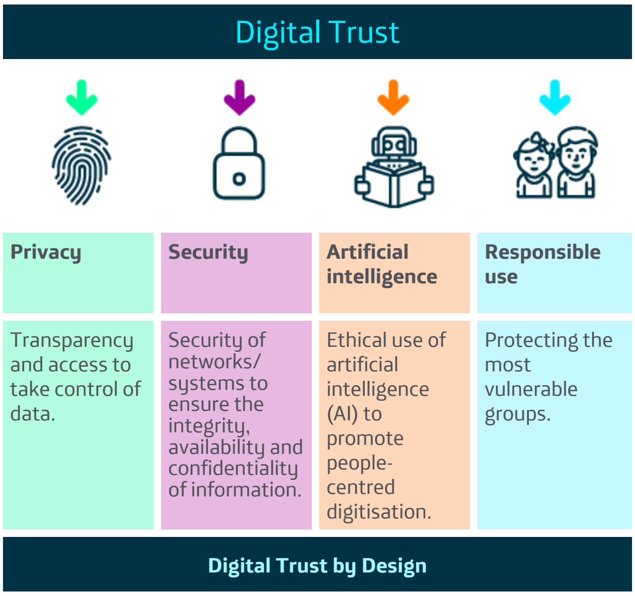
KEY POINTS

- **We protect our customers' data through high privacy and security standards, monitored at the highest level.**
- **We are transparent about how, why and when our customers' data is collected, used, stored and deleted, as well as how we protect it with a high level of security.**
- **We empower our customers to have access to and control of their personal data.**

2.4.1. Approach GRI 103

Trust in the use of digital services is one of the key elements in a human-centred digital transition. We want our customers to feel confident about using our products and services, and to be aware that we respect their rights at all times, offering them choices about the use of their personal information. In short, we want our customers to be in control of their digital experience.

We have therefore defined digital trust based on four pillars that shape our commitment to the customer.



Digital Trust

Privacy	Security	Artificial intelligence	Responsible use
Transparency and access to take control of data.	Security of networks/ systems to ensure the integrity, availability and confidentiality of information.	Ethical use of artificial intelligence (AI) to promote people-centred digitisation.	Protecting the most vulnerable groups.

Digital Trust by Design

Each pillar stands for policies and processes that not only ensure compliance with growing regulation, but also increase transparency in how we manage data privacy and security.

In this way we ensure that our customers are informed at all times about:

- How and why their data is collected, stored and used.
- The fact we protect their data with a maximum level of security.
- The fact we commit ourselves to using artificial intelligence ethically.
- The fact we promote the responsible use of technology, especially when it comes to vulnerable groups such as minors.

Our Digital Trust by Design approach also incorporates these policies into the design, development and management processes of our products and services.

The body responsible for all issues related to digital trust is the Board of Directors, as indicated in the governance section of each issue.

2.4.2. Privacy GRI 103

2.4.2.1. Strategy

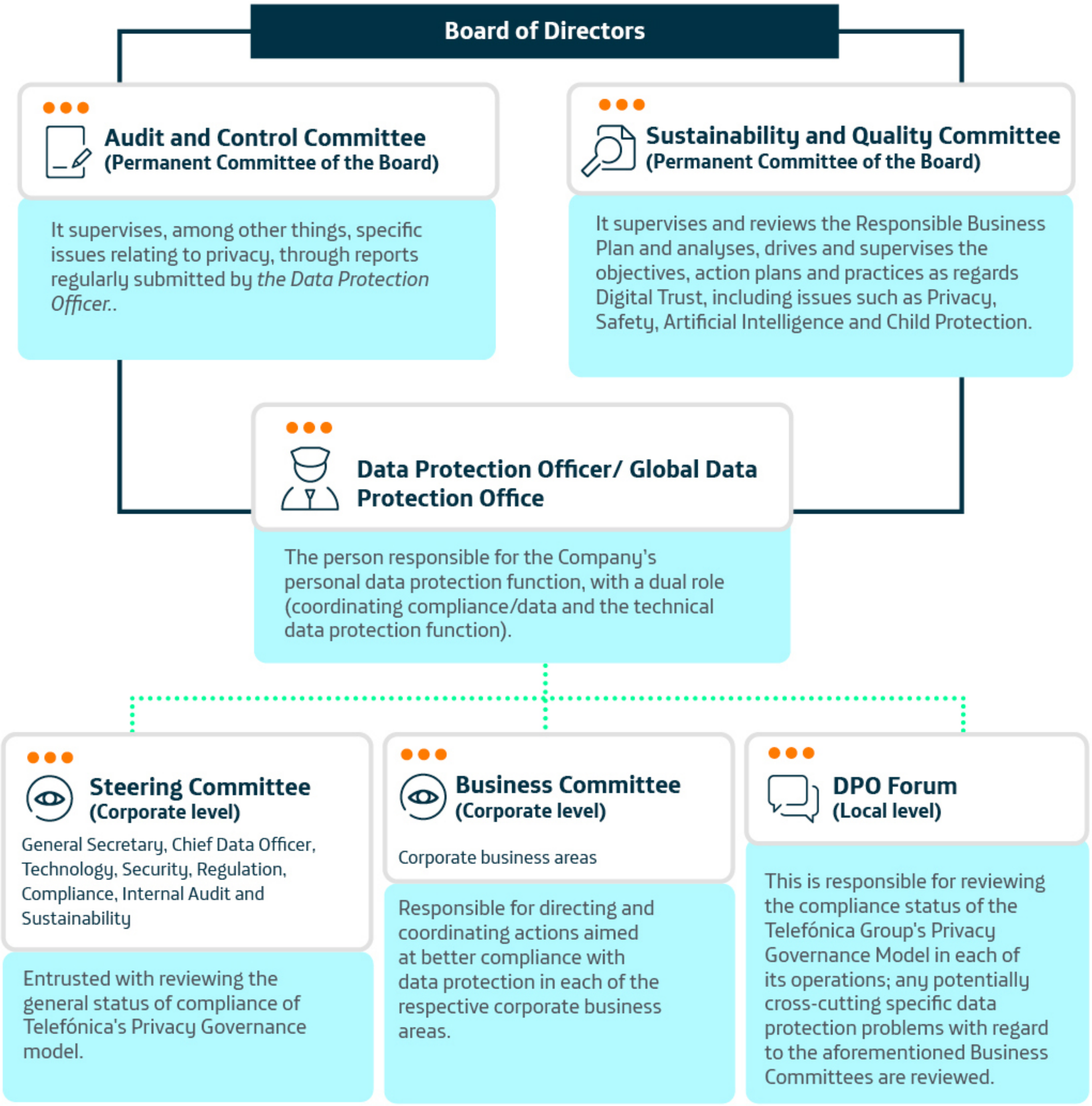
The privacy strategy is based on three pillars:

- **PROTECTION**: Protect our customers' personal data through robust policies and processes.
- **TRANSPARENCY**: Be transparent about how and why we collect, use, store and delete our customers' personal data.
- **EMPOWERMENT**: Empower our customers through simple and secure tools so that they can control the use of their personal data.

2.4.2.2. Governance

Telefónica has an array of processes designed to ensure its commitment to the right to privacy of all persons whose data we have access to. These processes are described in the Governance Model Rule on Personal Data Protection, whose lines of action are designed to ensure sufficient means and resources to guarantee that privacy management is in keeping with corporate strategy.

Privacy governance



Board of Directors

Audit and Control Committee
(Permanent Committee of the Board)

It supervises, among other things, specific issues relating to privacy, through reports regularly submitted by *the Data Protection Officer..*

Sustainability and Quality Committee
(Permanent Committee of the Board)

It supervises and reviews the Responsible Business Plan and analyses, drives and supervises the objectives, action plans and practices as regards Digital Trust, including issues such as Privacy, Safety, Artificial Intelligence and Child Protection.

Data Protection Officer/ Global Data Protection Office

The person responsible for the Company's personal data protection function, with a dual role (coordinating compliance/data and the technical data protection function).

Steering Committee
(Corporate level)

General Secretary, Chief Data Officer, Technology, Security, Regulation, Compliance, Internal Audit and Sustainability

Entrusted with reviewing the general status of compliance of Telefónica's Privacy Governance model.

Business Committee
(Corporate level)

Corporate business areas

Responsible for directing and coordinating actions aimed at better compliance with data protection in each of the respective corporate business areas.

DPO Forum
(Local level)

This is responsible for reviewing the compliance status of the Telefónica Group's Privacy Governance Model in each of its operations; any potentially cross-cutting specific data protection problems with regard to the aforementioned Business Committees are reviewed.

The person responsible for the Group's Personal Data Protection function is the Data Protection Officer, who reports directly to the Board of Directors of Telefónica, S.A. through the Audit and Control Committee. To ensure compliance with this function, the different corporate areas meet biannually as part of the Governance Model Monitoring Committee, the Business Committee and through the Local Data Protection Officers.

In addition, the Sustainability and Quality Committee (a permanent committee of the Board) is responsible for promoting and monitoring the implementation of

Telefónica's Global Responsible Business Plan, which includes specific targets in the area of privacy. The Board is informed monthly about the implementation of the plan by the Corporate Ethics and Sustainability department, which runs the Responsible Business Office and includes the heads of the global operational areas.

2.4.2.3. Policy

We promote and review different global and local policies and processes to strengthen our commitment to the right to privacy of all persons whose data we have access to through the definition and implementation of operational privacy domains throughout the data lifecycle.

Privacy regulations

Global Privacy Policy

Corporate Rule
Approved by the Board of Directors of Telefónica, S.A.

Telefónica, S.A.
3rd Edition: September 2018

Updated in 2018, it establishes obligatory rules of common behaviour for all the Company's entities, laying the foundations for an approved privacy culture based on the principles of legality, transparency, commitment to the rights of the data subjects, security and limitation of the retention period.

Governance Model Rule on Personal Data Protection

Corporate Rule
Approved by the DPO Office department of Telefónica, S.A.

Telefónica, S.A.
1st Edition: September 2018

Approved in 2018, it establishes the strategic, organisational and operational, and management framework applicable to the different actions in the field of data protection.

Global Rule on Requests made by Competent Authorities

Corporate Rule
Approved by the Ethics and Sustainability department

Telefónica, S.A.

Updated in 2019, it sets out the principles and minimum guidelines that must be referred to in the internal procedures of each of the Group's companies/business units/OB to comply with their duty to cooperate with the competent authorities as regards our customers' data.

2.4.2.4. Lines of action GRI 103

Our lines of action in the area of privacy are configured around the following subjects:

- Privacy by Design (PbD)
- Digital privacy
- Transparency initiatives
- Client empowerment
- Consultation and complaint mechanismsmsión

Privacy by Design (PbD)

The principle of Privacy by Design (PbD) is undoubtedly one of the Telefónica Group's essential, strategic pillars and is defined in its compulsory internal regulations.

The concept of Privacy by Design entails, among other relevant matters, the entire organisation's duty to establish a data management governance model to ensure consideration not only of the application of privacy protection measures from a legal and security point of view in the early stages of any project, but also all the business procedures and practices related to each processing activity or project involving personal data.

We have our own Privacy by Design Guidelines to define the set of rules, standards and legal and security processes that must be taken into account to comply with Privacy by Design obligations. This is in accordance with the legal framework and our Global Privacy Policy, both of which are to ensure that the rights and freedoms of the individuals who hold the personal data are guaranteed as from the initial definition of any processing project or activity.

These practical guidelines stand as reference documents for those Telefónica Group professionals whose functions include the conception, definition, development, standardisation and evolution of products and services. They also apply for internal use cases (IUCs) that directly or indirectly involve the processing of personal data and consequently affect the right to privacy of individuals, whether they are customers, users or employees, etc.

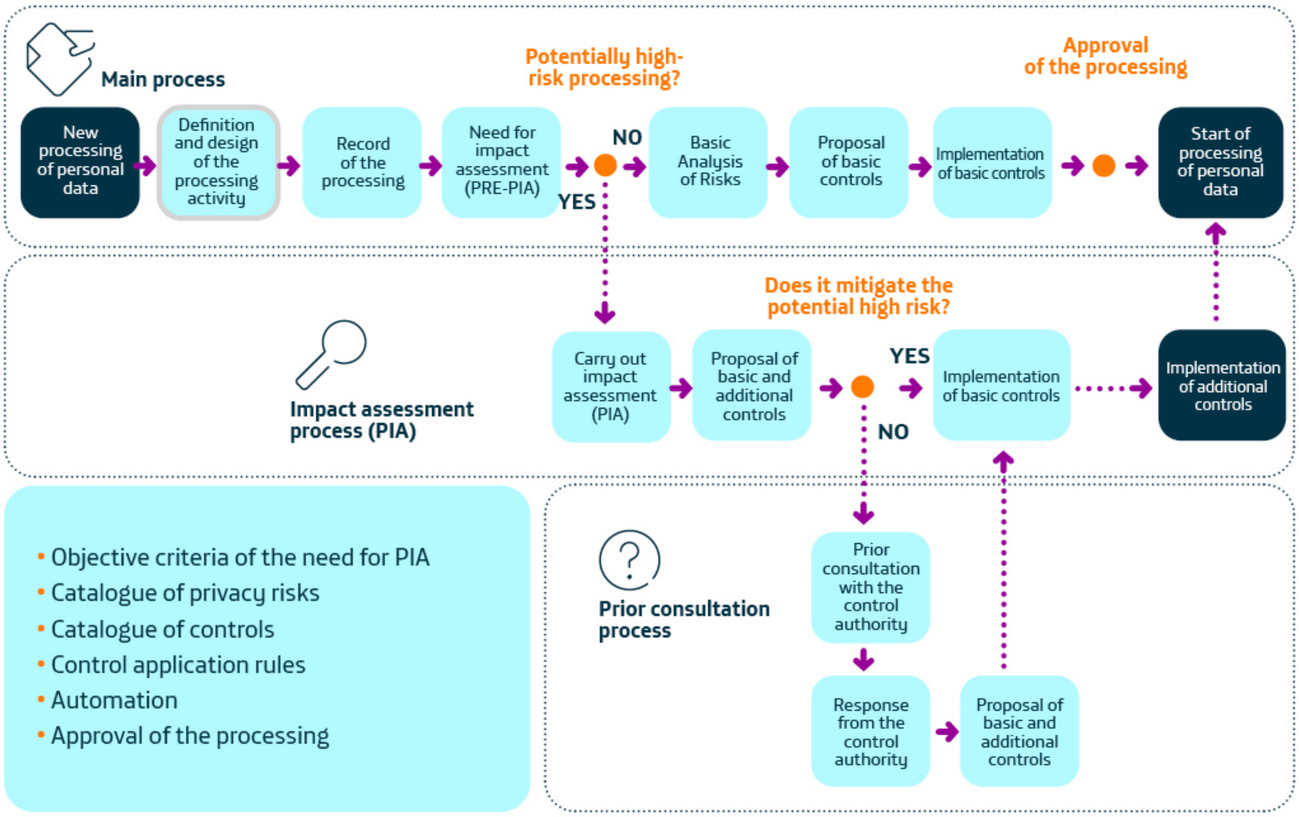
In addition, product managers are always supported by the specialists in the Privacy and Security area of each company and/or business unit of the Group, in order to ensure that all necessary legal and security requirements regarding privacy are taken into account from the very moment of the design of the specific product, service or internal Telefónica use cases in question.

We use a risk management-oriented approach of proactive responsibility (i.e. critical and continuous self-analysis of each company in the fulfilment of the obligations required by data protection regulations). The aim is to establish strategies that incorporate privacy throughout the entire data life cycle in the processing operations of each product or service: collection and obtainment, processing, exercise of rights and retention and deletion

When defining or developing any Telefónica Group product or service, the practical application of Privacy by Design throughout the process involves aspects such as: (i) the lawfulness and definition of the legitimising grounds for the processing; (ii) the guarantee that the data is secure and that the most appropriate security measures are being applied according to the potential risks; (iii) their transparency in the privacy clauses and policies in relation to the data subject; (iv) the minimisation of data in that it must be strictly necessary for the purposes of the processing; (v) the commitment to the data subjects' rights; and (vi) the limitation of the period of retention, among others.

The PbD process that was defined by the Telefónica Group's Global Data Protection Office includes at least the following activities:

Proceso de Privacidad por Diseño


Main process
Potentially high-risk processing?
Approval of the processing
New processing of personal data
Definition and design of the processing activity
Record of the processing
Need for impact assessment (PRE-PIA)
NO
YES
Basic Analysis of Risks
Proposal of basic controls
Implementation of basic controls
Start of processing of personal data
Does it mitigate the potential high risk?
Impact assessment process (PIA)
Carry out impact assessment (PIA)
Proposal of basic and additional controls
YES
NO
Implementation of basic controls
Implementation of additional controls
Prior consultation process
Prior consultation with the control authority
Response from the control authority
Proposal of basic and additional controls

- Objective criteria of the need for PIA
- Catalogue of privacy risks
- Catalogue of controls
- Control application rules
- Automation
- Approval of the processing

Digital Privacy Framework

At Telefónica, the PbD process is digitised through the Digital Privacy Framework implemented in the systems and platforms where processing takes place, such as the 4th platform.

The Digital Privacy Framework defines the global legal and privacy strategy framework with respect to GDPR and ePrivacy in data processing platform products and systems.

The Digital Privacy Framework adapts privacy guidelines to a technological reality by standardising and conceptualising the functional and technical requirements of the dynamics of privacy systems and applying them automatically and digitally to processing.

This digitisation is implemented by design and by default, and naturally enables us to build a transparent ecosystem, making it possible to build a dynamic and automatic privacy process between the customer and the systems that carry out the processing, in compliance with the GDPR.

In 2021, significant progress will be made in the digitisation of ePrivacy processing, and the personal data anonymisation tool will be available to add another layer of robustness to the Digital Privacy Framework.

Transparency initiatives

One of the challenges and key elements in privacy is to ensure transparency, and we aim to make privacy more human and understandable by applying the principles of human-centred design. In this regard, at Telefónica we are committed to putting transparency into practice by including it as one of the principles of the Global Privacy Policy and developing different initiatives to implement this principle:

a. Global Privacy Centre

The public reference point for our global privacy and security policy and processes. It is where our stakeholders can find all the information they need easily and in a simple format by means of visual and graphic resources.

b. Operators' Privacy and Security Centres

In 2020, new local Privacy and Security Centres were updated and created on the commercial websites of Telefónica Group operators. To roll out this project, we first conducted a study to understand our customers' perception of the use of their data. The study was the result of customer surveys, with more than 600 interviews in each of the 8 countries covered in this Report. The aim is for both our customers and any stakeholder to be able to obtain information, in a simple, digital and understandable way, on the processing of personal data performed by the operators, as well as other relevant information on privacy matters, such as the channels and means for exercising their rights, the security and confidentiality measures adopted to process their data and the privacy and security processes we adopt from the design stage. These Centres also include other relevant information such as the privacy terms and conditions applicable to our products and services, transparency reports, our Artificial Intelligence Principles, and the security and child protection issues that apply in all digital environments. The Centres are currently available or in the process of being launched in 100% of our operators.

c. Telecommunications Transparency Report

We publish an annual report on the requests we receive from the competent authorities in the countries in which we operate on lawful interception, metadata associated with communications, blocking and restriction of content and geographical and temporary suspension of services.

We follow a strict procedure for all requirements as set out in the regulations in response to requests from the competent authorities. This also guarantees fulfilment of our obligations in terms of collaboration with the authorities and the protection of the fundamental rights of those affected, as set out in our Chapter on Human Rights.

A total of 4,193,120 requests for customer information from competent authorities (lawful interception and access to metadata) were recorded in 2020. Of these requests, 36,598 were rejected, which means that 99% of the requests were executed. The number of accesses/customers affected is 6,025,744,

Client empowerment

As part of our principle of transparency, Telefónica provides its customers with access to the data they generate during the use of our products and services – data that are collected in the so-called "Personal Data Space" of 4th platform and which are accessible through different channels such as the Transparency Centre in the Mi Movistar app.

2020 saw the launch of the Transparency Centre in Spain, which offers all customers access to their privacy preferences and the management of data collected in the Personal Data Space, which is currently available to a group of users through the "My Movistar" application (in the Security and Privacy section of the User Profile).

In the Transparency Centre, through the Privacy Permissions section, customers can manage the legitimising grounds relating to the use of their data for certain purposes. The Access and Download section offers useful views of different types of data, with a user-friendly experience and in keeping with privacy criteria. It also has the option to download a document with further details of the datasets.

Our intention is to have the Transparency Centre available in all channels by 2021. Our customers will be able to access it from the movistar.es online channel, where both functionalities will be offered, and it will also be accessible from the television for the same groups of customers who currently have these functionalities.

The Transparency Centre experience has been designed to be user-centric, avoiding complex legal language and explaining the purpose for which data is processed and the nature of that data within Telefónica, providing clarity, transparency and reinforcing trust.

The Transparency Centre represents the next step towards fulfilling our promise to give our customers features for them to control and ensure the transparency of their data, always in accordance with applicable privacy regulations. For example, in Europe these processing activities will be fully aligned with the General Data Protection Regulation (GDPR).

Consultation and complaint mechanisms

Besides the mechanisms established in the Privacy Policies and Centres, Telefónica has implemented other means of consultation and mediation to deal with privacy issues:

a. Responsible Business Channel: We have a public channel on our website via which all our stakeholders can consult or complain about any aspect related to the Responsible Business Principles. In 2020, 15 communications on privacy and 0 on freedom of expression were processed or received a reply or remedy.

b. Voluntary mediation system with AUTOCONTROL: This system has been operational since January 2018 to provide a swift response to complaints related to identity theft and the receipt of unsolicited advertising. The procedure was developed by the Asociación para la AUTOrregulación de la Comunicación Comercial (AUTOCONTROL) in collaboration with the Spanish Data Protection Agency (AEPD). It also involves the participation of Orange, Telefónica and Vodafone and is open to other entities. This information can be found in the Movistar Privacy Centre.

2.4.3. Security

2.4.3.1. Strategy

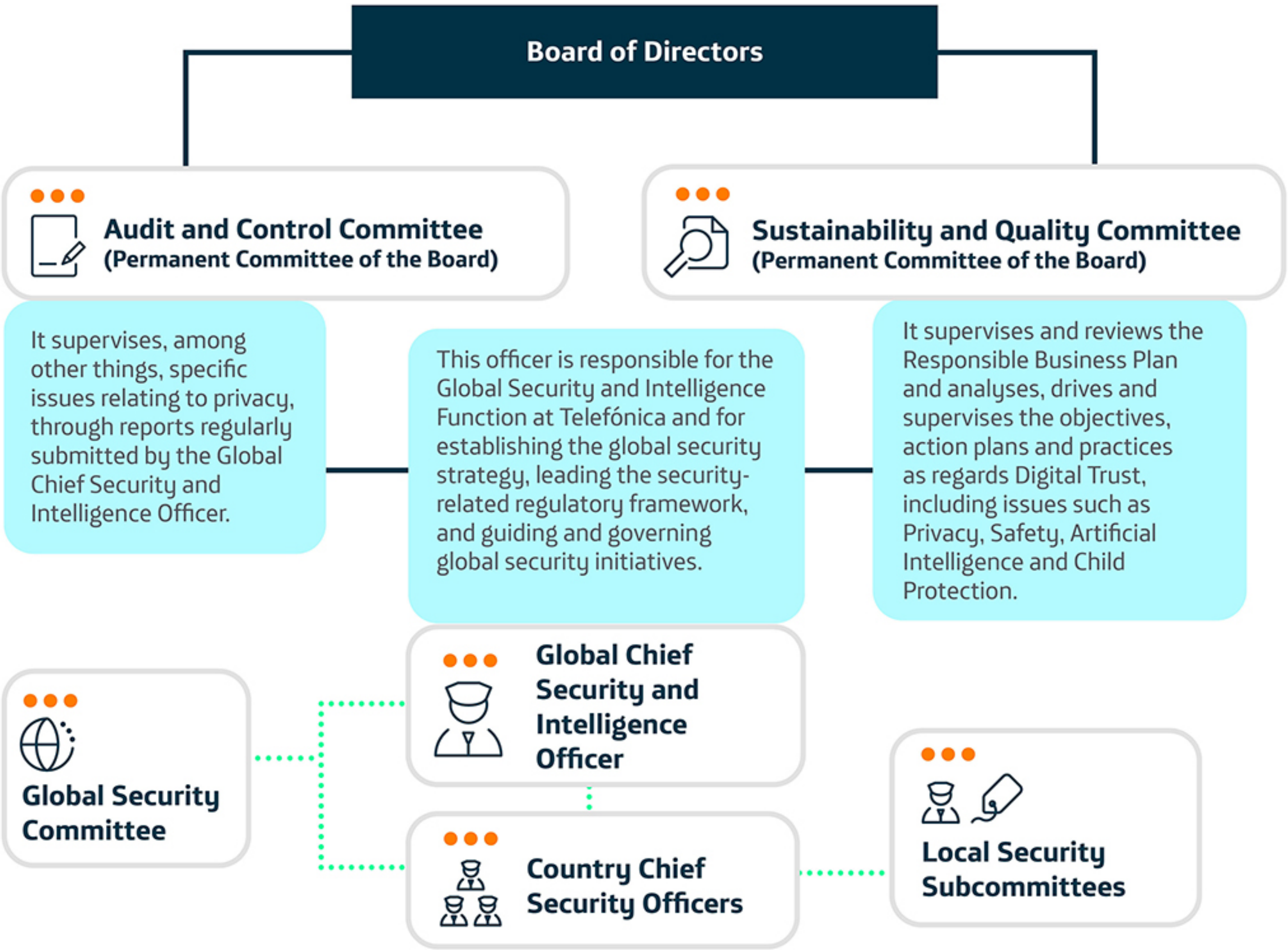
The increase in the number and complexity of security threats, together with their diversification, leads to the constant application and management of security measures. For this reason, we believe that security should be considered a process of continuous improvement, and understood as an integral concept that encompasses physical and operational security, information security including cyber security, business continuity and fraud prevention.

The security strategy is based on a number of processes and activities that reinforce the Company's business operating processes and transformation initiatives. This group of processes is encompassed in a security management system that conforms to international reference frameworks and standards such as ISO 27001 and NIST.

2.4.3.2. Governance

To achieve effective protection of the Telefónica Group's assets, including services and data, and to ensure the necessary resources and support, it is essential for the Security area to have the backing of the Company's management and report to the highest level. The Security area is indexed on a solid organisational structure starting from the Board of Directors through its Sustainability and Quality and Audit and Control Committees, to the security structures in the local operators.

Governance Committee


Board of Directors
Audit and Control Committee
(Permanent Committee of the Board)
Sustainability and Quality Committee
(Permanent Committee of the Board)
It supervises, among other things, specific issues relating to privacy, through reports regularly submitted by the Global Chief Security and Intelligence Officer.
This officer is responsible for the Global Security and Intelligence Function at Telefónica and for establishing the global security strategy, leading the security-related regulatory framework, and guiding and governing global security initiatives.
It supervises and reviews the Responsible Business Plan and analyses, drives and supervises the objectives, action plans and practices as regards Digital Trust, including issues such as Privacy, Safety, Artificial Intelligence and Child Protection.
Global Chief Security and Intelligence Officer
Global Security Committee
Country Chief Security Officers
Local Security Subcommittees

The chief responsible of the Global Security and Intelligence department in Telefónica is the Global Director of Security and Intelligence who has been delegated the authority and responsibility by the Board of Directors of the Company to establish the global security and intelligence strategy, as well as to lead the security and intelligence policy framework and to guide and govern global security and intelligence initiatives.

The Global Director of Security and Intelligence reports to the Board of Directors of the Company through the Audit Committee and the Sustainability and Quality Committee.

In each Telefónica Group company, there is a local security responsible/head, proposed by the Global Director of Security and Intelligence.

For the purposes of governance and coordination, there is a Global Security Committee, which is chaired by the Global Director of Security and Intelligence, and its members are the corporate heads of different areas of the Company (Compliance, Audit, Legal, Technology and Operations, People, Sustainability, etc.), and the country responsibles/heads of security. There are also local security subcommittees chaired by the local security responsibles/heads. They collaborate in the definition of strategic initiatives and global guidelines, and implement them in each Telefónica group company.

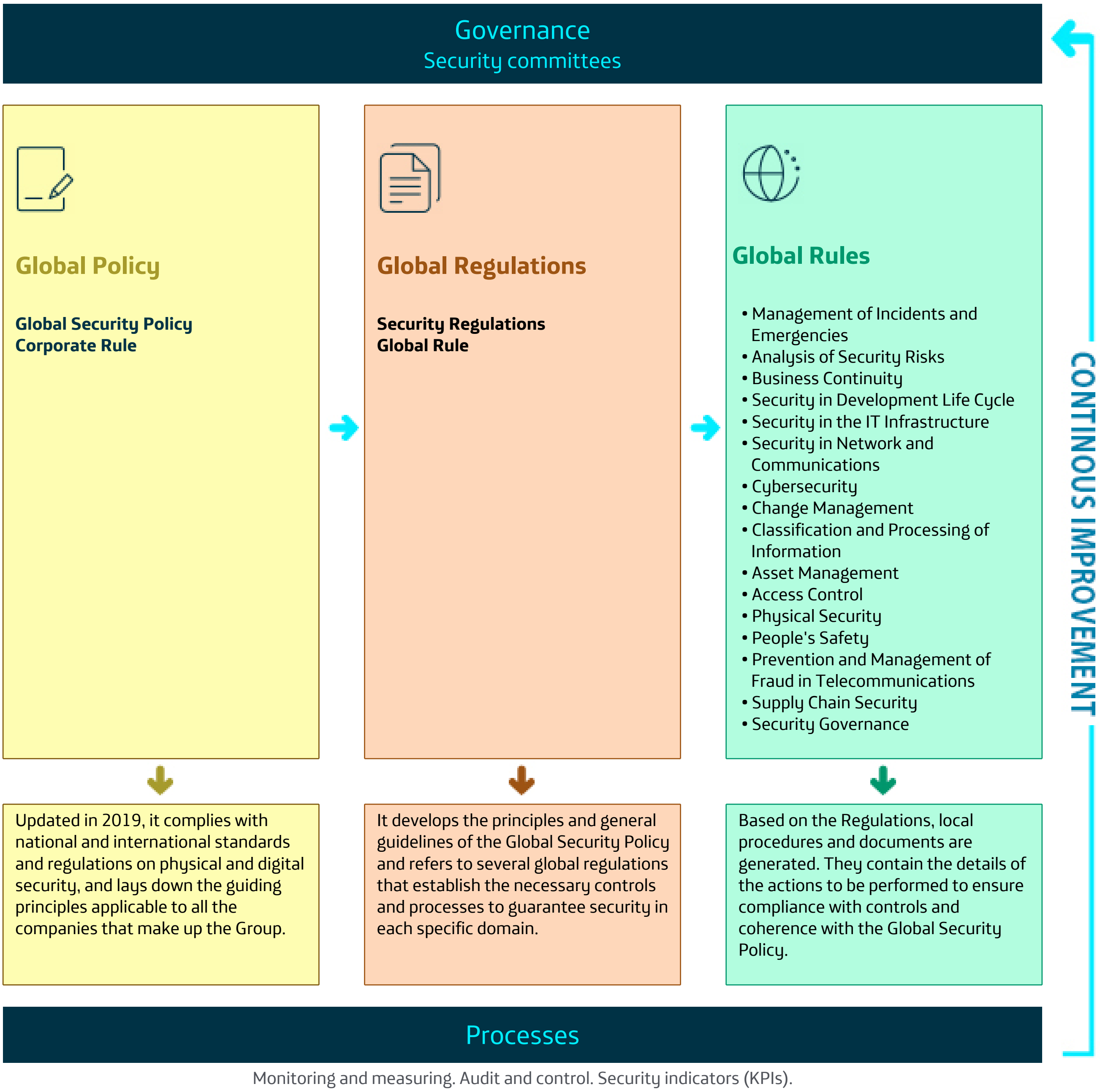
In addition, the Global Security and Intelligence area promotes and drives the Global Digital Security Committee, in which several members of the Company's Executive Committee participate.

Furthermore, Telefónica has a Security Advisory Council involving significant external figures of the Company in the broad field of Security and Intelligence. Its aim is to offer advice based on best industry practices and give its opinion on the Company's strategy in security and intelligence matters.

2.4.3.3. Policies and processes

The security lifecycle aims to protect the Company against potential damage, protecting people and property, and guaranteeing the confidentiality, integrity and availability of the Company's information assets, including services and data. To achieve these objectives, we promote and update different security policies and processes to adapt them to the changing context and new risks as they are identified. This group of processes is included in a Security Management System compatible with international reference frameworks and standards, and integrates a cycle of continuous improvement. Likewise, and following the process of continuous improvement, the policies and processes are adapted to the monitoring and measurement of the activities and processes of the security life cycle.

Security Regulations



Governance
Security committees

Global Policy

Global Security Policy Corporate Rule

Updated in 2019, it complies with national and international standards and regulations on physical and digital security, and lays down the guiding principles applicable to all the companies that make up the Group.

Global Regulations

Security Regulations Global Rule

It develops the principles and general guidelines of the Global Security Policy and refers to several global regulations that establish the necessary controls and processes to guarantee security in each specific domain.

Global Rules

- Management of Incidents and Emergencies
- Analysis of Security Risks
- Business Continuity
- Security in Development Life Cycle
- Security in the IT Infrastructure
- Security in Network and Communications
- Cybersecurity
- Change Management
- Classification and Processing of Information
- Asset Management
- Access Control
- Physical Security
- People's Safety
- Prevention and Management of Fraud in Telecommunications
- Supply Chain Security
- Security Governance

Based on the Regulations, local procedures and documents are generated. They contain the details of the actions to be performed to ensure compliance with controls and coherence with the Global Security Policy.

Processes

Monitoring and measuring. Audit and control. Security indicators (KPIs).

Our security control framework is formalised in official certifications, such as ISO27000 or PCI-DSS, wherever efficient or necessary for customer relations and compliance processes, and we may require our IT service providers to have certified security management systems or ISAE 3402 reports or similar.

2.4.3.4. Lines of action

Security is one of the pillars on which the Telefónica Group's global organisation is built. It is understood as a comprehensive concept that aims to protect assets, interests and strategic objectives, ensuring on the one hand integrity and on the other removing potential threats that could damage value, affect confidentiality, reduce effectiveness or alter operation and availability.

Integral security includes not only physical and operational security (of people and goods), but also information security, cybersecurity, information technology security, network security, business continuity, fraud prevention and any other relevant area or function whose objective is corporate protection against any form of potential damage or loss.

The security activities carried out by the different organisational structures, those responsible for assets and employees are governed by the principles of legality, efficiency, co-responsibility, cooperation and coordination, for whose promotion, management, control and improvement the appropriate mechanisms are to be established.

The Company's Global Strategic Security Plan, reviewed and approved by the Global Security Committee on 26 November 2020, aims to integrate security policy into the broader framework of Telefónica's strategy, and identifies and prioritises the main lines of action and associated resources; for example, Security by Design and Supply Chain Security. In 2020, security measures related to remote access and teleworking were reviewed and reinforced due to the situation caused by COVID-19.

Telefónica's main lines of action in this area are as follows:

- Digital security or cybersecurity
- Physical or operational security
- Security by Design
- Supply chain security

Digital security or cybersecurity

Digital security is a key element of our business. Its ultimate goal is to ensure our resilience, in other words, our ability to withstand and contain attacks so that our business is either not affected at all or, if it is affected, the level is tolerable. This is applied in practices, processes, tools and capabilities that aim to anticipate and prevent cybersecurity risks.

Given the current context of cybersecurity and Telefónica's status as a digital operator, special focus is placed on the following processes:

a.Cyber-intelligence and incident management

We have tools and capabilities for the entire cycle of potential incidents:

- **Anticipation**, before it can affect us.
- **Prevention**, ensuring the protection of both facilities and assets, as well as customer data and identity.
- **Detection**, through twelve Security Operation Centres.
- **Response**, through a network of 15 Incident Response Centres (CSIRT) working in a coordinated manner at local and global level to resume normal service as soon as possible and with the least possible impact.

Our approach to cyber-intelligence is based on a proactive approach, applying knowledge and technology to achieve the required levels of protection by quickly detecting breaches or attacks on assets. We also build the technical and human capabilities needed to respond effectively and quickly to any breach or incident in order to minimise attacks and their consequences.

We have a bug-bounty programme in place with selected industry experts.

We have a global network of Incident Response Centres (CSIRTs) that coordinate to understand and analyse the risks of potential cyber-threats, monitor the serious bugs in the most critical technological assets, establish relationships with other national and international CSIRTs/CERTs in the public and private sectors, detect potential security incidents that affect the organisation's technological assets and respond to and manage security incidents.

In 2020, 1 single high-impact security incident was managed. We consider high-impact incidents to be those that meet certain criteria determined at global level (e.g. economic, legal, service or media impact). In the aforementioned incident there was no leakage of customer data and existing response protocols were followed.

Lessons learned from incidents are a major part of the feedback used in security improvement projects for processes and technological capabilities and platforms.

The CSIRT Network CyberExercise is an initiative by the global CSIRT that offers an evaluation, training and coaching environment specifically designed for incident response teams. It involves teams from Telefónica's international CSIRT network.

We have a global public mailbox via which users can report bugs or threats that could affect Telefónica's technological infrastructure. The mailbox is located in the Global Privacy/ Security Centre. There are also equivalent local mailboxes at each of our locations.

Since 2015 the Company has had various insurance programmes in place to soften the impact a large number of risks could have on the balance sheet. In particular, there is cover for cyber-risks that could cause a loss of income, loss of customers, extra costs or recovery costs for digital assets, among other costs, and cover for technological errors and omissions in the event of claims for damages to customers and third parties in general. The current global insurance limits are:

- Cyber-risks insurance: € 100,000,000
- Technological errors and omissions insurance: € 300,000,000 .

b. Network security

Our approach to networks and communications is based on a good knowledge of our assets and sites, as well as their characteristics and their importance for the business. Accordingly, our networks are properly planned and executed in keeping with applicable security requirements to minimise the risk of downtimes, unauthorised access or destruction.

Telefónica's role as a telecommunications operator makes it essential to improve controls for the security of its own fixed and mobile communications networks and infrastructure and the associated service platforms (e.g. video, IoT). Accordingly, the aforementioned security processes are applied in an integral manner to manage the risks associated with attacks and the exploitation of bugs in networks and protocols. This involves significant activity with our main technological partners and international organisations (e.g. GSMA) to reduce potential impacts. Examples can be found in the work done on 4G/LTE, SS7, BGP and other critical enabling technologies.

It is also worth highlighting the importance of the evolution to 5G and the Company's position in actively contributing to making the new networks as safe as or even safer than their forerunners. The Company's technological developments in this area, such as the evolution of our network virtualisation platform, UNICA NEXT, network splitting and new radio access technologies are considering Security by Design.

Physical and operational security

In the field of operational security, the Company strives continuously to improve its capabilities for the physical protection of infrastructures and assets. Accordingly, it has several ongoing programmes, in particular:

- The interconnection of control centres to create a resilient network that reinforces the availability of infrastructures for surveillance and protection services;
- The management of travel security for Telefónica personnel, which substantially improves response time and mechanisms for dealing with incidents occurring during a business trip;
- The implementation of consistent digital procedures and tools for global security monitoring.

Security by Design

Importance is placed on security from the earliest stages in every business area to make sure it is an integral part of the entire technology life cycle. The approach is based on: the risk management and analysis process; the development of in-house technologies, which make a commitment to innovation and national technology; employee awareness; and the security requirements demanded of our supply chain.

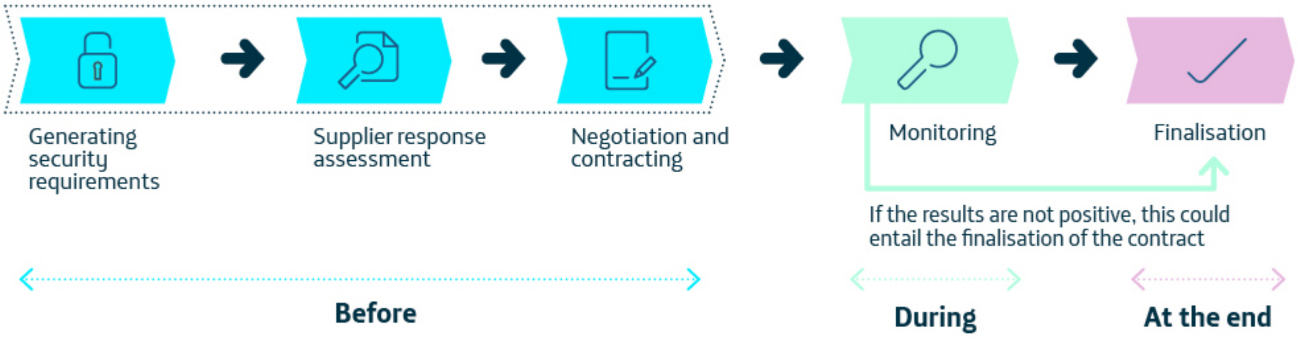
- Design of secure systems: Security requirements are a consideration from the design phase of applications and systems, incorporating controls against known bugs and ensuring that there are no security weaknesses at source. This results in systems and applications that are more resistant to malicious attacks.
- Reception by management bodies of consolidated monitoring and control information for analysis: The analysis is used to define the preventive actions to be included in the strategic plan, considering security by default and from the design phase. It also reviews the aspects required in the Global Security Policy and regulatory frameworks to take into account the appropriate considerations.

Supply chain security

For some years now, establishing a baseline of compliance with security requirements for our suppliers, and identifying the risks associated with the provision of a service/product, has been a priority for the Telefónica Group. This is why in 2020 we continued to support and evolve the implementation of the Supply Chain Security initiative.

This year has been essential in this transformation thanks to the creation of a tool called 3PS+, which allows the entire process of managing security aspects throughout the supplier lifecycle to be digitised. This tool is an application that allows the user to have all the information related to the security aspects of a procurement process and its suppliers before contracting, during and after delivery. Its main characteristics are as follows:

Supply Chain Security Process


Generating security requirements
Supplier response assessment
Negotiation and contracting
Monitoring
Finalisation
If the results are not positive, this could entail the finalisation of the contract
Before
During
At the end

- **Before contracting**, the application allows the user to generate security requirements for new procurement processes that can be interacted with, e.g. by generating and modelling security requirements; uploading the answers given by suppliers; obtaining objective assessments of the level of compliance, etc.

- **During provision of the service**, the user has the possibility of monitoring the security aspects related to the service. To this end, the system generates alerts based on the start date of the service and the selected monitoring period, and allows the user to record relevant information that could pose a risk to Telefónica's assets.

- **After delivery of the service**, the user can control how the provider's output is executed, and mitigate or even avoid the most common security risks at service termination: failure to block physical and logical access, failure to check VPNs/ports/systems used for services, etc.

All Telefónica Group employees worldwide have access to this tool, which simplifies and facilitates not only the obtaining of security requirements, but also the knowledge and management of the risks involved in the provision of a service/product by a supplier.

2.4.3.5. Business continuity and crisis management

Strategy

The Business Continuity function integrates various activities and processes aimed at improving the Company's resilience in all its aspects.

In this area, our priority as a company is to ensure the following in the event of a crisis:

- Protect the integrity of people, ensuring the well-being of employees and collaborators.

- Provide the agreed services to our customers, with the agreed availability and quality.

- Protect and look after the interests of our shareholders and institutional investors.

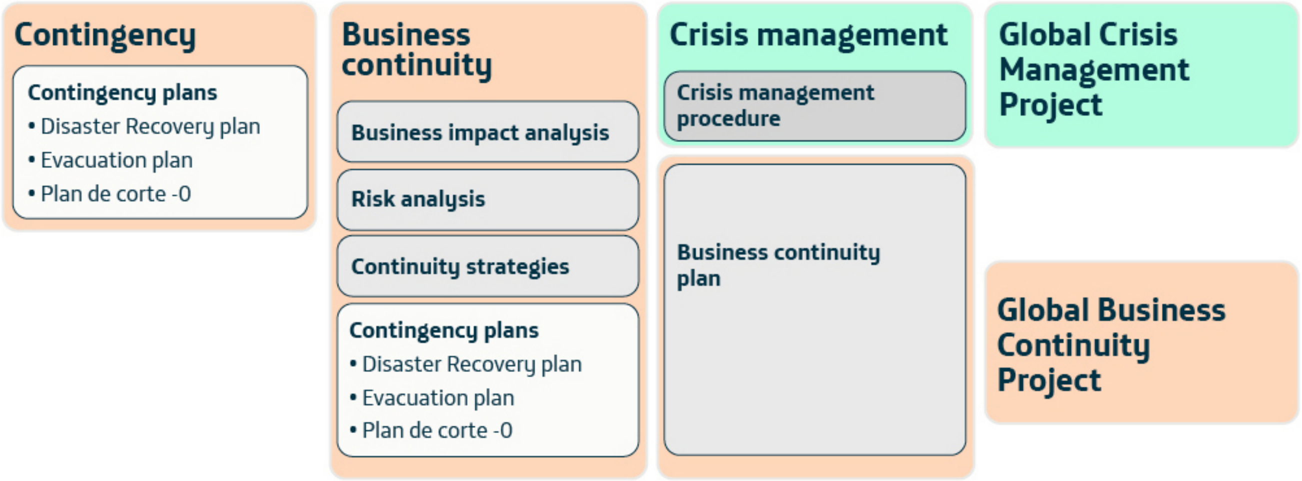
- Comply with our regulatory and legal obligations.

- Protect and secure the business from a sustainability point of view.

The Business Continuity function is included in the Global Security Policy. The details of this function are defined in the Global Business Continuity Regulation and in various pieces of global and local documentation corresponding to each business unit.

To ensure its continued evolution and support from the Company's management, this initiative is included as part of the Global Security and Intelligence Directorate's Strategic Plan in the form of a Global Crisis Management Plan, which in turn is composed of the Global Crisis Management Project and the Global Business Continuity Project.

Global Crisis Management Plan



Contingency

Contingency plans
- Disaster Recovery plan
- Evacuation plan
- Plan de corte -0

Business continuity

Business impact analysis

Risk analysis

Continuity strategies

Contingency plans
- Disaster Recovery plan
- Evacuation plan
- Plan de corte -0

Crisis management

Crisis management procedure

Business continuity plan

Global Crisis Management Project

Global Business Continuity Project

The Company's strategy has evolved in recent years from a distributed model to a global model. This has entailed strengthening the following aspects:

- **Strategic vision:** The global threats facing the Company require global action. Having a strategic vision of the Company's business continuity enables global decisions to be made that result in greater resilience.
- **Effective crisis management:** This entails having a proven crisis management model, common to the entire Company, both in its definitions and in the execution of its procedures.
- **Coordination and collaboration:** The organisational model guarantees, aligns and promotes the homogeneous development of business continuity in the various business units.
- **Standardisation of measurement:** This allows us to measure, without bias, various indicators that show us the degree of maturity from the business continuity point of view, and the level of resilience of the Company. It also allows us to set SMART objectives for the medium and long term.

Each business unit has its own local Business Continuity Office, and all local offices are aligned and coordinated through the global office, functionally located in the Global Security and Intelligence Directorate, which is part of the Company's corporate area.

The Company has a Crisis Management Plan consisting of a Global Crisis Management Project and a Global Business Continuity Project, which is based on international standards such as ISO 22301 for business continuity management and ISO 22320 for emergency management.

For the execution of the Crisis Management Plan: the processes of each of the areas are identified, detecting scenarios that could lead to their interruption; potential treatment plans are considered; the business continuity strategies to be applied are decided; and, if necessary, business continuity plans are generated with the appropriate actions to be taken.

At least 2 global simulations are carried out annually, one to check business continuity mechanisms and another simulating a crisis scenario, unless during this period there has been an opportunity to check the effectiveness or identify opportunities for improvement due to real continuity or crisis management situations.

Governance model

The strategic evolution of the Company's Business Continuity function requires its own corporate governance. To this end, the Global Business Continuity Committee is responsible for making strategic decisions on aspects related to business continuity for the Telefónica Group. This body enables the definition of an overall strategy to take business continuity into account by design, ensure that the necessary resources are available and define where efforts need to be focused.

Similarly, local business continuity committees are defined as the bodies responsible for ensuring business continuity in each business unit. Their function is, on the one hand, to guarantee the implementation of the strategic decisions made at a global level and, on the other hand, to transfer the needs, achievements and maturity indicators that allow a holistic view of business continuity in the Telefónica Group.

The business continuity committees, whether at global or local level, prioritise and focus the resources of this function where they can generate the greatest impact and value for the Company, based on the following focal points:

- Strategic services
- Strategic projects
- Strategic suppliers
- Organisational aspects

Business continuity in the Telefónica Group has evolved from a model distributed among its different business units to a global model through the creation of a Global Business Continuity Office (OGCN according to the Spanish initials) that coordinates the different local Business Continuity Offices (OLCN according to the Spanish initials).

The Global Business Continuity Office is also the vehicle that transfers the different strategic decisions defined by the Global Business Continuity Committee to the Telefónica Group's business units.

On an annual basis, each local Business Continuity Office, under the prism of the Global Business Continuity Project, generates its Statement of Work (SOW). The SOW represents the planning of business continuity work and tasks to be addressed in the next 12 months.

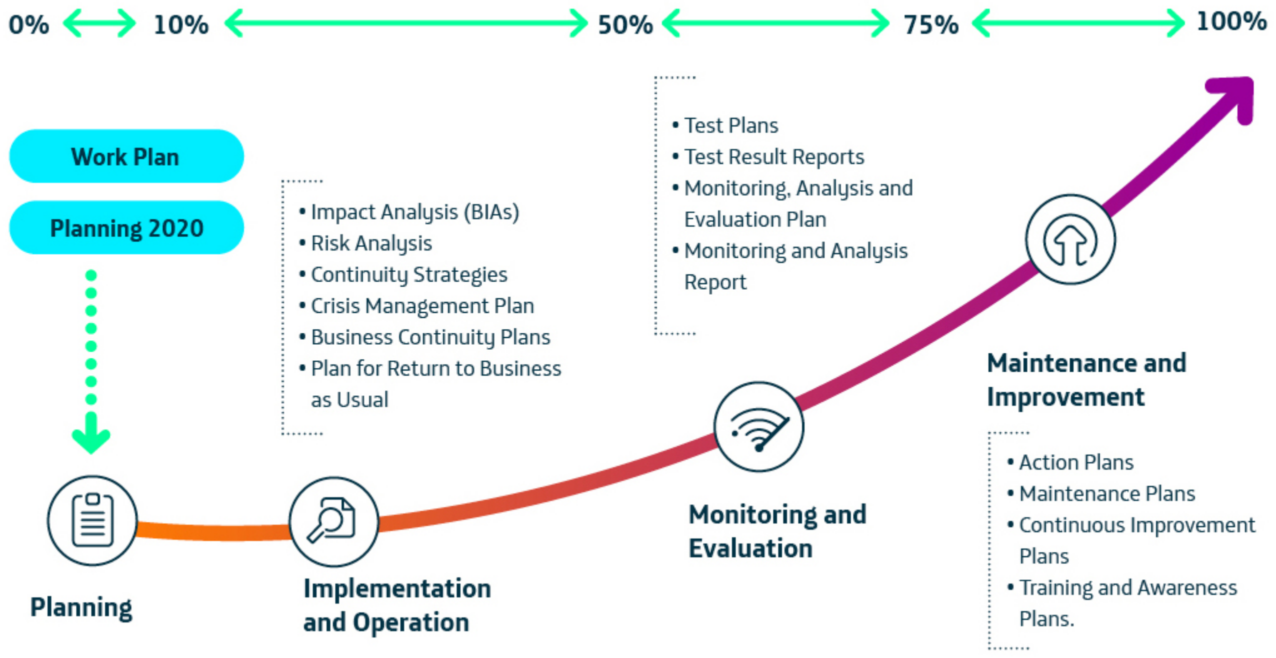
Local Business Continuity Offices also conduct a business impact analysis (BIA), which identifies the most relevant processes or services in relation to their tolerance to unavailability and business impact.

The list of processes, together with their level of relevance, will be taken into account in each local office's decision on the target scope.

Business continuity maturity in the Telefónica Group
The Telefónica Group has established a business continuity maturity model based on four levels and aligned with ISO Standard ISO 22301. The four levels are:

1. Planning: Includes the preparation of a Statement of Work (SoW) detailing the scope of business continuity and a plan of the activities to be undertaken in the relevant year.
2. Implementation and operation: Contains the set of deliverables aimed at establishing and documenting the different existing business continuity mechanisms – impact analyses (BIAs), risk analyses, continuity plans, return to normality plans, etc.
3. Monitoring and evaluation: Assesses the effectiveness of the business continuity arrangements in place by testing them in realistic and bounded scenarios. Indicators are available to assess the performance, maturity level and implementation of the overall business continuity project.
4. Maintenance and improvement: Brings together both lessons learned and opportunities for improvement from business continuity testing and improvement initiatives arising from annual planning.

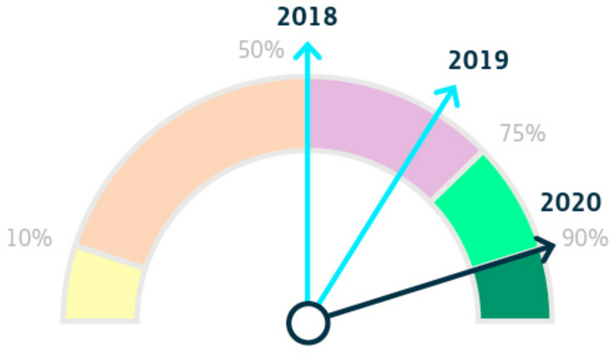
Business continuity maturity model


0%
10%
50%
75%
100%
Work Plan
Planning 2020
• Impact Analysis (BIAs)
• Risk Analysis
• Continuity Strategies
• Crisis Management Plan
• Business Continuity Plans
• Plan for Return to Business as Usual
• Test Plans
• Test Result Reports
• Monitoring, Analysis and Evaluation Plan
• Monitoring and Analysis Report
Maintenance and Improvement
• Action Plans
• Maintenance Plans
• Continuous Improvement Plans
• Training and Awareness Plans.
Planning
Implementation and Operation
Monitoring and Evaluation

In terms of business continuity process management capabilities, this homogeneous maturity model allows the different units to define medium and long-term objectives. It also provides the Telefónica Group with a holistic and consolidated vision that accompanies its strategic decisions.

Over the last few years, the evolution of the Telefónica Group's maturity level has allowed us to reach an optimised level, which means that the defined business continuity mechanisms have been established, tested and lessons learned:

Evolution of the degree of maturity

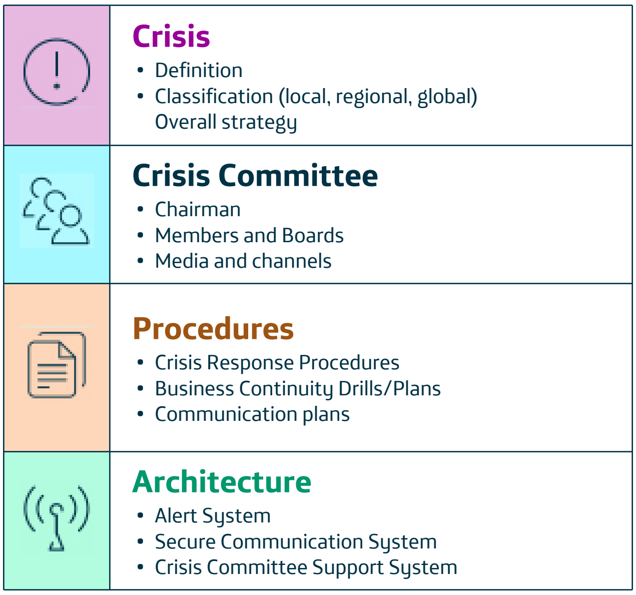


Level of maturity Telefónica Group

Crisis management
The Telefónica Group's Global Crisis Management Project is structured on the basis of four distinct layers.

1. The first layer defines and classifies, in a univocal and homogeneous manner, the crises, their typology and the general strategy for dealing with them in the Company.
2. The second layer defines, in a univocal and homogeneous manner, the roles, responsibilities, means and channels involved in crisis management, as well as the relationship and responsibilities between Crisis Committees.
3. The third layer groups together the procedures, plans and documentation necessary for crisis management.
4. The fourth layer defines, on a global basis, the architecture of warning systems, secure communication and, in general, the aspects related to digitisation that support the activities of the different Crisis Committees.

Layers of crisis management



Crisis
- Definition
- Classification (local, regional, global)
  Overall strategy

Crisis Committee
- Chairman
- Members and Boards
- Media and channels

Procedures
- Crisis Response Procedures
- Business Continuity Drills/Plans
- Communication plans

Architecture
- Alert System
- Secure Communication System
- Crisis Committee Support System

The Global Crisis Management Project provides additional and complementary mechanisms to business continuity, making it possible to manage incidents that have a broad impact on the Telefónica Group.

Three types of crises are described as part of the modelling:

- **Local crisis:** Confined to one organisation or business unit of the Telefónica Group in one country.
- **Regional crisis:** Confined to several countries belonging to the same geographical region.
- **Global crisis:** Present in several companies or business units of the Telefónica Group in more than one country.

Depending on the type of crisis that is triggered, there are active protocols and means of alert, notification, management and coordination, which are known to all those involved in the Global Crisis Management Project.

The main role in crisis management is played by the members of the Crisis Committee, whether global or local. There is a differentiation between permanent members who participate in any activation, ad hoc members who participate depending on the typology of the crisis, and working or support panels for these members.

The Global Crisis Management Project enables the Telefónica Group to:

- Accelerate the decision-making process.
- Enable a unified crisis management model.
- Centralise the receipt of information.
- Act as a unified tactical and decision-making figure.

- Decide how to act based on the crisis scenario being faced and, building on the business continuity aspects worked on previously, avoid making decisions "in the heat of the moment".

- Reliably transmit information about what has happened to customers, authorities, organisations or any other stakeholder.

Finally, it defines the obligation to conduct tests and simulations on different scenarios that could potentially be harmful to the Company. By carrying out these drills, the following actions can be performed and improved:

- Assessing reactions to particular circumstances.

- Assessing the preparation of documentation to support crisis management activity.

- Assessing the coordination mechanisms.

- Preparing Crisis Committee members to take action.

COVID-19

During the exceptional situation generated by COVID-19, the Business Continuity Offices have continued their work to identify the most important processes, both to ensure that they are sufficiently robust and to guarantee the resilience of the Company.

As a result of the pandemic, both the crisis management process and the available resources have been activated satisfactorily, managing to maintain at all times the service levels agreed with customers and adapting the network capacity to changes in demand. This scenario has enabled the practical application of the Global Crisis Management Project in all Telefónica Group business units, strengthening the common management model, the standardisation of the architecture that supports this function, the digitisation of crisis alert processes and the training and awareness of critical personnel.

The COVID-19 pandemic, which has affected all the territories in which the Telefónica Group is present, has led us to work ceaselessly on coordination, management and decision-making. All areas related to business continuity and crisis management in the Telefónica Group have demonstrated their readiness to deal with such an exceptional situation.

More than 90% of employees have teleworked without notable incidents, more than 80 Crisis Committees and simulations have been activated at regional and global level, there have been hundreds of meetings involving Crisis Committees and Drills at local level (with a frequency adapted to the situation) and there has been a very high level of coordination between the different areas and business units, among other achievements. All these place the Telefónica Group at a very high level of maturity in terms of its ability to react to critical events.

Furthermore, the Telefónica Group has been a fundamental part of society as a whole from the point of view of securing communications. This fact has been recognised and valued by various entities and bodies in all the countries in which the Telefónica Group is present.países donde el Grupo Telefónica tiene presencia.

The following are the four events discussed by the Crisis Committee, in addition to the (global) pandemic:

Events discussed by the Crisis Committee

CHILE (LOCAL)	February 2020
Crisis	Cable stolen (affecting Voice + Internet services)
Type of crisis	Cable stolen
Impact	There was a growing wave of cables being stolen, impacting the copper network. It affected 573 cable points nationally and left over 45,000 customers without service (Voice+Internet). This mainly affected the metropolitan region, although the damage was concentrated in five regions in the central-southern area of Chile: Metropolitan RM, Valparaíso V, O'Higgins VI, La Araucanía VIII and Los Lagos X. There was an economic, reputational and regulatory impact. There was no impact of any kind on people.
Actions	The Crisis Committee was activated on 14 February 2020. This committee is made up of a multidisciplinary team from the Call Centre, Technical Customer Service (ATC), Network Infrastructure, Quality and Customer Experience, Enterprise and Security areas. When the committee was activated there were a total of 573 cable points affected, which left 45,576 customers without voice (STB) and Internet (ADSL-VDSL) services. Daily working group meetings were held to detect, analyse and implement action plans to mitigate the cable thefts in the aforementioned regions. Following the improvements obtained by initiatives implemented at different stages of the process, a request was made to close the mass failure crisis caused by cable thefts on 31/08/2020, due to the decrease in the number of customers affected.

PERÚ (LOCAL) June 2020	
Crisis	Fire in the Chiclayo office – Department of Lambayeque
Type of crisis	Fire
Impact	Due to the extent of the impact, the main priority was to restore home services (telephony, Internet and TV) mobile services and State services (health, police, among others). The fixed line network was 47% affected, Internet 50% affected and mobile service 47% affected. There was a level 2 impact on the business service owing to the fact that the incident occurred on a Saturday and by decree of the Peruvian government shops were closed on weekends due to the effects of the COVID-19 pandemic. Communications were re-routed through the Piura and Trujillo nodes. The regulator and authorities were notified in a timely manner, so as not to incur any penalties.
Actions	With the restoration of the power supply, services returned to normal at 12:30 p.m.

BRASIL (LOCAL) September 2020	
Crisis	Unavailability of voice and charging services due to data centre power failure
Type of crisis	Power failure

Impact	Unavailability of voice and charging services for 50% of the prepaid customer base and loss of control of the following units in the Federation:
	a. PR (Paraná - area codes 41 to 46);
	b. RS (Rio Grande do Sul - area codes 51 to 55);
	c. SC (Santa Catarina - area codes 47 and 48);
	d. SP (São Paulo - area codes 13 and 16).

Actions	As the demonstrators' reaction intensified, the Crisis Committee was convened to make the appropriate decisions and inform all employees that they were authorised for teleworking. Instructions were also given to protect their physical safety.

COLOMBIA (LOCAL) November 2020	
Crisis	Hurricane Iota
Type of crisis	Unavailability of infrastructure – natural disaster
Impact	On 16 November 2020, the Category 5 hurricane Iota passed over the archipelago, with the greatest impact on the island of Providencia, where 98% of the island's infrastructure was devastated. On the island of San Andrés, there were also strong impacts on infrastructure, although to a lesser degree. The islands had 28 mobile network stations, 6,123 fixed voice customers and 1,327 broadband customers. After the hurricane on San Andrés island 65% of mobile services, 5% of voice services and 18% of broadband services were affected. The island of Providencia was 100% affected and cut off from communication
Actions	On 14 November, alerted by the hurricane forecasts, the Network Service Contingency Plan was activated in order to deploy preparatory measures to respond in the shortest possible time to the impacts that could occur. Thus, with the support of different entities, it was possible to provide personnel and resources to begin the recovery work. For San Andrés, by the third day, most of the island's services were restored, although due to the damage to a large percentage of the 2G radio base, work began on a plan to modernise the island's mobile services with the implementation, by 31 December, of 10 new LTE radio bases. In the case of Providencia, Telefónica was the first operator to re-establish communications on Sunday 22 November at 7:00 pm. Subsequently, we continued the recovery of coverage on the island with 4 other sites where temporary 3G solutions were deployed.

2.4.3.6. Security services

At the end of 2019, the new Telefónica Tech division was created. This encompasses the Cybersecurity, Cloud and IOT/Big Data technology businesses. In this way, Telefónica Tech brings together businesses with high growth potential. Leveraging internal knowledge of technologies, networks, systems and digital processes allows us to generate business opportunities and round out our digital service offering to our customers.

Telefónica's cybersecurity unit is called ElevenPaths. We make security more human and give people the confidence and peace of mind they need.

In 2020, ElevenPaths reached €448 million in turnover.

As providers of intelligent managed security services in a world where cyber-threats are inevitable, we cover each phase of a threat —i.e. preparation, prevention, detection, response and recovery— to reduce attacks, protect digital assets and services, and thus ensure the cyber-resilience of our customers and their businesses. We anticipate the most sophisticated and frequent attacks.

Therefore, we need to be increasingly receptive to cybersecurity measures and redefine our strategy on cyber-resilience. To this end, we dedicate all our experience and efforts to creating innovative cybersecurity products in order to stay ahead of the attackers that have become a growing threat in our digital lives.

Since the creation of ElevenPaths, we have combined the development of innovative, patented technologies with the technologies of the main market players (partners) to provide unique solutions that allow us to be prepared for and respond to any type of attack.

Global cybersecurity services are designed to continually improve the effectiveness of our security infrastructure. To this end:

- We work to develop new security services and capabilities designed to help protect businesses and people from threats and bugs in the environments in which they operate.

- We collaborate and exchange information about threats in real time with the main agencies and entities, such as the European Commission, the Cyber Threat Alliance (CTA), ECSO, EUROPOL and INCIBE.

- We manage more than 5 million endpoints and monitor more than 16,500 devices with an integrated global SOC operating from 11 locations across Europe and the Americas. Thanks to our intelligent and automated platforms, we can act efficiently. Telefónica's SOCs have been strengthened by the formation of the world's largest telecommunications security alliance with Etisalat, Singtel and Softbank, which allows us to position ourselves with a complete portfolio of services. We have experts ready to help our customers face new digital challenges in a world of uncertainty.

- We have six Innovation and Development Centres in Spain, Buenos Aires and Miami, where the technology developed internally by ElevenPaths was born.

- We created Telefónica Tech Ventures in 2020, the investment vehicle for startups and companies focused on cybersecurity, driven by ElevenPaths and Telefónica Innovation Ventures. Its objective is to detect disruptive innovation in cybersecurity, especially in the fields of threat intelligence, cloud security, data protection and artificial intelligence applied to cybersecurity.

- Also in 2020 we invested in established international companies such as Nozomi Networks and in Spanish startups such as Alias Robotics.

Thanks to these collaborations, alliances and our own experience, ElevenPaths is present across the security chain of value and has a portfolio of comprehensive security solutions for the Internet of Things (IoT) world, solutions for cloud security, identity and privacy, anti-fraud, industrial cyber-security, secure mobility, digital exposure, risk management and regulatory compliance. All this effort has earned us the acclaim of being the leading industry analysts in the field.

2.4.4. Artificial intelligence

Artificial intelligence (AI) and Big Data are booming. They can be applied to areas as diverse as content recommendations, chatbots, image recognition, machine translation, fraud detection, medical diagnostics, autonomous vehicles, law, education, transport and logistics, to name but a few. They are not only used in business, but also for social purposes such as better understanding and reducing the effects of climate change, natural disasters, pandemics and migration.

However, concerns have recently been expressed about the use of AI, in particular in relation to possible discrimination, the lack of interpretability of algorithmic findings and the lack of transparency of personal data used. To address these potential issues, Telefónica published its Artificial Intelligence Principles in October 2018 and has since worked on their implementation through the following approach:

- A *strategic model (strategy)* that gives a strategic vision of how the Artificial Intelligence Principles fit with the Company's values and objectives.

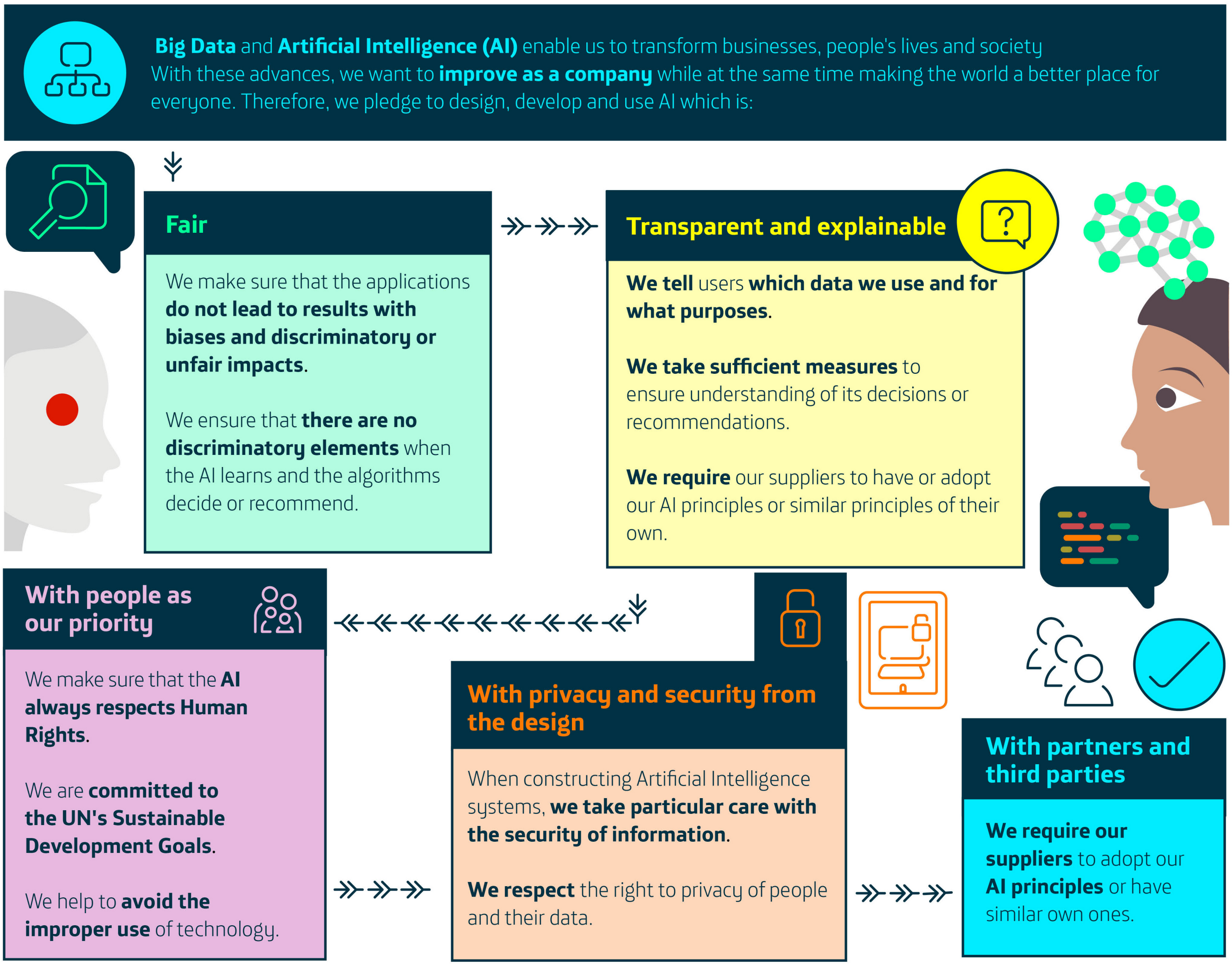
- An *organisational model (governance)* that defines the necessary roles and the relationships between them, in accordance with the corporate structure, to implement the Artificial Intelligence Principles.

- An *operational model (lines of action)* that defines the main procedures together with the roles of those responsible for the tasks to be carried out.

2.4.4.1. Strategy

Telefónica has a firm commitment to human rights, as indicated in our Business Principles and our Human Rights Policy. Technology must contribute to creating a more inclusive society and offer better opportunities for all, and AI can contribute to these goals. In order to guide the Company in its application of AI and Big Data across all lines of business, the Executive Committee adopted our Artificial Intelligence Principles in October 2018. Based on these Principles, we undertake to design, develop and use artificial intelligence (1) in a fair and non-discriminatory manner; (2) in a transparent and explainable way; (3) with people as a priority; (4) with Privacy and Security by Design; and (5) with suppliers and partners that are committed to these or similar ethical standards in the field of artificial intelligence.

Our Artificial Intelligence Principles



Big Data and **Artificial Intelligence (AI)** enable us to transform businesses, people's lives and society
With these advances, we want to **improve as a company** while at the same time making the world a better place for everyone. Therefore, we pledge to design, develop and use AI which is:

Fair

We make sure that the applications **do not lead to results with biases and discriminatory or unfair impacts**.

We ensure that **there are no discriminatory elements** when the AI learns and the algorithms decide or recommend.

Transparent and explainable

We tell users **which data we use and for what purposes**.

We take sufficient measures to ensure understanding of its decisions or recommendations.

We require our suppliers to have or adopt our AI principles or similar principles of their own.

With people as our priority

We make sure that the **AI always respects Human Rights**.

We are **committed to the UN's Sustainable Development Goals**.

We help to **avoid the improper use** of technology.

With privacy and security from the design

When constructing Artificial Intelligence systems, **we take particular care with the security of information**.

We respect the right to privacy of people and their data.

With partners and third parties

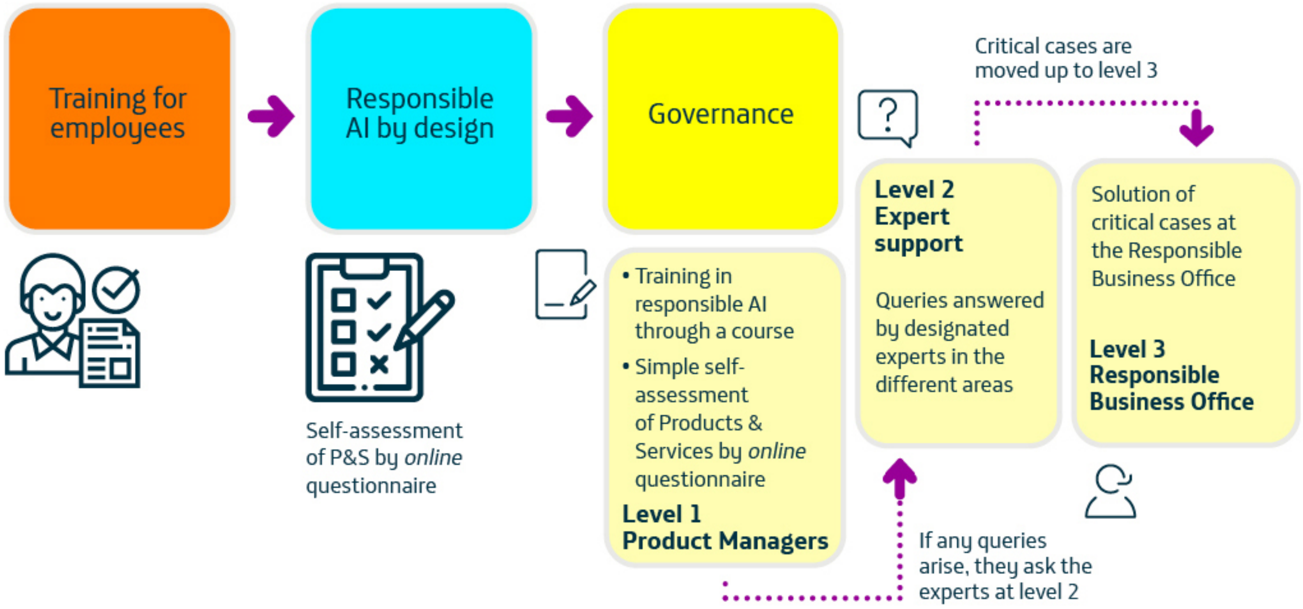
We require our suppliers to adopt our **AI principles** or have similar own ones.

2.4.4.2. Governance

We are implementing responsible AI through an organisational and relationship model that defines which Company departments are involved, what their roles are and how they relate to each other to achieve the responsible use of AI.

We promote a self-assessment approach with an on-demand scaling model. There is a three-step scalability process illustrated in the following graphic.

Implementation of the Artificial Intelligence Principles


Training for employees
Responsible AI by design
Governance
Self-assessment of P&S by *online* questionnaire
• Training in responsible AI through a course
• Simple self-assessment of Products & Services by *online* questionnaire
Level 1
Product Managers
Level 2
Expert support
Queries answered by designated experts in the different areas
Solution of critical cases at the Responsible Business Office
Level 3
Responsible Business Office
Critical cases are moved up to level 3
If any queries arise, they ask the experts at level 2

The product managers/developers who buy, develop or use AI should carry out a simple self-assessment when designing the product/service they are developing by means of an online questionnaire. The self-assessment explicitly addresses the potential human rights risks associated with the use of artificial intelligence. This self-assessment is embedded in a three-tier governance model supported by a wider expert community. If a product manager/developer (Tier 1) has concerns about a possible adverse impact of a certain product or service after completing the self-assessment, these concerns will automatically be raised to a multidisciplinary expert group of the Company (Tier 2), who together with the product manager/developer, will try to solve the problem. In case of a potential risk to human rights and/or the Company's reputation, the matter will be escalated to the Responsible Business Office, which brings together all relevant department heads at global level (Tier 3).

2.4.4.3. Lines of action

The operating model describes the procedures for implementing the responsible AI approach in the Company's day-to-day business. Integrated within a broader vision of Responsibility by Design, it includes a methodology called "Responsible Use of AI" inspired by existing methodologies in Privacy and Security by Design. The operational model consists, inter alia, of:

- Training and awareness-raising activities: Telefónica has developed courses related to AI and ethics that are accessible to all employees through the corporate portals and in three languages (Spanish, English and Portuguese).
- The online self-assessment questionnaire: Each AI principle is put into practice through a series of questions and a series of recommendations. The questionnaire is available online in Spanish and English, and is part of the Telefónica Group's global Responsibility by Design initiative.
- A set of technical tools to help answer the questions: As some of the questions in the questionnaire are impossible to answer without specific tools, our methodology includes both internal and external (mostly open source) tools.

Go to the chapter on Clients

2.4.5. Responsible use of technology

2.4.5.1. Strategy

The life our children lead is now a digital life. When we accept this, we will be able to integrate and adapt our long-standing educational traditions to an ecosystem in which the analogical arm has lost its hegemony. It is not a question of inventing anything new, but rather of continuing to educate in values, accompanying and setting an example, generating spaces for dialogue and discovering the advantages and disadvantages of our use of technology together. We need to learn that there are times for connecting to the Internet and times for connecting with other people.

Precisely because of this, and because Telefónica is convinced that it is people who make sense of technology and not the other way round, we have drawn up a global strategy based on the promotion of a responsible and intelligent use of the Internet and connected devices in all areas of our lives, but with special emphasis on the protection of children and teenagers.

2.4.5.2. Governance

The Sustainability and Quality Committee of the Board of Directors of Telefónica, S.A. is responsible for the development of the Global Responsible Business Plan, which includes the responsible use of technology and a special focus on one of the most vulnerable groups: minors.

Reflecting the Company's firm commitment to this group, the protection of children and teenagers is set out in the Responsible Business Principles and various corporate policies, such as the Diversity Policy, the Responsible Communication Policy and the Supply Chain Sustainability Policy.

2.4.5.3. Lines of action

Our commitment to and strategy for protecting minors on the Internet and promoting the responsible use of technology take the form of six lines of work:

Alliances with stakeholders

Ensuring a more secure Internet is a task we cannot tackle alone. At Telefónica, we work with sectoral and civil society partners to make young people aware that the Internet is an open window of opportunity, but also that there are risks that need to be managed.

In this regard, we emphasise our collaboration with:

- National law enforcement forces, as well as support for the different national reporting lines (Equipo Niños, Alianza por la Seguridad en Internet, Safernet, Te Protejo, the Centre for Child Protection on the Internet, Alerta Amber and INADI, etc.)
- NGOs, national associations (Pantallas Amigas, Safernet, UNICEF, Faro Digital, NSPCC, RedPapaz, Argentina Cibersegura, Nativo Digital, Brave Up, Colegium, Fundación Tecnología Responsable, Mamá Digital, Asociación de Padres de Familia, Fundación Ideas para la Infancia, Comisión Unidos vs la Trata, Fundación Sonrisa, Aldeas SOS Ecuador, ChildFund Ecuador, Puntos México Conectado, El Consejo Ciudadano, Luchadoras AC, Moders, Sin Trata A.C. and FEISS (Fundación Ecuatoriana por un Internet Sano y Seguro), etc.).
- Actions with key stakeholders in the area of online protection for children and teenagers (Inhope, Insafe, ANATEL, AECI Asociación Ecuatoriana de CiberSeguridad, CONNA, UNODC, Asociación Ecuatoriana de Protección de Datos, Red de Aliados por la Niñez, Zentrum für Kinderschutz im Internet, INAI, ITAIPUE, Red Contra la Pornografía Infantil, Capital Humano Social CHS, Comunidad de Divulgadores de Conocimiento Científico KUNA, Fundación Habla, End Violence Against Children and Gobiernos, etc.).

Telefónica is also part of the following alliances to promote the sharing of best practices and specific actions for the proper use of the Internet at global level:

- Alliance with the GSMA to combat content involving the sexual abuse of minors.
- The ICT Coalition.
- Alliance for the greater protection of minors online.

Locally, the Company participates in numerous working groups for the responsible and intelligent use of technology by young people: Digitales (Spain), Convivencia Escolar Working Group - Ministry of Education (Chile), TIC e Infancia Working Group (Colombia), Generación Única UNICEF (Argentina), Accesibilidad y Uso de las TIC Working Group - Ministry of Education (Ecuador), Internet seguro para todos y todas Working Group (Mexico).

Blocking of content

In the proactive fight against content showing images of the sexual abuse of minors on the Internet, Telefónica blocks these materials following the guidelines and lists provided by the Internet Watch Foundation in the following countries: Chile, Ecuador, Spain, Mexico, Peru, the United Kingdom, Uruguay and Venezuela. Telefónica Colombia does the same through MINTIC and DIJIN. The procedure complies with network neutrality, the right to free expression and, above all, current regulations at all times, and the blocking of content is also coordinated with the corresponding police forces and other public bodies.

The audiovisual environment

The way people consume TV content has changed; however, it is no surprise to anyone that both children and teenagers make increasingly intensive use of audiovisual content. Screens also play a fundamental part in their personal, social and civic development, which is why Movistar believes it is vital to:

- Ensure that our programming protects children from potentially inappropriate content;
- Establish the necessary tools to make good use of

television, making sure parents have the effective technical resources to exercise their responsibility over the televisual content their children watch;

- Promote digital literacy among children and their families in order to leverage the potential of audiovisual media, making them aware of the need for responsible and intelligent use of screens.

That is why we have included the following initiatives in our operations:

- Labelling and cataloguing of content by age and type of content.
- Parental controls, parental PINs and purchase PINs on the device so that customers can block channels and content on demand for minors;
- Presentation of specific adult content in a separate section with a special PIN required to access it;
- Information on responsible TV use on the device itself and on the commercial website, as well as other awareness-raising activities on the proper use of screens.
- Movistar Junior Application: Children's app for smartphones and tablets (iOS and Android) via which children can enjoy Movistar+ children's content in a safe and secure environment. Some of the functionalities of the application include: children's zone with live TV channels; children's series on demand; videos of activities; musical content; and parents' zone, from which families can carry out their desired configuration actions – parental PINs, definition of the age range for which the content will be available (up to 4 years, from 5 to 7 years and/or from 8 to 12 years), language of the content, consumption times and/or time zone of use.

Products and services

Although we firmly believe that nothing can replace the mediating, educational work of an adult in the responsible use of technology, when this is not possible, we will always have the support of technology. To this end, we are committed to the promotion and development of products and services that help families successfully face the challenges of the digital world:

- Parental controls: Vivo Filhos Online (Brazil), Qustodio (Spain, Chile), Control Parental Movistar TV (Venezuela).
- Security solutions with parental control functionalities: Smart WiFi (Spain).
- Other services (anti-virus, personalised packs): Conexión Segura (Spain, Argentina, Chile), O2 Protect (Germany), Vivo Protege (Brazil), Localizador Familiar (Argentina), Seguridad Dispositivo (Spain), Seguridad Total (Chile, Colombia), Seguridad Total + Conexión Privada Móvil (Argentina), McAfee Seguridad Digital (Brazil) and McAfee Mobile Security Plus (United Kingdom).

Working together with our suppliers

Together with our suppliers, we evaluate the implementation of the basic parameters for the protection of minors, especially in the field of security, from the design of terminals to operating systems.

We ask device manufacturers and operating system providers to ensure the following:

- The inclusion of mechanisms that protect children and teenagers (parental controls, age restrictions, approval systems for the installation of applications, protection systems for purchases, limits on the use of applications and devices, etc.);
- The incorporation of self-monitoring mechanisms, known as "digital well-being", to enable better use of devices and offer user options to reduce dependence; The provision of regular security updates to protect customers from new risks and threats that are constantly emerging and endangering users' data and privacy while extending the lifetime of devices.
- The inclusion of functionalities that help the user to reduce distractions due to misuse of the mobile phone at the wheel (voice operation, muting of notifications, etc.).

Education and awareness initiatives

We continually talk about the challenge of being aware of every technological development that appears on the market today. This does not just mean hearing about the most modern versions of gadgets, the latest in robotics or artificial intelligence, but, because each advance puts us all, old and young alike, before a new educational challenge, it means we need to know how to use technological developments to our advantage.

Being fully aware of the situation, Telefónica is committed to developing training and awareness-raising initiatives for the general public in order to facilitate coexistence in an increasingly digital society:

The Dialogando portal is an example of this. The initiative has been implemented in 10 countries in which the Company operates and helps society at large to reflect on how we use technology in our daily lives thanks to resources prepared by a committee of experts in different issues related to digital life.

A hundred awareness initiatives have been carried out on the following topics: use of technology during the pandemic, grooming, sexting, cyberbullying, the digital divide, cybercontrol and violence, tolerance on the Internet, digital well-being, responsible driving, online fraud, data privacy, digital identity, fake news, eSports and gaming, digital leisure, etc. More than 166 million people have been reached through these actions, with the help of collaborators such as Club de Malasmadres, FAD, iWomanish, Gonvarri, Faro Digital, RedPapaz, Sin Trata A.C., Fundación Habla, CHS Alternativo, NSPCC, among many others.

2.4.6. Cross-cutting digital trust issues

2.4.6.1. Internal control

In order to address and comply with national legal provisions related to local data protection and privacy laws and regulations, within the Annual Plan 2020, a total of 10 specific audits were carried out to verify compliance and identify best practices in data protection issues.

The most relevant aspect in our European operators, which are affected by the new data protection legislation (GDPR), has been to review the implementation of the Governance Model. In the rest of the countries affected by local data protection laws, the most important aspects reviewed were: verification of the application of security measures in the processing of personal data, verification that the integrity and quality of the information is ensured, and verification that the consent of users has been obtained for the processing of their personal data.

The Annual Plan also promoted auditing work related to cybersecurity and security in networks and systems, with the aim of validating the level of logical access and the integrity of the information and content stored in the elements that make up our networks and systems. In 2020, 65 works of this nature were carried out.

2.4.6.2. Training and awareness-raising

In 2020, 80,222 attendees completed training on privacy, data protection, security and cybersecurity. A total of 105,700 hours of training were provided.

In addition, we have been reinforcing communication and awareness-raising programmes on different channels to ensure

2.4.6.3. Stakeholder relations

Telefónica actively participates in various international organisations and forums, most of which are multipartite. Highlights in 2020:

Internet Governance Forum (IGF)

Our Director of Public Policy and the Internet completed the maximum three-year term as a member of the Advisory Group (MAG) at the end of 2020. Its main objective is to advise the Secretary-General on the programme and schedule of the Forum's meetings.

This year we participated in the 15th edition of the IGF, held online for the first time in its history under the organisation of the United Nations with the theme "Internet for Resilience and Human Solidarity", which highlighted the adoption of the Internet as a tool with which to address the crisis associated with COVID-19 and how to address the barriers that limit its adoption and have resulted in increased inequalities most evident during the pandemic. Among others, we participated in the workshop #128 Global Crises and Socially Responsible Uses of Data and in the Pre-Event #30 From Principles to Implementation: Artificial Intelligence and the Role of the Private Sector.

Internet Governance Forum in Spain

This focused on the debates surrounding digitisation and sustainability in a post-COVID-19 world, the social benefits of data use, the use of technology in the fight against COVID-19, its social impact and how to advance digitisation and sustainable development, and the geopolitics of technology. among others.

Global Network Initiative (GNI)

We have been participating in this multi-stakeholder organisation since 2017 to advance the protection and promotion of freedom of expression and privacy in the ICT industry.

To this end, we reach agreements on joint strategies and positions on the rights of freedom of expression and privacy. Several online events were organised this year with a special focus on the impact of COVID-19 on the use of tracking technologies and government requests affecting the rights to freedom of expression and privacy in different regions of the world.

Council of Europe

We are members of the partnership established in 2017 by digital companies, operators, sectoral organisations and the Council of Europe for the promotion of digital rights. In 2020 we actively participated in the working group established by the Ad Hoc Committee on Artificial Intelligence (CAHAI) to prepare a preparatory study on the regulation of artificial intelligence in the fields of human rights, democracy and the rule of law, which will serve as a basis for a future proposal of the Council of Europe in this area.

Internet & Jurisdiction

We cooperate with this multi-stakeholder organisation that focuses on the jurisdictional issues raised by the cross-border nature of the Internet by facilitating a structured dialogue process among its members to enable the development of global standards that facilitate transnational cooperation and policy coherence.

In 2020, we actively participated in the preparation of the regional status report on Latin America that was carried out with the Economic Commission for Latin America and the Caribbean (ECLAC) and Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). It is the first and most comprehensive report in the region to identify the different policy trends surrounding the cross-border nature of the Internet and how it affects different stakeholders, such as governments, businesses and civil society.

Cybersecurity Tech Accord

Telefónica is a founding member of this private sector initiative. It is the joint effort of more than 140 companies from around the world whose main objective is to protect Internet users against the growing evolution of cyber threats. Raising awareness among users about the adoption of cyber health measures and among governments about the need to adopt responsible cybersecurity measures are the other main tasks carried out by the organisation.

fAIrLAC Initiative

Telefónica is once again participating in the Inter-American Development Bank's fAIrLAC initiative, together with other technology partners. The objective is to promote the development of ethical and transparent AI in public services in the Latin American region.

In 2020, despite the COVID-19 pandemic, progress has been made in developing several use cases for responsible AI in health, and a new hub was inaugurated in Medellín to promote the use of AI in gender diversity policies.

Telefónica is also involved in promoting the use of AI in employment policies, contributing the use case of Fundación Telefónica's Destination Employment Programme in Chile.

OECD

We are a member of Business at the OECD, where our Director of Public Policy and the Internet is Deputy Chairman of the Digital Economy Committee. In 2020 we continued to collaborate with the Artificial Intelligence Group (AIGO), and on the review of broadband and digital market recommendations in Brazil.

EU Expert Group on B2G Data Sharing

We participate in the European Commission's Expert Group on Business-to-Government (B2G) Data Sharing.

The European AI Alliance

Our Chief AI & Data Strategist is a member of the European Commission's European AI Alliance, a platform for open discussion on artificial intelligence issues and their impact.

GSMA & ETNO AI Initiatives

We are members of the GSMA (Global System for Mobile Communications) Task Force on AI for Impact and the ETNO (European Telecommunications Network Operators' Association) Task Force on Artificial Intelligence.

Digital Deal

In July 2020 we published our Digital Deal (https://www.telefonica.com/es/web/public-policy/pacto-digital-de-telefonica) to better rebuild our societies and economies after the pandemic. Following on from the 2018 Manifesto (https://www.telefonica.com/manifiesto-digital/), the Digital Deal promotes the establishment of rules of the game adapted to the new post-COVID-19 reality in order to avoid inequalities in the digital world, promote access to next-generation connectivity and protect human rights from technological threats. It is a Digital Deal that, once again, focuses on people and is based on dialogue and agreement between administrations, society and business. It is built around five priorities:

- **Boosting digitisation for a more sustainable society and economy;**
- **Addressing inequalities by investing in digital skills and adapting the welfare state;**
- **Building inclusive and sustainable connectivity;**
- **Ensuring fair competition by modernising fiscal, regulatory and competition frameworks;**

Improving trust through ethical and responsible use of technology.

2.4.7. Milestones 2020 and Challenges 2021 GRI 418-1

> Milestones 2020:

In 2020 we achieved 100% compliance with each of the following goals:

- To establish local privacy centres in 100% of countries.
- To digitise the entire management process related to security aspects throughout the entire life cycle of suppliers.
- To implement the Artificial Intelligence Principles in the Company through a global governance model.
- To develop new lines of action that allow us to address the responsible use of technology and the protection of minors on the Internet.
- To form collaborations/alliances that allow us to deepen the scope of our awareness-raising actions in the field of responsible use of mobile phones at the wheel.

We also reached the following milestones:

- We published Telefónica's Digital Deal.
- We reviewed and reinforced security measures related to remote access and teleworking.

> Challenges 2021:

- To update the Global Transparency Centre.
- To progress in implementing the digitisation of privacy.
- To digitise business continuity management processes.
- To continue implementing the Artificial Intelligence Principles in the Company.
- To develop new formats and channels to communicate messages related to child protection and responsible use of technology that allow us to connect more and better with different audiences.

Summary of key indicators

Indicators	2019	2020
Number of attendees on training courses in data protection and cybersecurity	54,991	80,222
Number of hours of training in data protection and cybersecurity	104,558	105,700
Number of open procedures for data protection issues	66	61
Number of fines for data protection issues (*)	22	15
Sum of fines (euros) for data protection issues (*)	243,595	328,594
Number of enquiries/complaints on data protection/privacy issues in the Responsible Business Channel	6	15
Número de consultas/ reclamaciones en temas de Libertad de Expresión en el Canal de Negocio Responsable	0	0
Number of internal audits in data protection and cybersecurity	69	75
Number of external audits in the area of product and service security (**)	13	10
Number of high-impact information security or cybersecurity incidents/breaches that have affected personal data of customers	1	0
Scope of training and awareness initiatives on the responsible use of technology (people)	223,725,282	166,470,613

(*) Following the application of the “firm resolution/final decision” criteria regarding fines, one ruling/fine in Brazil has been moved from 2019 to 2020.
(**) Products and services that are audited: Vamps, Cyberthreats, AntiDDoS, Monitorización de seguridad, Navegación segura, Redes Limpias, Trafico Limpio de Correo, UTM Gestionado, WAF as a service, Soporte y Gestión de Dispositivos.