2.4. Confianza digital

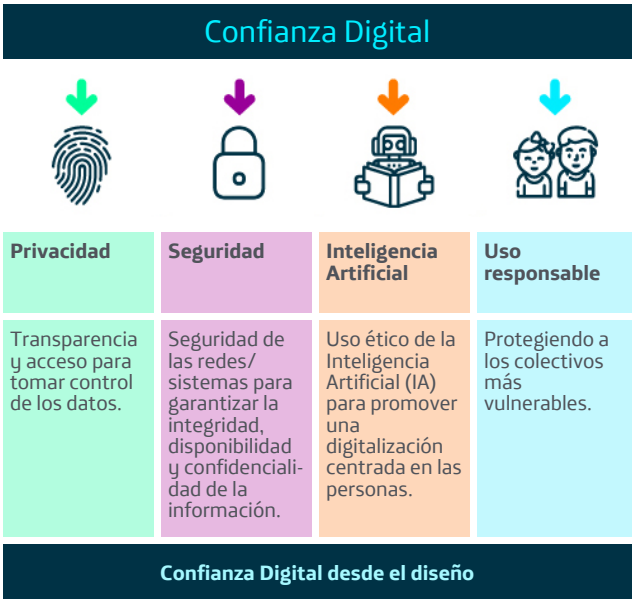
PUNTOS CLAVE

- **Protegemos los datos de nuestros clientes con unos elevados estándares de privacidad y seguridad, supervisados al más alto nivel.**
- **Somos transparentes sobre cómo, por qué y cuándo se recogen, utilizan, almacenan y eliminan los datos de nuestros clientes, así como sobre cómo los protegemos con un alto nivel de seguridad.**
- **Empoderamos a nuestros clientes para que tengan acceso y control de sus datos personales.**

2.4.1. Planteamiento GRI 103

La confianza en el uso de los servicios digitales es uno de los elementos clave en una transición digital centrada en las personas. Queremos que nuestros clientes se sientan seguros usando nuestros productos y servicios y que sean conscientes de que respetamos en todo momento sus derechos, ofreciéndoles opciones para elegir libremente el uso de su información personal. En pocas palabras, queremos que sean nuestros clientes quienes tengan el control de su experiencia digital.

Por lo tanto, hemos definido la confianza digital basándonos en cuatro ejes que conforman nuestro compromiso frente al cliente.



En cada uno de estos ejes contamos con unas políticas y procesos, que no sólo aseguran el cumplimento de una regulación creciente sino que aumentan la transparencia sobre cómo gestionamos la privacidad y seguridad de los datos.

De esta forma aseguramos que nuestros clientes estén informados en todo momento sobre:

- Cómo y para qué se recogen, almacenan y emplean sus datos.
- Que protegemos sus datos con un nivel de seguridad máximo.
- Que nos comprometemos a usar la Inteligencia Artificial de manera ética.
- Que promovemos el uso responsable de la tecnología, en especial cuando se trata de colectivos vulnerables como pueden ser menores de edad.

Nuestro enfoque de Confianza Digital desde el diseño, incorpora todos estos aspectos además al proceso de diseño, desarrollo y gestión de nuestros productos y servicios.

El órgano responsable de todos los temas relacionados con la confianza digital es el Consejo de Administración, como se refleja en la sección de gobernanza de cada uno de los temas.

2.4.2. Privacidad GRI 103

2.4.2.1. Estrategia

La estrategia de privacidad se fundamenta en tres pilares:

- **PROTECCIÓN**: Proteger los datos personales de nuestros clientes a través de políticas y procesos robustos.
- **TRANSPARENCIA**: Ser transparente sobre cómo y por qué se recogen, utilizan, almacenan y eliminan los datos personales de nuestros clientes.

- **EMPODERAMIENTO**: Empoderar a nuestros clientes a través de herramientas sencillas y seguras para que puedan controlar el uso de sus datos personales.

2.4.2.2. Gobernanza

Telefónica cuenta con un conjunto de procesos destinados a asegurar nuestro compromiso con el derecho a la privacidad de todas aquellas personas a cuyos datos tenemos acceso. Este conjunto de procesos se describe en el Reglamento de Gobierno de Protección de Datos cuyas líneas de actuación están destinadas a garantizar que se dispone de los medios y recursos suficientes para que la gestión de la privacidad se encuentre alineada con la estrategia de la Compañía.

Gobernanza de privacidad

El máximo responsable de la función de protección de datos personales del Grupo es el Delegado de Protección de Datos, quien reporta directamente al Consejo de Administración de Telefónica, S.A. a través de la Comisión de Auditoría y Control. Para asegurar el cumplimiento de esta función, se reúnen semestralmente las diferentes áreas corporativas en el Comité de Seguimiento del Modelo de Gobierno, el Comité de Negocio y los Delegados de Protección de Datos locales.

Asimismo, la Comisión de Sostenibilidad y Calidad (Comisión permanente del Consejo) se encarga de impulsar y seguir la implementación del Plan Global de Negocio Responsable de Telefónica, que incluye objetivos específicos en materia de privacidad. El Consejo es informado mensualmente sobre la implementación del Plan a través de la Dirección de Ética Corporativa y Sostenibilidad que dirige la Oficina de Negocio Responsable y que integra los máximos responsables de las áreas operativas a nivel global.

2.4.2.3. Políticas

Impulsamos y revisamos diferentes políticas y procesos, globales y locales, para fortalecer nuestro compromiso con el derecho a la privacidad de todas aquellas personas a cuyos datos tenemos acceso a través de la definición e implantación de los dominios operativos de privacidad a lo largo del ciclo de vida del dato.

Normativas de privacidad

Política Global de Privacidad

Norma Corporativa
Aprobada por el Consejo de Administración de Telefónica S.A.

Telefónica S.A.
3ª Edición - septiembre 2018

Actualizada en el 2018, establece unas normas de comportamiento común obligatorias para todas las entidades de la Compañía, sentando las bases de una cultura de privacidad basada en los principios de licitud, transparencia, compromiso con los derechos de los interesados, seguridad y limitación del plazo de conservación.

Reglamento del Modelo de Gobierno de la Protección de Datos Personales

Norma Corporativa
Aprobada por la Dirección de la Oficina DPO de Telefónica S.A.

Telefónica S.A.
1ª Edición - septiembre 2018

Aprobado en el 2018, establece el marco estratégico, organizativo y operativo y de gestión aplicable a las diferentes actuaciones en materia de protección de datos.

Reglamento ante Peticiones por parte de Autoridades Competentes

Norma corporativa
Aprobada por la Dirección de Ética y Sostenibilidad

Telefónica S.A.
2ª Edición - septiembre 2019

Actualizada en el 2019, establece los principios y directrices mínimas que deben ser contemplados en los procedimientos internos propios de cada una de las Compañías del Grupo/Unidades de Negocio/OB para cumplir con su deber de colaboración con las autoridades competentes en lo referente a los datos de nuestros clientes.

2.4.2.4. Líneas de actuación GRI 103

Nuestras líneas de actuación en materia de privacidad se configuran en torno a las siguientes materias:

- Privacidad por Diseño
- Privacidad digital
- Iniciativas de transparencia
- Empoderamiento del cliente
- Mecanismos de consulta y reclamación

Privacidad por Diseño

El principio de Privacidad por Diseño (PbD) se constituye sin duda como uno de los pilares esenciales y estratégicos del Grupo Telefónica y así viene estipulado en nuestra normativa interna de obligado cumplimiento.

El concepto de Privacidad por Diseño implica, entre otros aspectos relevantes, el deber de toda la organización de establecer un modelo de gobernanza de la gestión de datos, en el sentido de que se tengan en cuenta no solo la aplicación de medidas de protección de la privacidad desde el punto de vista legal y de seguridad en las etapas tempranas de cualquier proyecto sino también que se contemplen todos los procesos y prácticas de negocio involucrados en cada actividad o tratamiento que pueda afectar a datos de carácter personal.

Contamos con nuestras propias guías de privacidad desde el diseño con el objetivo de definir de forma ordenada el conjunto de reglas, estándares, así como de procesos legales y de seguridad que se deben tener en cuenta para dar cumplimiento a las obligaciones de privacidad por diseño, de conformidad con lo previsto tanto en el marco legal como en nuestra Política Global de Privacidad, todo ello con el fin de que los derechos y libertades de las personas titulares de los datos personales queden garantizados desde el mismo

momento de la definición de cualquier proyecto o actividad de tratamiento.

Dichas guías prácticas son los documentos de referencia para aquellos profesionales del Grupo Telefónica que tienen entre sus funciones la ideación, definición, desarrollo, normalización y evolución de productos y servicios, así como de casos de uso internos que impliquen, directa o indirectamente, el tratamiento de datos de carácter personal y, en consecuencia, que puedan ser susceptibles de afectar al derecho a la privacidad de las personas, ya se trate de clientes, usuarios, empleados, etc.

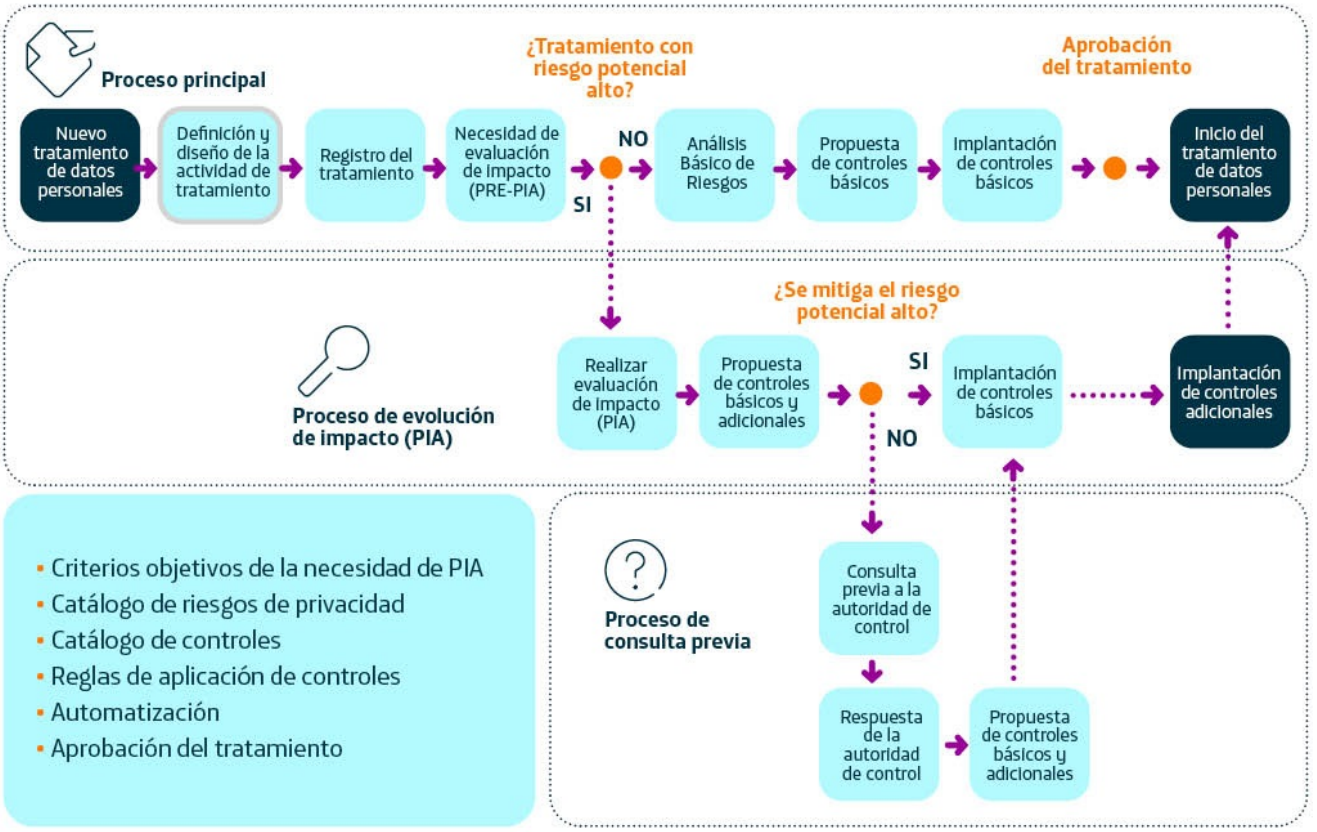
Adicionalmente, los responsables de producto cuentan siempre con el apoyo de los especialistas de privacidad y seguridad del área de cada compañía y/o unidad de negocio del Grupo, con el fin de asegurar que se tienen en cuenta todos los requisitos legales y de seguridad necesarios en materia de privacidad desde el mismo momento del diseño de su concreto producto, servicio o casos de uso internos de Telefónica de que se trate.

Utilizamos un enfoque orientado a la gestión del riesgo y de la responsabilidad proactiva (esto es, autoanálisis crítico y continuo de cada compañía en el cumplimiento de las obligaciones que exige la normativa de protección de datos) para establecer estrategias que incorporen la privacidad a lo largo de todo el ciclo de vida del dato en las operaciones de tratamiento de cada producto o servicio: Recogida y obtención, Tratamiento, Ejercicio de derechos y Conservación y supresión.

La aplicación práctica de la privacidad desde el diseño a lo largo de todo el proceso supone tener en mente, siempre en la definición o evolución de cualquier producto o servicio del Grupo Telefónica, aspectos como (i) la licitud y definición de la base legitimadora del tratamiento, (ii) la garantía de que los datos están seguros y se cumplen las medidas de seguridad más adecuadas en función de los potenciales riesgos, (iii) la transparencia del mismo en relación con el interesado en las cláusulas y políticas de privacidad, (iv) la minimización de datos en el sentido de que éstos deben ser los estrictamente necesarios para los fines del tratamiento, (v) el compromiso con los derechos de los interesados y (vi) la limitación del plazo de conservación, entre otros.

El proceso de PbD que fue definido por la Oficina Global de Protección de Datos del Grupo Telefónica incluye, al menos, las actividades siguientes:

Proceso de Privacidad por Diseño



Marco de Privacidad Digital

En Telefónica se digitaliza el proceso del PbD a través del Marco de Privacidad Digital (*Digital Privacy Framework)* implementado en los sistemas y plataformas donde tienen lugar los tratamientos de datos, como por ejemplo 4º plataforma.

El *Digital Privacy Framework*, define el marco de estrategia global legal y de privacidad con respecto a GDPR y ePrivacy en productos y sistemas de plataformas de procesamiento de datos.

Mediante el *Digital Privacy Framework* se adaptan las pautas de privacidad a una realidad tecnológica al estandarizar y conceptualizar los requisitos funcionales y técnicos de la dinámica de los sistemas de privacidad, y aplicarlos de forma automática y digital en los tratamientos.

Esta digitalización se implementa desde el diseño y por defecto y nos habilita de forma natural el ecosistema de transparencia, haciendo posible construir un proceso de privacidad dinámica y automática entre el cliente y los sistemas que llevan a cabo los tratamientos, en cumplimiento con el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés).

Durante el año 2021 se avanzará de forma significativa en la digitalización de los tratamientos en el ámbito ePrivacy y se dispondrá de la herramienta de anonimización de datos personales para añadir otra capa de robustez al *Digital Privacy Framework.*

Iniciativas de transparencia

Uno de los retos y elementos clave en la privacidad es garantizar la transparencia, siendo nuestro objetivo hacer la privacidad más humana y entendible, aplicando los principios de diseño centrado en las personas o *human-centered design.* En este sentido, en Telefónica hemos apostado por llevar la transparencia a la práctica incluyéndola como uno de los principios de la Política Global de Privacidad y desarrollando diferentes iniciativas que implementan este principio:

a. Centro de Privacidad Global

Punto de referencia público sobre nuestra política y procesos en materia de privacidad y seguridad globales. Ahí, nuestros grupos de interés pueden encontrar toda la información relevante de forma fácil y comprensible mediante recursos visuales y gráficos.

b. Centros de Privacidad y Seguridad de las operadoras

Durante el 2020 se han actualizado y creado nuevos centros locales de privacidad y seguridad ubicados en las webs comerciales de las operadoras del Grupo Telefónica. Para llevar a cabo este proyecto, primero realizamos un estudio para conocer la percepción de nuestros clientes sobre el uso de sus datos. Este estudio fue el resultado de las encuestas realizadas a nuestros clientes, con más de 600 entrevistas en cada uno de los ocho países objeto de este Informe. El objetivo es que tanto nuestros clientes como cualquier grupo de interés, puedan obtener información, de una manera sencilla, digital y entendible, sobre el tratamiento de datos personales realizado por las operadoras y otra información relevante en materia de privacidad como son los canales y vías para el ejercicio de sus derechos, las medidas de seguridad y confidencialidad que son adoptadas para tratar sus datos o cuáles son los procesos de privacidad y seguridad que adoptamos desde el diseño. Estos centros también incluyen otra información relevante como, por ejemplo, conocer los términos y condiciones de privacidad aplicables en nuestros productos y servicios, los informes de transparencia, nuestros principios de Inteligencia Artificial, así como las cuestiones relativas a seguridad y la protección del menor que se aplican en cada caso en entornos digitales. Actualmente, los centros se encuentran disponibles o en proceso de lanzamiento en el 100% de las operadoras.

c. Informe de Transparencia de las Telecomunicaciones

Anualmente publicamos el informe sobre las peticiones que recibimos de las autoridades competentes en los países donde operamos, sobre interceptación legal, metadatos asociados a las comunicaciones, bloqueo y restricción de contenidos y suspensión geográfica y temporal del servicio.

Para cualquier requerimiento, seguimos un procedimiento estricto, recogido en el Reglamento, ante peticiones de autoridades competentes que garantiza al mismo tiempo el cumplimiento de nuestras obligaciones en materia de colaboración con dichas autoridades y la protección de los derechos fundamentales de los afectados, de acuerdo a lo recogido en nuestra sección de respeto a los derechos humanos.

En el 2020 se han registrado un total de 4.193.120 de solicitudes de información de clientes por parte de las autoridades competentes (Interceptación legal y acceso a metadatos). De estas solicitudes se han rechazado 36.598, lo que supone un 99% de solicitudes atendidas. El número de accesos/clientes afectados es de 6.025.744

Empoderamiento del cliente

Como parte del principio de transparencia, Telefónica pone a disposición de los clientes el acceso a los datos que generan durante el uso de nuestros productos y servicios, datos que son recogidos en el denominado 'Espacio de Datos Personales' de la 4ª plataforma y que resultan accesibles a través de diferentes canales como p. ej. el Centro de Transparencia en la *app* Mi Movistar.

Este año 2020 se ha lanzado el Centro de Transparencia en España, que ofrece el acceso a sus preferencias de privacidad para todos los clientes y la gestión de los datos recogidos en el Espacio de Datos Personales, que actualmente está disponible para un grupo de usuarios a través de la aplicación Mi Movistar (en el apartado Seguridad y Privacidad del Perfil de Usuario).

En el Centro de Transparencia, a través de la sección Permisos de Privacidad, los clientes pueden gestionar las bases legitimadoras relativas al uso de sus datos para determinados propósitos. Y desde la sección de Acceso y Descarga se ofrecen útiles visualizaciones de diferentes tipos de datos, con una experiencia amigable y respetando los

criterios de privacidad, con la opción de descargar un documento con mayor nivel de detalle de esos conjuntos de datos.

Nuestra intención es que el Centro de Transparencia esté disponible en todos los canales en el año 2021. Nuestros clientes podrán acceder a él desde el canal *online* movistar.es donde se ofrecerán ambas funcionalidades y también será accesible desde la televisión para los mismos grupos de clientes que disponen actualmente de estas funcionalidades.

La experiencia del Centro de Transparencia se ha diseñado centrada en el usuario, evitando emplear un lenguaje legal complejo, y explicando el propósito para el cual se tratan sus datos y la naturaleza de esos datos dentro de Telefónica, ofreciendo claridad, transparencia y reforzando la confianza.

Con el Centro de Transparencia se dan los primeros pasos para cumplir nuestra promesa de empoderar a nuestros clientes con funciones de control y transparencia sobre sus datos, siempre de acuerdo con la normativa aplicable desde el punto de vista de la privacidad. Por ejemplo, en Europa este tratamiento estará plenamente alineado con el Reglamento Europeo de Protección de Datos.

Mecanismos de consulta y reclamación
Además de los mecanismos establecidos en las políticas de privacidad y los centros de privacidad, Telefónica ha implementado otros medios de consulta y mediación para atender cualquier incidencia en materia de privacidad:

a. Canal de Negocio Responsable: Contamos con un canal público en nuestra web donde todos nuestros grupos de interés pueden consultar o reclamar sobre cualquier aspecto relacionado con los Principios de Negocio Responsable. Durante 2020 se han tramitado, respondido o remediado, en su caso, 15 comunicaciones asociadas a privacidad y 0 a libertad de expresión.

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

2.4.3. Seguridad

2.4.3.1. Estrategia
El aumento en la cantidad y complejidad de las amenazas en materia de seguridad, así como su diversificación, conducen a aplicar y gestionar medidas de manera constante. Por esta razón, consideramos que la seguridad debe ser considerada como un proceso de mejora continua, y entendida como un concepto integral que englobe la seguridad física y operativa, la seguridad de la información incluyendo la ciberseguridad, la continuidad del negocio, y la prevención del fraude.

La estrategia de seguridad se apoya en una serie de procesos y actividades que refuerzan tanto los procesos operativos de negocio como las iniciativas de transformación de la Compañía. Este grupo de procesos se engloba en un sistema de gestión de la seguridad, alineada con marcos de referencia y estándares internacionales como ISO 27001 y NIST.

2.4.3.2. Gobernanza
Para lograr una protección eficaz de los activos del grupo Telefónica, incluyendo servicios y datos, y garantizar que se cuenta con los recursos y apoyo necesarios, es fundamental que el área de Seguridad tenga el respaldo de la Dirección de la Compañía y reporte al más alto nivel. El área de Seguridad se indexa en una sólida estructura organizativa que comienza en el Consejo de Administración a través de sus Comisiones de Sostenibilidad y Calidad y de Auditoría y Control, hasta las estructuras de seguridad en las operaciones locales.

Gobernanza de seguridad

El máximo responsable del área global de Seguridad Global e Inteligencia en Telefónica es el Director Global de Seguridad e Inteligencia y tiene delegada por el Consejo de Administración de la Compañía la autoridad y la responsabilidad de establecer la estrategia global de seguridad e Inteligencia, así como de liderar el marco normativo de seguridad e Inteligencia y guiar y gobernar las iniciativas globales de seguridad e Inteligencia.

El Director Global de Seguridad e Inteligencia reporta al Consejo de Administración de la Compañía a través de la Comisión de Auditoría y de la Comisión de Sostenibilidad y Calidad.

En cada empresa del grupo Telefónica existe un responsable local de seguridad, propuesto por el director global de Seguridad e Inteligencia.

Desde el punto de vista del Gobierno y Coordinación, se establece el Comité Global de Seguridad presidido por el director global de Seguridad e Inteligencia, y en el que participan los responsables corporativos de diferentes áreas de la Compañía (Cumplimiento, Auditoría, Legal, Tecnología y Operaciones, Personas, Sostenibilidad, etc.), además de los responsables locales de Seguridad. También existen subcomités de Seguridad locales presididos por los responsables locales de Seguridad, que colaboran en la definición de las iniciativas estratégicas y directrices globales y las implantan en cada empresa del grupo Telefónica.

Además, el área global de Seguridad e Inteligencia promueve e impulsa el Comité Global de Seguridad Digital en el que participan varios miembros del Comité Ejecutivo de la Compañía.

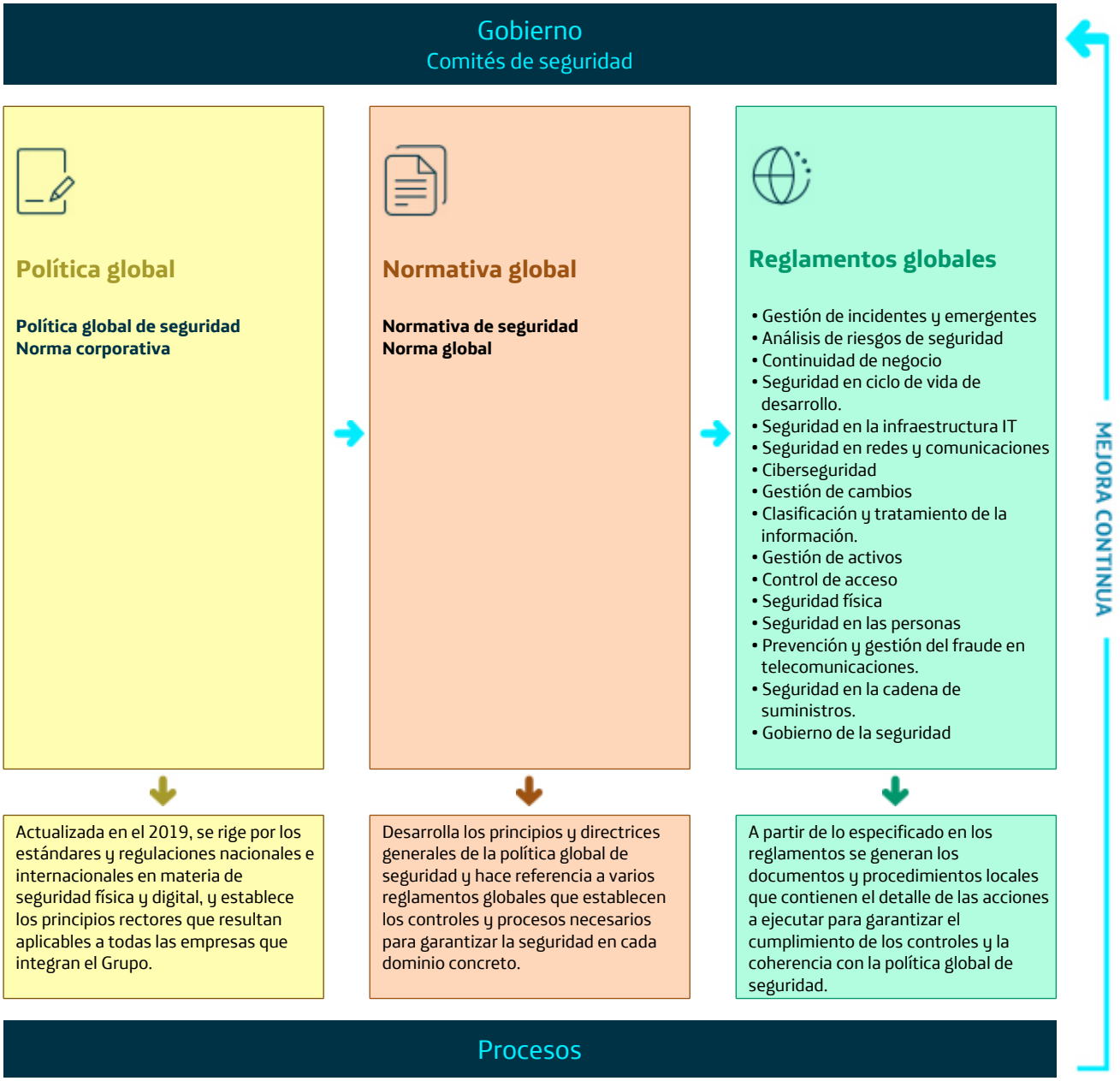
Adicionalmente, Telefónica cuenta con un Consejo Asesor de Seguridad integrado por figuras relevantes externas a la Compañía en el ámbito amplio de la seguridad e Inteligencia, con el objetivo de asesorar con las mejores prácticas de la industria y aportar su opinión a los ejes estratégicos de la Compañía en materia de seguridad e Inteligencia.

2.4.3.3. Políticas y procesos

El ciclo de vida de seguridad tiene como objetivo la protección corporativa frente a potenciales daños, protegiendo personas y bienes, y garantizando la

confidencialidad, integridad y disponibilidad de los activos de información de la Compañía, incluyendo servicios y datos. Para alcanzar estos objetivos impulsamos y actualizamos diferentes políticas y procesos en materia de seguridad para adecuarlas a los cambios de contexto y a los nuevos riesgos identificados. Este grupo de procesos se engloba en un sistema de gestión de seguridad compatible con marcos de referencia y estándares internacionales, en el que se integra un ciclo de mejora continua. Asimismo, y siguiendo el proceso de mejora continua, las políticas y procesos se adaptan en función del seguimiento y medición que se hace sobre las actividades y procesos del ciclo de vida de seguridad.

Normativas de seguridad



Nuestro marco de controles de seguridad se formaliza en certificaciones oficiales, como por ejemplo ISO27000 o PCI-DSS, en aquellos casos en los que es eficiente o necesario para procesos de relación con clientes y cumplimiento normativo, y podemos requerir a nuestros proveedores de servicios TI que tengan sistemas de gestión de seguridad certificados o informes ISAE 3402 o similares.

2.4.3.4. Líneas de actuación

La seguridad es uno de los pilares sobre los que se construye la organización global del Grupo Telefónica. Se entiende como un concepto integral que tiene por finalidad preservar sus activos y proteger sus intereses y objetivos estratégicos, garantizando, por una parte, su integridad y sustrayéndolos, por otra, a potenciales amenazas que pudieran dañar su valor, afectar a su confidencialidad, mermar su eficacia o afectar a su operatividad y disponibilidad.

La seguridad integral engloba, por lo demás, no solo la seguridad física y operativa (de personas y bienes) sino también la seguridad de la información, la ciberseguridad, la seguridad de las tecnologías de la información, la seguridad de la red, la continuidad de negocio, la prevención del fraude, así como cualquier otro ámbito o función relevante cuyo objetivo sea la protección corporativa frente a potenciales daños, sean cuales fueren, o eventuales pérdidas.

Las actividades de seguridad desarrolladas por las diferentes estructuras organizativas, responsables de activos y empleados se rigen por los principios de legalidad, eficiencia, corresponsabilidad, cooperación y coordinación, para cuyo impulso, conducción, control y mejora se establecerán los mecanismos adecuados.

El Plan Estratégico Global de Seguridad de la Compañía, revisado y aprobado por el Comité global de Seguridad el 26 de noviembre de 2020, persigue la integración de la política de seguridad en el marco más amplio de la estrategia de Telefónica, e identifica y prioriza las principales líneas de actuación y de los recursos asociados; por ejemplo, la Seguridad por Diseño (SbD) y la seguridad en la cadena de suministro. A lo largo del 2020 se han revisado y reforzado las medidas de seguridad relacionadas con el acceso remoto y el teletrabajo, debido a la situación provocada por la evolución del COVID-19.

Las principales líneas de acción de Telefónica en esta materia son las siguientes:

- Seguridad digital o ciberseguridad
- Seguridad física u operativa
- Seguridad por Diseño
- Seguridad en la cadena de suministro

Seguridad digital o ciberseguridad

La seguridad digital es un elemento clave de nuestro negocio. Su objetivo último es garantizar nuestra resiliencia, esto es, la capacidad para resistir y contener ataques, de forma que nuestra actividad no se vea afectada o lo sea en un nivel tolerable. Esto se materializa en la práctica en procesos, herramientas y capacidades que persiguen anticipar y prevenir los riesgos de ciberseguridad.

Dado el contexto actual de ciberseguridad y la naturaleza de Telefónica como operador digital, se hace especial foco en los siguientes procesos:

a.Ciberinteligencia y gestión de incidentes

Contamos con herramientas y capacidades en torno a todo el ciclo de potenciales incidencias:

- **Anticipación**, antes de que pueda afectarnos.
- **Prevención**, garantizando la protección tanto de las instalaciones y activos como de los datos e identidad de cliente.
- **Detección**, a través de doce Centros Operativos de Seguridad.
- **Respuesta**, mediante una red de quince Centros de Respuesta a Incidentes (CSIRT) que trabajan coordinadamente, a nivel local y global, para restaurar la normalidad en el menor tiempo y con el menor impacto posible.

Nuestro enfoque en ciberintenligencia se basa en la proactividad, en aplicar el conocimiento y la tecnología para alcanzar los niveles de protección requeridos detectando rápidamente las infracciones o ataques en los activos y construyendo las capacidades técnicas y humanas necesarias para responder con eficacia y celeridad ante cualquier brecha o incidente, con el fin de minimizar los ataques y las consecuencias de esto.

Disponemos de un programa de recompensas por descubrimiento de vulnerabilidades (*bug-bounty*) con empresas seleccionadas expertas en la industria.

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

Durante 2020 se ha gestionado 1 único incidente de seguridad con impacto alto. Consideramos que son de impacto alto aquellos incidentes que cumplen con unos criterios determinados a nivel global (por ejemplo, por su impacto económico, legal, en los servicios, o repercusión mediática). En el incidente mencionado no hubo fuga de datos de clientes y se siguieron los protocolos existentes de respuesta.

Las lecciones aprendidas a partir de los incidentes constituyen una parte fundamental de la realimentación hacia los proyectos de mejora de la seguridad, tanto en procesos como en capacidades y plataformas tecnológicas.

El ciberejercicio de la red de CSIRT es una iniciativa realizada por el CSIRT global que ofrece un entorno de evaluación, entrenamiento y formación especialmente diseñada para equipos de respuesta ante incidentes, y cuenta con la participación de equipos integrantes de la red de CSIRT de Telefónica a nivel internacional.

Contamos con un buzón público, a nivel global y a disposición de cualquier usuario, con el fin de reportar alguna vulnerabilidad o amenaza que pudiera afectar a la infraestructura tecnológica de Telefónica. Este buzón se encuentra en el Centro de Privacidad Global/Seguridad. Asimismo, se dispone de buzones equivalentes a nivel local en cada una de nuestras geografías.

Durante el período 2015-2020 y hasta la fecha, la Compañía dispone de diversos programas de seguros, de forma que se mitigue el impacto en el balance derivado de la materialización de un gran número de riesgos. En particular, existe una cobertura para ciberriesgos que ocasionen una pérdida de ingresos, pérdida de clientes, costes extra o gastos de recuperación de activos digitales, entre otros, y una cobertura de Errores y Omisiones Tecnológicos para el caso de reclamaciones por perjuicios ocasionados a clientes y terceros en general. Los límites actualmente contratados a nivel global son:

- Seguro ciberriesgos: 100.000.000 euros.
- Seguro errores y omisiones tecnológicos: 300.000.000 euros.

b. Seguridad en la red

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

El papel de Telefónica como operador de telecomunicaciones hace imprescindible la profundización en los controles para la seguridad de las propias redes e infraestructuras de comunicaciones fijas y móviles, así como de las plataformas de servicios asociadas (p.e. vídeo, IoT). En ese sentido se aplican de forma integral los procesos de seguridad citados para gestionar los riesgos asociados a ataques y explotación de vulnerabilidades en redes y protocolos, con actividad relevante a nivel interno, con los principales socios tecnológicos y con organizaciones internacionales (p.e. GSMA) para reducir potenciales impactos. Ejemplos de esto son los trabajos sobre 4G/LTE, SS7, BGP y otras tecnologías habilitadoras críticas.

Cabe además destacar la importancia de la evolución a 5G y el posicionamiento de la Compañía en contribuir activamente a que las nuevas redes sean tanto o más seguras que las precedentes. Los desarrollos tecnológicos de la Compañía en este ámbito, como por ejemplo la evolución de nuestra plataforma de virtualización de la red, UNICA NEXT, la segmentación por servicios (*network split*), o las nuevas tecnologías de acceso radio están considerando la seguridad por diseño.

Seguridad física y operativa

En el ámbito de la seguridad operativa, la Compañía invierte un esfuerzo continuado en la mejora de sus capacidades para la protección física de infraestructuras y activos. Con este fin se siguen desarrollando varios programas, entre los que podemos destacar:

- La interconexión de centros de control para convertirlos en una red resiliente que refuerce la disponibilidad de las infraestructuras que soportan los servicios de vigilancia y protección.
- La gestión de la seguridad en viajes del personal de Telefónica que permite mejorar sustancialmente el tiempo de respuesta y los mecanismos de actuación ante cualquier incidente que pueda acaecer durante un viaje de trabajo.
- La implantación de procedimientos y herramientas homogéneas y digitales para la monitorización global de la seguridad.

Seguridad por Diseño

La seguridad se contempla desde las fases más tempranas en todos los ámbitos de la actividad para garantizar que la seguridad sea parte integral de todo el ciclo de vida de la tecnología. Este enfoque, basado en el proceso de análisis y gestión de riesgos y el desarrollo de tecnologías propias y que apuesta por la innovación y la tecnología nacional, la concienciación de empleados y los requisitos de seguridad exigidos a nuestra cadena de suministro, se efectúa en los siguientes ámbitos:

- Diseño de sistemas seguros: se consideran los requisitos de seguridad desde la fase de diseño de aplicaciones y sistemas, incorporando controles frente a vulnerabilidades conocidas y garantizando que no existen debilidades de seguridad en origen. Como resultado de esto se obtienen sistemas y aplicaciones más resistentes a ataques maliciosos.
- Los órganos de gobierno reciben información consolidada de seguimiento y control para análisis. En base a ese análisis se determinan las acciones preventivas a incorporar en el plan estratégico, considerando la seguridad por defecto y desde la fase del diseño, y revisando a su vez los aspectos necesarios en la Política y marco normativo global de seguridad para tener en cuenta las consideraciones oportunas.

Seguridad en la cadena de suministro

Desde hace unos años, el establecimiento de una línea base de cumplimiento en cuanto a los requisitos de seguridad para nuestros proveedores, y la identificación de los riesgos asociados a la prestación de un servicio/producto, han sido una prioridad para el Grupo Telefónica. Es por ello que, durante el año 2020, se ha continuado apoyando y

evolucionando en la implantación de la iniciativa de seguridad en la cadena de suministro.

Este año ha sido esencial en esta transformación gracias a la creación de una herramienta —denominada 3PS+—, que permite digitalizar todo el proceso de gestión de los aspectos de seguridad a lo largo de todo el ciclo de vida de los proveedores. Esta herramienta es una aplicación que permite al usuario disponer de toda la información relacionada con los aspectos de seguridad de un proceso de compra antes de la contratación, y de sus proveedores, durante y después de la prestación. Sus principales características son las siguientes:

Proceso de seguridad en la cadena de suministro

- **Antes de la contratación**, la aplicación permite al usuario generar los requisitos de seguridad para nuevos procesos de compras con los que se puede interactuar, por ejemplo, generando y modelando los requisitos de seguridad; cargando las respuestas dadas por los proveedores; obteniendo valoraciones objetivas sobre el nivel de cumplimiento, etc.

- **Durante la prestación del servicio**, el usuario tiene la posibilidad de monitorizar los aspectos de seguridad relacionados con el servicio. Para ello el sistema genera alertas en función de la fecha de inicio del servicio y del período de monitorización seleccionado, y permite al usuario registrar información relevante que pueda suponer un riesgo para los activos de Telefónica.

- **Al finalizar la prestación del servicio**, el usuario puede controlar cómo se ejecuta la salida del proveedor, y mitigar e incluso evitar los riesgos de seguridad más comunes en la finalización de los servicios: no bloqueo de accesos físicos y lógicos, no revisión de VPNs/puertos/sistemas usados para los servicios, etc.

Todos los empleados del Grupo Telefónica a nivel global tienen acceso a esta herramienta que simplifica y facilita, no sólo la obtención de unos requisitos de seguridad, sino el conocimiento y la gestión de los riesgos que supone la prestación de un servicio/producto por parte de un proveedor.

2.4.3.5. Continuidad de negocio y gestión de crisis

Estrategia

La función de continuidad de negocio integra diversas actividades y procesos orientados a mejorar la resiliencia de la Compañía en todas sus vertientes.

Nuestra prioridad como compañía es garantizar, en este ámbito, y ante la ocurrencia de una crisis, lo siguiente:

- Proteger la integridad de las personas, procurando el bienestar de los empleados y colaboradores.

- Proporcionar los servicios acordados a nuestros clientes, con la disponibilidad y calidad acordada.

- Proteger y velar por los intereses de nuestros accionistas e inversores institucionales.

- Cumplir con nuestras obligaciones regulatorias y legales.

- Proteger y asegurar los negocios desde el punto de vista de la sostenibilidad.

La función de continuidad de negocio se recoge en la política global de seguridad. Los detalles de dicha función se definen en el Reglamento Global de Continuidad de Negocio y en diversa documentación, tanto a nivel global como local, de cada unidad de negocio.

Para garantizar su constante evolución y el apoyo por parte de la dirección de la Compañía, esta iniciativa se incluye como parte del Plan Estratégico de la Dirección Global de Seguridad e Inteligencia en forma de Plan Global de Gestión de Crisis, que se compone, a su vez, del Proyecto Global de Gestión de Crisis y del Proyecto Global de Continuidad de Negocio.

Plan global de gestión de crisis

La estrategia de la Compañía ha evolucionado en los últimos años, de un modelo distribuido a un modelo global, lo que ha significado fortalecer los siguientes aspectos:

- **Visión estratégica:** Las amenazas globales a las que se enfrenta la Compañía requieren de acciones globales. Disponer de una visión estratégica de la continuidad de negocio en la Compañía, permite tomar decisiones globales que redundan en mayor resiliencia.
- **Eficacia en la gestión de crisis:** Disponiendo de un modelo de gestión de crisis probado, común a toda la Compañía, tanto en sus definiciones como en la ejecución de sus procedimientos.
- **Coordinación y colaboración:** El modelo organizativo garantiza, alinea y promueve el desarrollo homogéneo de la continuidad de negocio en las diversas unidades de negocio.
- **Estandarización de la medición:** De tal forma que permite medir, sin sesgos, diversos indicadores que nos muestran el grado de madurez desde el punto de vista de la continuidad de negocio, y el nivel de resiliencia de la Compañía. Además nos permite marcar objetivos SMART a medio y largo plazo.

Cada unidad de negocio dispone de su propia oficina local de continuidad de negocio, siendo todas las oficinas locales alineadas y coordinadas por medio de la oficina global, ubicada funcionalmente en la Dirección Global de Seguridad e Inteligencia, que pertenece al área de corporativa de la Compañía.

La Compañía dispone de un plan de gestión de crisis compuesto por un proyecto global de gestión de crisis y un proyecto global de continuidad de negocio. Todo lo anterior se basa en estándares internacionales como la ISO 22301 de gestión de continuidad de negocio y la ISO 22320 de gestión de emergencias.

Para la ejecución del plan de gestión de crisis se identifican los procesos de cada una de las áreas, detectando escenarios que puedan provocar su interrupción; se contemplan potenciales planes de tratamiento; se deciden las estrategias de continuidad de negocio a aplicar y, si fuera necesario, se generan los planes de continuidad de negocio con las acciones oportunas a seguir.

Anualmente se realizan al menos 2 simulacros globales, uno para chequear mecanismos de continuidad de negocio y otro simulando un escenario de crisis, salvo que en ese periodo se haya tenido ocasión de comprobar la efectividad o identificar oportunidades de mejora debido a situaciones reales de continuidad o de gestión de crisis.

Modelo de gobierno

La evolución estratégica de la función de continuidad de negocio en la Compañía requiere de su propio gobierno corporativo. Para ello se dispone del Comité Global de Continuidad de Negocio, órgano encargado de tomar las decisiones estratégicas sobre aspectos relacionados con continuidad de negocio para el Grupo Telefónica. Dicho órgano permite definir una estrategia global para tener en cuenta la continuidad de negocio desde el diseño, además de garantizar que se disponga de los recursos necesarios y definir dónde es necesario centrar los esfuerzos.

De forma similar, se definen los comités locales de continuidad de negocio, órganos encargados de velar por esta función en cada unidad de negocio. Tienen la función, por un lado, de garantizar la implantación de las decisiones estratégicas tomadas en el ámbito global y, por otro lado, trasladar las necesidades, logros e indicadores de madurez que permiten una visión holística de la continuidad de negocio en el Grupo Telefónica.

Los Comités de Continuidad de Negocio, ya sean a nivel global o local, priorizan y focalizan los recursos de esta función allá donde mayor impacto y valor puedan generar a la Compañía, basándose en los siguientes ejes de atención:

- Servicios estratégicos
- Proyectos estratégicos
- Proveedores estratégicos
- Aspectos organizativos

La continuidad de negocio en el Grupo Telefónica ha evolucionado desde un modelo distribuido en las diferentes unidades de negocio que lo componen, hacia un modelo global mediante la creación de una Oficina Global de Continuidad de Negocio (OGCN) que coordina las diferentes Oficinas Locales de Continuidad de Negocio (OLCN).

La Oficina Global de Continuidad de Negocio es, además, el vehículo que traslada las distintas decisiones estratégicas definidas por el comité global de continuidad de negocio, a las unidades de negocio del Grupo Telefónica.

Con periodicidad anual, cada una de las Oficinas Locales de Continuidad de Negocio, bajo el prisma del proyecto global de Continuidad de Negocio, genera su Plan de Trabajo (*Statement Of Work*, SOW). Este SOW representa la planificación de los trabajos y tareas de Continuidad de Negocio, que se abordarán en los siguientes doce meses.

Las Oficinas Locales de Continuidad de Negocio también disponen de un análisis de impacto al negocio (BIA), que identifica los procesos o servicios más relevantes en relación con su tolerancia a la indisponibilidad y el impacto al negocio.

El listado de procesos, junto con su nivel de relevancia, se tendrá en cuenta para la decisión que cada Oficina Local tomará en cuanto al alcance objetivo.

Madurez de la continuidad de negocio en el Grupo Telefónica

El Grupo Telefónica tiene establecido un modelo de madurez de la continuidad de negocio basado en cuatro niveles y alineado con el estándar establecido por la ISO 22301. Los cuatro niveles son:

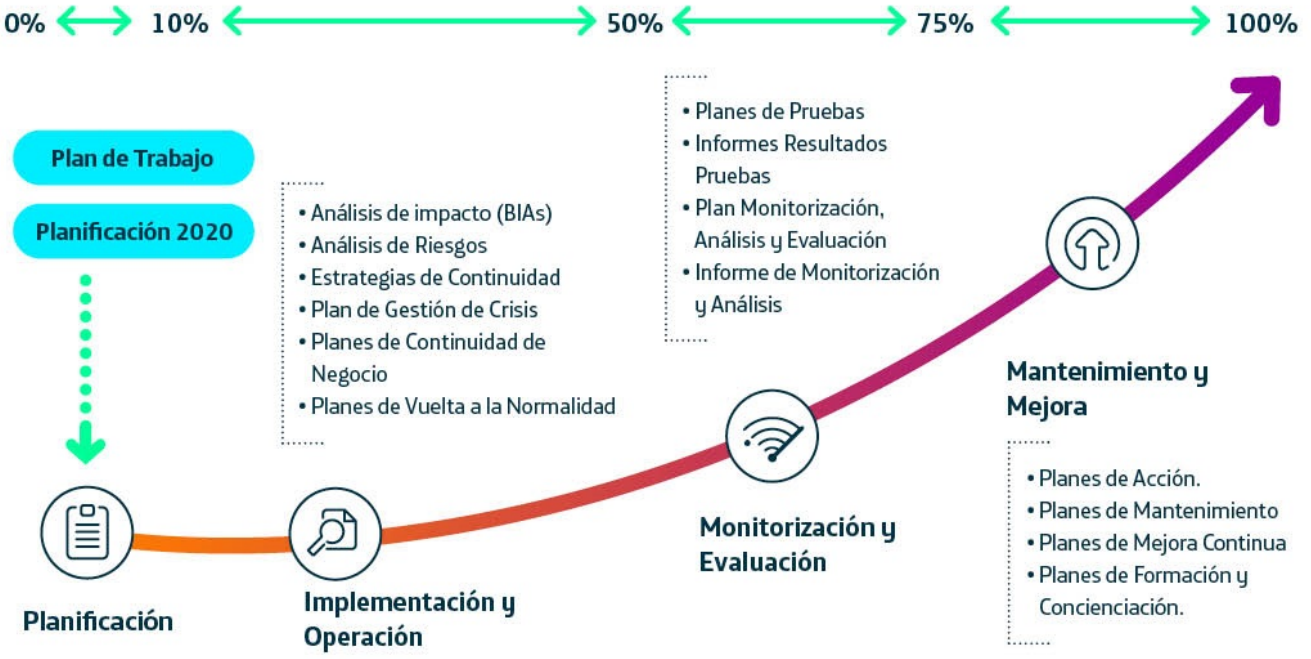
1. Planificación: engloba la elaboración de un *Statement of Work* (SoW) que detalla el alcance de la continuidad de negocio y una planificación de las actividades a acometer en el año correspondiente.

2. Implementación y operación: contiene el conjunto de entregables destinados a establecer y documentar los diferentes mecanismos de continuidad de negocio existentes: análisis de impacto (BIAs), análisis de riesgos, planes de continuidad, planes de vuelta a la normalidad, etc.

3. Monitorización y evaluación: evalúa la eficacia de los mecanismos de continuidad de negocio establecidos sometiéndolos a pruebas en escenarios realistas y acotados. Se dispone de indicadores para evaluar el desempeño, el nivel de madurez e implantación del proyecto global de continuidad de negocio.

4. Mantenimiento y mejora: aúna tanto las lecciones aprendidas y oportunidades de mejora obtenidas tras las pruebas de Continuidad de Negocio como las iniciativas de mejora que surjan en las planificaciones anuales.

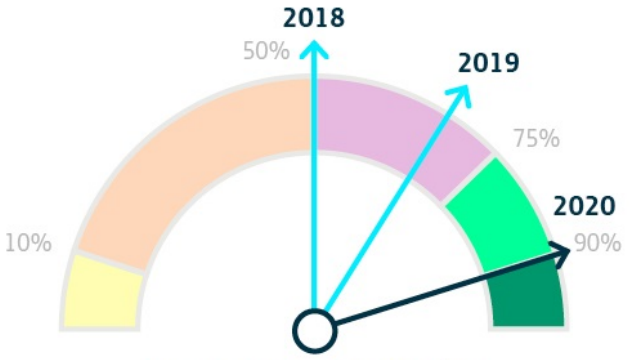
Modelo de grado de madurez de la continuidad de negocio



Este modelo de grado de madurez homogéneo, en cuanto a las capacidades de gestión del proceso de Continuidad de Negocio, permite a las distintas unidades definir los objetivos a medio y largo plazo. Además, facilita al Grupo Telefónica una visión holística y consolidada que acompaña a sus decisiones estratégicas.

Durante los últimos años, la evolución del nivel de madurez del Grupo Telefónica nos ha permitido alcanzar el nivel de optimizado, lo que implica que se han establecido, probado y obtenido lecciones aprendidas sobre los mecanismos de continuidad de negocio definidos:

Evolución del grado de madurez



Nivel de madurez Grupo Telefónica

Gestión de crisis

El Proyecto global de gestión de crisis en el Grupo Telefónica se estructura en base a cuatro capas diferenciadas.

1. La primera capa define y clasifica, de manera unívoca y homogénea, las crisis, su tipología y la estrategia general de cómo afrontarlas en la Compañía.

2. La segunda capa define, de manera unívoca y homogénea, los roles, responsabilidades, medios y canales que intervienen en la gestión de las crisis así como la relación y responsabilidades entre los comités de crisis.

3. La tercera capa agrupa los procedimientos, planes y documentación necesarias para la gestión de las crisis.

4. La cuarta capa define, con carácter global, la arquitectura de sistemas de alerta, de comunicación segura y, en general, los aspectos relacionados con la digitalización que da soporte a las actividades de los distintos comités de crisis.

Capas de la Gestión de Crisis

	Crisis • Definición • Clasificación (Local, Regional, Global) • Estrategia general
	Comité de crisis • Presidente • Miembros y mesas • Medios y cnales
	Procedimientos • Procedimientos de actuación ante crisis • Simulacros/Planes de continuidad de negocio • Planes de comunicación
	Arquitectura • Sistema de alerta • Sistema de comunicación segura • Sistema de soporte al comité de crisis

El proyecto global de gestión de crisis proporciona mecanismos adicionales y complementarios a la continuidad de negocio, que permiten gestionar incidentes con amplio impacto en el grupo Telefónica.

Como parte del modelado se describen tres tipos de crisis:

- **Crisis local:** circunscrita a una organización o unidad de negocio del Grupo Telefónica en un país.

- **Crisis regional:** circunscrita a varios países que pertenecen a una misma región geográfica.

- **Crisis global:** circunscrita a varias empresas o unidades de negocio del Grupo Telefónica en más de un país.

Dependiendo el tipo que crisis que se desencadene, existen unos protocolos y medios activos, tanto de alerta como de notificación, gestión y coordinación, que son conocidos por todos los involucrados en el proyecto global de gestión de crisis.

El rol principal en la gestión de crisis lo representan los miembros del Comité de Crisis, ya sea en el global o en los locales. Existe una diferenciación entre miembros fijos que participan en cualquier activación, miembros *ad hoc* que participan dependiendo de la tipología de la crisis, y mesas de trabajo o de apoyo a dichos miembros.

El Proyecto Global de Gestión de Crisis permite al Grupo Telefónica:

- Acelerar el proceso de toma de decisiones.

- Permitir un modelo de gestión unificada de la crisis.

- Centralizar la recepción de información.

- Actuar como figura táctica y de toma de decisiones unificada.

- Decidir cómo actuar en base al escenario de crisis que se afronte, y apoyándose en los aspectos de continuidad de negocio trabajados con anterioridad, evitar tomar decisiones 'en caliente'.
- Trasladar, de forma fiable, la información sobre lo acontecido a los clientes, estamentos, organismos o cualquier otro *stakeholder.*

Por último, se define la obligatoriedad de la realización de pruebas y simulacros sobre distintos escenarios potencialmente dañinos para la Compañía. La realización de estos simulacros permite identificar los siguientes aspectos y mejorar los mismos:

- Evaluar reacciones a circunstancias particulares.
- Evaluar la preparación de la documentación que soporte la actividad de gestión de crisis.
- Evaluar los mecanismos de coordinación.
- Preparar a los miembros de los comités de crisis para actuar

COVID

Durante la situación excepcional generada por el COVID-19, las oficinas de Continuidad de Negocio han continuado con su labor de identificar los procesos más relevantes, tanto para garantizar que son lo suficientemente robustos como para garantizar la resiliencia de la Compañía.

Como consecuencia de la pandemia, han sido activados de forma satisfactoria tanto el proceso de gestión de crisis como los medios disponibles, logrando mantener en todo momento los niveles de servicio acordados con los clientes y adaptando la capacidad de la red a los cambios en la demanda. Este escenario ha permitido la aplicación práctica del proyecto global de gestión de crisis en todas las Unidades de Negocio del Grupo Telefónica, fortaleciendo el modelo de gestión común, la homogeneización de la arquitectura que soporta esta función, la digitalización de los procesos de alerta de crisis y la formación y concienciación del personal crítico.

La pandemia del COVID-19, sufrida en toda la huella del Grupo Telefónica, nos ha llevado a un trabajo incesante de coordinación, gestión y toma de decisiones. Todas las áreas relacionadas con la continuidad de negocio y la gestión de crisis en el Grupo Telefónica han demostrado su preparación para afrontar una situación tan excepcional como la vivida.

Más del 90% de los empleados actuando en modalidad de teletrabajo sin incidencias reseñables, más de 80 comités de crisis y simulacros a nivel regional y global, centenares de reuniones incluyendo comités de crisis y simulacros a nivel local —con frecuencia adaptada a la situación—, un altísimo nivel de coordinación entre las distintas áreas y unidades de negocio, entre otros, sitúan al Grupo Telefónica en un grado de madurez muy alto en relación a la capacidad de reacción ante eventos críticos.

Por otro lado, el Grupo Telefónica ha sido una pieza fundamental para toda la sociedad desde el punto de vista del aseguramiento de las comunicaciones. Este hecho ha sido reconocido y valorado por diversos entes y estamentos en todos los países donde el Grupo Telefónica tiene presencia.

A continuación detallamos los cuatro eventos tratados en el comité de crisis, adicionales a la pandemia (global):

Eventos tratados en el Comité de Crisis

CHILE (LOCAL) Febrero de 2020	
Crisis	Robo de Cable (Afectación a Servicios VOZ+INTERNET)
Tipo de crisis	Robo de cable
Impacto	Se genera una creciente ola de robos de cables impactando la red de cobre y dejando a 573 puntos de cable afectados a nivel nacional, con más de 45 mil clientes sin sus servicios (Voz+Internet). La principal afectación fue en la región metropolitana, sin embargo, los daños se focalizan en 5 regiones del centro Sur de Chile: Metropolita RM, Valparaíso V, O'Higgins VI, La Araucanía VIII y Los Lagos X. Hubo impacto económico, reputacional y regulatorio. No hubo ningún tipo de afectación en las personas.
Actuaciones	Se activó comité de crisis el 14 de febrero del 2020. Este comité se compone por un equipo multidisciplinario de las áreas de Call Center, Atención Técnica de Clientes (ATC), Infraestructura de red, Calidad y experiencia cliente, segmento empresas y seguridad. Al inicio de la activación había un total de 573 puntos de cables afectados con un impacto en 45.576 clientes para sus servicios de voz (STB) e Internet (ADSL- VDSL). Se realizaron mesas de trabajo diarias donde se detectaron, analizaron y ejecutaron planes de acción para mitigar el robo de cables en las regiones antes señaladas. Tras las mejoras obtenidas con las iniciativas implementadas en diferentes etapas del proceso se solicita la finalización de la crisis de fallas masivas por robo de cable el día 31/08/2020, debido a la disminución de los clientes afectados.

PERÚ (LOCAL) Junio de 2020	
Crisis	Incendio en local Chiclayo – Departamento Lambayeque
Tipo de crisis	Incendio
Impacto	La principal prioridad fue la de recuperar los servicios domiciliarios (telefonía, internet y tv) y móviles debido al impacto de la afectación y los del estado (salud, policía, entre otros). La red fija estuvo afectada en un 47%, internet en un 50% y el servicio móvil en un 47%. El servicio empresarial tendría nivel de importancia 2 debido a que el incidente ocurrió un sábado y por decreto del gobierno peruano, los días de fin de semana cerraban los comercios por efectos de la pandemia del COVID-19. Se realizaron labores de re-enrutameinto de las comunicaciones por los nodos de Piura y Trujillo. Se comunicó de manera oportuna al ente regulador y autoridades, y así no incurrir en penalidades.
Actuaciones	Con la restauración del suministro eléctrico, los servicios se estandarizaron a las 12:30.

BRASIL (LOCAL) Septiembre de 2020	
Crisis	Indisponibilidad de servicios de Voz y Recarga por fallo eléctrico en Datacenter
Tipo de crisis	Fallo de suministro eléctrico
Impacto	Indisponibilidad de servicios de voz y recarga para el 50% de la base de clientes de prepago y control de las siguientes unidades de la federación: a. PR (Paraná – códigos de área 41 ao 46), b. RS (Rio Grande do Sul – códigos de área 51 ao 55), c. SC (Santa Catarina – códigos de área 47 y 48) y d. SP (São Paulo – códigos de área, 13 y 16).
Actuaciones	Según se fue intensificando la reacción de los manifestantes, se convocó el comité de crisis para tomar las decisiones oportunas y comunicar a todos los empleados la autorización de teletrabajo. Además, se dieron indicaciones para proteger la seguridad física de los trabajadores.

COLOMBIA (LOCAL) Noviembre de 2020	
Crisis	Huracán IOTA
Tipo de crisis	Indisponibilidad de infraestructura – desastre natural
Impacto	El 16 de Noviembre de 2020 el huracán IOTA de categoría 5, hizo paso por encima del territorio del Archipiélago, generando mayor impacto sobre la Isla de Providencia en la cual dejo devastado el 98% de la infraestructura de la misma. En la Isla de San Andrés también presentaron fuertes impactos a la infraestructura, aunque de menor nivel. En las islas se tenían 28 estaciones de red móvil, 6.123 clientes de Voz fija y 1.327 clientes de Banda Ancha. Tras el huracán el impacto en la Isla de San Andrés fue del 65% del servicio móvil, 5% de Voz, 18% BA. La isla de Providencia quedo 100% afectada e incomunicada.
Actuaciones	Desde el 14 de noviembre, alertados por los pronósticos del huracán, se activó el plan de contingencia del servicio de redes con el fin de desplegar medidas preparatorias para responder en el menor tiempo posible a los impactos que se pudieran presentar. De tal manera, con apoyo de diferentes entidades se logró hacer llegar personal y recursos para dar inicio de las recuperaciones. Para San Andrés, al tercer día, se logró la recuperación de la mayoría de los servicios de la isla, aunque debido al daño de un gran porcentaje de la radiobase 2G se comenzó a trabajar en un plan de modernización de los servicios móviles de la isla con la implementación, a 31 de diciembre, de 10 nuevas radiobases LTE. Para el caso de Providencia, Telefónica fue el primer operador en lograr restablecer las comunicaciones el domingo 22 de noviembre a las 7:00 PM. Posteriormente continuamos con la recuperación de la cobertura en la isla con otros cuatro sitios donde se desplegaron soluciones temporales 3G.

2.4.3.6. Servicios de seguridad

A finales de 2019 se creó la nueva división Telefónica Tech, que engloba los negocios tecnológicos de Ciberseguridad, Cloud e IOT/Big Data. De esta manera, en Telefónica Tech aglutinamos los negocios con alto potencial de crecimiento, aprovechando el conocimiento interno de tecnologías, redes, sistemas y procesos digitales, lo que permite generar oportunidades de negocio y redondear nuestra oferta de servicios digitales a nuestros clientes.

ElevenPaths es la unidad de Ciberseguridad de Telefónica. Nos encargamos de hacer la seguridad más humana y generar en las personas la confianza y tranquilidad que necesitan.

En 2020, ElevenPaths alcanzó los 448 mill de euros de facturación.0

En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente cubrimos todas las fases de una amenaza: preparación, prevención, detección, respuesta y recuperación para disminuir los ataques, proteger los activos y servicios digitales y así garantizar la ciberresilencia de nuestros clientes y su negocio. Nos adelantamos a los ataques más sofisticados y frecuentes.

Por eso, necesitamos ser cada vez más receptivos a las medidas de ciberseguridad y redefinir nuestra estrategia hacia la ciberresiliencia. Con este objetivo dedicamos toda nuestra experiencia y esfuerzo a la creación de productos innovadores en ciberseguridad con el fin de estar siempre por

delante de los atacantes que se han convertido en una amenaza creciente en nuestra vida digital.

Desde la creación de ElevenPaths hemos combinado el desarrollo de tecnologías innovadoras, patentadas con las tecnologías de los principales actores del mercado *(partners)*, para proporcionar soluciones únicas que permiten estar preparado y responder ante cualquier tipo de ataque.

Los servicios de ciberseguridad globales están diseñados para mejorar continuamente la eficacia de la infraestructura de seguridad. Por ello:

- Trabajamos para desarrollar nuevos servicios y capacidades de seguridad que ayuden a proteger los negocios y a las personas de las amenazas y vulnerabilidades, presentes en los entornos en los que operan.
- Colaboramos e intercambiamos información sobre amenazas en tiempo real con los principales organismos y entidades como la Comisión Europea, *Cyber Threat Alliance* (CTA), ECSO, EURPOL e INCIBE.
- Gestionamos más de cinco millones de *Endpoints* y monitorizamos más de 16.500 dispositivos con un SOC global integrado que opera desde 11 localizaciones distribuidas por Europa y América. Gracias a nuestras plataformas inteligentes y automatizadas, podemos actuar de forma eficiente. Los SOCs de Telefónica se han visto reforzados con la firma de la mayor alianza mundial de seguridad de telecomunicaciones junto a Etisalat, Singtel y Softbank, que nos permite posicionarnos con una completa cartera de servicios. Tenemos personas expertas dispuestas a ayudar a nuestros clientes ante los nuevos retos digitales en un mundo de incertidumbre.
- Contamos con seis centros de Innovación y Desarrollo repartidos por España, Buenos Aires y Miami, desde donde nace la tecnología desarrollada internamente por ElevenPaths.
- Creamos Telefónica Tech Ventures en 2020, el vehículo de inversión en *startups* y empresas con foco en ciberseguridad, impulsado por ElevenPaths y Telefónica Innovation Ventures. Su objetivo es detectar la innovación disruptiva en ciberseguridad, especialmente en los ámbitos de *Threat Intelligence*, seguridad cloud, protección de datos e Inteligencia Artificial aplicada a la ciberseguridad.
- Hemos invertido, también en 2020, en compañías internacionales consolidadas como Nozomi Networks y también en *startups* españolas como Alias Robotics.

Gracias a estas colaboraciones, alianzas y a nuestra propia experiencia, ElevenPaths está presente en toda la cadena de valor de la seguridad y cuenta con un *portfolio* de soluciones de seguridad integral para el mundo de Internet de las Cosas (IoT), soluciones de *cloud security*, identidad y privacidad, antifraude, ciberseguridad industrial, movilidad segura, exposición digital, gestión del riesgo y cumplimiento normativo. Todo este esfuerzo nos ha valido el reconocimiento de los mejores analistas de la industria en este campo.

2.4.4. Inteligencia Artificial

La Inteligencia Artificial (IA) y el *Big Data* están en auge. Pueden aplicarse a ámbitos tan diversos como las recomendaciones de contenido, los chatbots, el reconocimiento de imágenes, la traducción automática, la detección de fraudes, los diagnósticos médicos, los vehículos autónomos, el ámbito jurídico, la educación, el transporte y la logística, por nombrar solo algunos. No solo se utilizan en los negocios, sino también para fines sociales como un mejor entendimiento y reducción de los efectos del cambio climático, los desastres naturales, las pandemias y la migración.

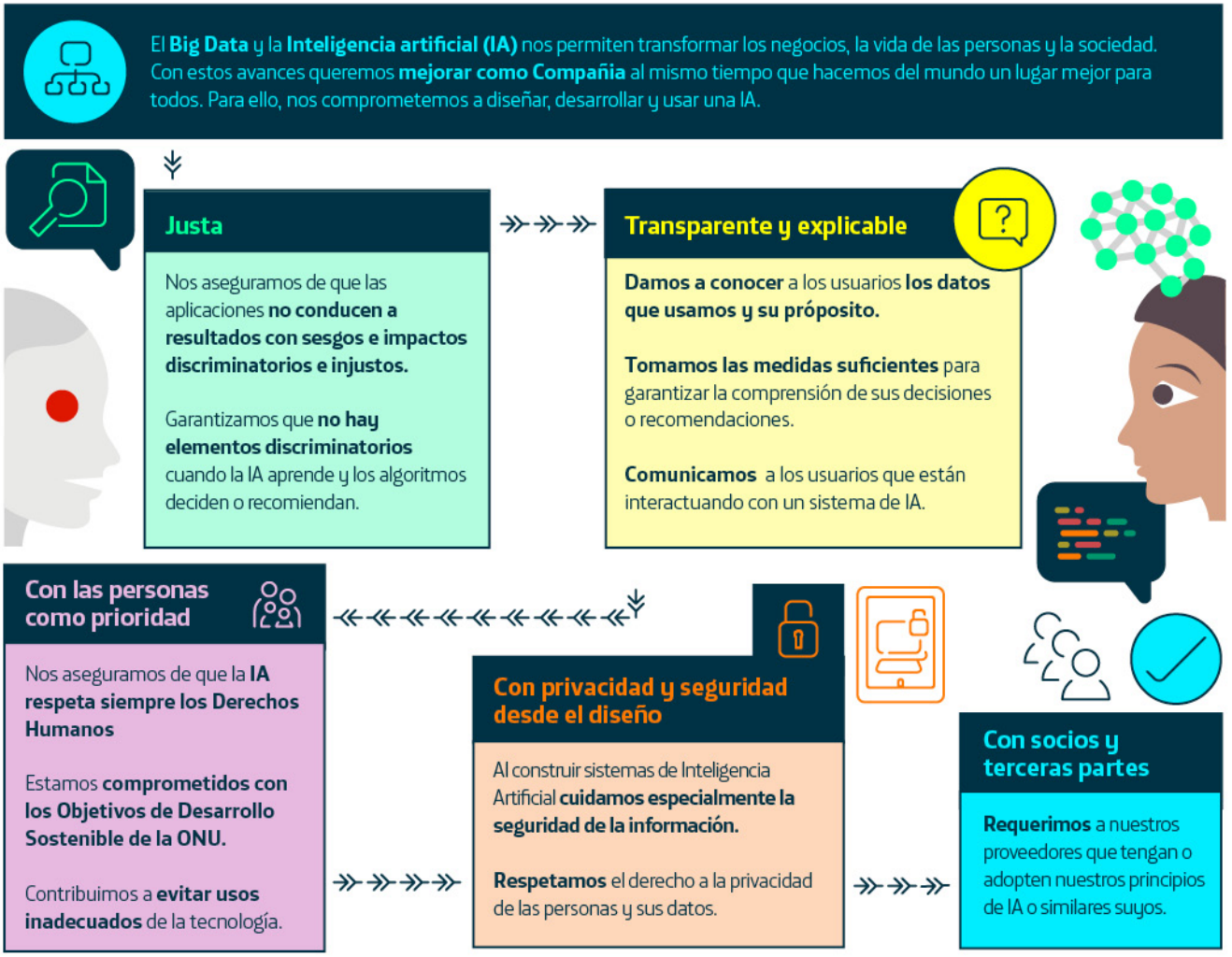
Sin embargo, recientemente se ha expresado una preocupación por el uso de la IA, en particular en relación con la posible discriminación, la falta de interpretabilidad de las conclusiones algorítmicas y la falta de transparencia de los datos personales utilizados. Para hacer frente a esos posibles problemas, Telefónica publicó sus Principios de IA en octubre de 2018 y desde entonces ha trabajado en su implementación a través del siguiente enfoque:

- Un *modelo estratégico (estrategia):* la visión estratégica sobre cómo los Principios de IA encajan con los valores y objetivos de la Compañía.
- Un *modelo organizativo (gobernanza)* que define los roles necesarios y las relaciones entre ellos, de acuerdo con la estructura corporativa, para implementar los Principios de IA.
- Un *modelo operativo (líneas de acción)* que define los principales procedimientos junto con las funciones de los responsables encargados de las tareas a realizar.

2.4.4.1. Estrategia

Telefónica tiene un compromiso firme con los derechos humanos, tal y como se indica en los Principios de Negocio Responsable y la Política de Derechos Humanos. La tecnología debe contribuir a crear una sociedad más inclusiva y ofrecer mejores oportunidades para todos, y la IA puede contribuir a estos objetivos. Con el fin de guiar a la empresa en su aplicación de la IA y el *Big Data* en todas las líneas de negocio, el Comité Ejecutivo adoptó nuestros Principios de IA en octubre de 2018. A través de estos principios nos comprometemos a diseñar, desarrollar y usar la Inteligencia Artificial, 1) de forma justa y no discriminatoria, 2) de manera transparente y explicable, 3) con las personas como prioridad, 4) con privacidad y seguridad desde el diseño y 5) con proveedores y socios que se comprometan con estas u otras normas éticas similares en materia de Inteligencia Artificial.

Nuestros principios de Inteligencia Artificial



2.4.4.2. Gobernanza

Estamos implementando una IA responsable a través de un modelo organizativo y de relación que define qué departamentos de la empresa se ven involucrados, cuáles son sus funciones y cómo se relacionan entre sí para alcanzar un uso responsable de la IA.

Promovemos un enfoque de autorresponsabilidad con un modelo de escalado a demanda. Existe un proceso de escalabilidad de tres pasos que se ilustra en el siguiente gráfico.

Implementación de los Principios de IA

Los jefes/desarrolladores de producto que compran, desarrollan o utilizan IA, deben realizar una simple autoevaluación desde el diseño del producto/servicio que están desarrollando mediante un cuestionario *online*. Esta autoevaluación trata explícitamente los posibles riesgos que puede haber para los derechos humanos relacionados con el uso de la Inteligencia Artificial. Esta autoevaluación se integra en un modelo de gobernanza de tres niveles apoyado por una comunidad de expertos más amplia. Si un jefe/desarrollador de producto (nivel 1) tiene dudas sobre un posible impacto adverso de un determinado producto o servicio una vez completada la autoevaluación, se le plantearán estas dudas automáticamente a un grupo de expertos multidisciplinar de la Compañía (nivel 2), que junto con el jefe/desarrollador de producto, intentarán resolver el problema. En caso de que sea un riesgo potencial para los derechos humanos y/o la reputación de la empresa, el asunto se elevará a la Oficina de Negocio Responsable, que reúne a todos los directores de departamentos relevantes a nivel global (nivel 3).

2.4.4.3. Lineas de Acción

El modelo operativo describe los procedimientos para implementar el enfoque de IA responsable en el día a día de la empresa. Integrada dentro de una visión más amplia de Diseño Responsable, incluye una metodología llamada 'Uso responsable de la IA' inspirada en metodologías ya existentes en privacidad y seguridad por diseño. El modelo operativo consiste, entre otras cosas, en:

- Actividades de formación y concienciación: Telefónica ha desarrollado unos cursos relacionados con la IA y la ética que son accesibles a todos los empleados a través de los portales corporativos habilitados y en tres idiomas (español, inglés y portugués).

- El cuestionario de autoevaluación *online*, donde cada principio de la IA se pone en práctica a través de una serie de preguntas para responder y una serie de recomendaciones. El cuestionario está disponible *online* en español e inglés y se integra dentro de la iniciativa global Diseño Responsable del grupo Telefónica.

- Un conjunto de herramientas técnicas que ayudan a responder a las preguntas. Dado que algunas de las preguntas del cuestionario son imposibles de responder sin herramientas específicas, nuestra metodología incluye tanto herramientas internas como externas (en su mayoría de código abierto).

Ir al capítulo de Cliente

2.4.5. Uso responsable de la Tecnología

2.4.5.1. Estrategia

La vida de nuestros hijos ya es una vida digital. En el momento en el que seamos capaces de asumir esto, seremos capaces de integrar y adaptar las pautas educativas de siempre a un ecosistema en el que lo analógico ha perdido la hegemonía. No se trata de inventar nada nuevo, sino de seguir educando en valores, de acompañar y dar ejemplo, de generar espacios de diálogo y de ir descubriendo de manera conjunta las ventajas y desventajas derivadas del uso que hacemos de la tecnología. De aprender que hay momentos para conectarse a la Red y momentos para conectar con los demás.

Precisamente por esto, y porque en Telefónica estamos convencidos de que son las personas las que dan sentido a la tecnología y no al revés, hemos definido una estrategia global basada en la promoción del uso responsable e inteligente de Internet y de los dispositivos conectados en todos los ámbitos de nuestra vida, pero haciendo especial hincapié en la protección de niños, niñas y jóvenes.

2.4.5.2. Gobernanza

La Comisión de Sostenibilidad y Calidad del Consejo de Administración de Telefónica, S.A. es la responsable de impulsar el desarrollo del Plan Global de Negocio Responsable, que incluye el uso responsable de la tecnología haciendo especial foco en uno de los colectivos más vulnerables: los menores de edad.

Reflejo del compromiso firme de la Compañía con este colectivo, la protección de niños, niñas y adolescentes se encuentra recogida en los Principios de Negocio Responsable y en diferentes políticas corporativas como la Política de Diversidad, la Política de Comunicación Responsable o la Política de Sostenibilidad en la cadena de suministro.

2.4.5.3. Líneas de Acción

Nuestro compromiso y estrategia con la protección al menor de edad en la Red y la promoción del uso responsable de la tecnología, se materializa en seis líneas de trabajo:

Alianzas con grupos de interés

Velar por una Red más segura es una tarea que no podemos abordar en solitario. En Telefónica trabajamos de manera conjunta con aliados sectoriales y de la sociedad civil con el objetivo de que los más jóvenes sean conscientes de que Internet es una ventana abierta llena de oportunidades, pero que también existen riesgos que hay que aprender a gestionar.

En este sentido, podemos destacar nuestra colaboración con:

- Fuerzas y Cuerpos de Seguridad del Estado, así como el apoyo a las diferentes líneas de denuncia nacionales (Equipo Niños, Alianza por la Seguridad en Internet, *Safernet*, Te Protejo, *Centre for Child Protection on the Internet*, Alerta Amber, INADI, etc.).
- ONG, asociaciones nacionales (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., Fundación Ecuatoriana por un Internet Sano y Seguro, AMID, etc.).
- Acciones con grupos de interés clave en la protección *online* de niñas, niños y adolescentes (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 Alternativo CHS, Comunidad de Divulgadores de Conocimiento Científico KUNA, Fundación Habla, *End Violence Against Children*, Gobiernos, etc.).

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

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

A nivel local, la Compañía participa en numerosos grupos de trabajo que fomentan el uso responsable e inteligente de la tecnología entre los más jóvenes: Digitales (España), Mesa de trabajo de Convivencia Escolar – Ministerio de Educación (Chile), Mesa TIC e Infancia (Colombia), Generación Única UNICEF (Argentina), Mesa de trabajo de Accesibilidad y Uso de las TIC – Ministerio de Educación (Ecuador), Grupo de trabajo Internet seguro para todos y todas (México).

Bloqueo de contenidos

En la lucha proactiva contra los contenidos de imágenes de abusos sexuales a menores de edad en la Red, Telefónica procede al bloqueo de estos materiales siguiendo las pautas y las listas proporcionadas por la *Internet Watch Foundation* en los siguientes países: Chile, Ecuador, España, México, Perú, Reino Unido, Uruguay y Venezuela. Telefónica Colombia hace lo propio a través de MINTIC y la DIJIN. En este procedimiento siempre se respeta la neutralidad de red, derecho a libre expresión y sobre todo la normativa vigente, con un bloqueo de contenidos coordinado también con las policías u organismos públicos correspondientes.

Entorno audiovisual

La forma de consumir televisión ha cambiado, sin embargo, no es ajeno a nadie que tanto niños como adolescentes hacen cada vez un uso más intensivo de los contenidos audiovisuales. Las pantallas, además, constituyen una parte

fundamental en su desarrollo personal, social y cívico, razón por la que desde Movistar creemos fundamental:

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

Por ello, contamos con las siguientes iniciativas en nuestras operaciones:

- Etiquetado y catalogación de contenidos por edad y tipología de contenido.
- Controles parentales, PIN parental y PIN de compra en el dispositivo, que permiten al cliente la posibilidad de bloquear canales y contenidos bajo demanda para menores.
- El contenido específico para adultos se presenta en una sección separada de los demás contenidos y es necesario introducir un pin especial para poder acceder a ella.
- Información sobre el uso responsable de la TV en el propio dispositivo y en la web comercial, así como otras actividades de sensibilización sobre el buen uso de las pantallas.
- Aplicación Movistar Junior: *App* infantil para Smartphone y Tablet (iOS y Android) con la que los más pequeños podrán disfrutar del contenido para niños de Movistar+ en un entorno seguro y protegido. Algunas de las funcionalidades de la aplicación: zona de niños con canales de TV en directo, series infantiles bajo demanda, vídeos de actividades, contenidos musicales y zona de padres desde la que las familias podrán realizar las acciones de configuración que deseen: PIN parental, definición del rango de edad para el que estarán disponibles los contenidos (hasta 4 años, de 5 a 7 años y/o de 8 a 12 años), idioma de los contenidos, tiempos de consumo y/o franja horaria de uso.

Productos y servicios

Aunque realmente pensamos que nada podrá sustituir la labor mediadora y educativa de un adulto en el uso responsable de la tecnología, cuando esto no es posible, siempre tendremos el apoyo de la tecnología. Para ello, apostamos por la promoción y el desarrollo de productos y servicios que ayuden a las familias a abordar con éxito el desafío del mundo digital:

- Controles parentales: Vivo Filhos Online (Brasil), Qustodio (España, Chile), Control Parental Movistar TV (Venezuela).
- Soluciones de seguridad con funcionalidad de control parental: Smart WiFi (España).
- Otros servicios (antivirus, packs personalizados): Conexión Segura (España, Argentina, Chile), O_2 Protect (Alemania), Vivo Protege (Brasil), Localizador Familiar (Argentina), Seguridad Dispositivo (España), Seguridad Total (Chile, Colombia), Seguridad Total + Conexión Privada Móvil (Argentina), McAfee Seguridad Digital (Brasil) y McAfee Mobile Security Plus (UK).

Trabajo conjunto con nuestros proveedores

Evaluamos junto a nuestros proveedores la implantación de los parámetros básicos de protección al menor de edad, especialmente en el ámbito de la seguridad, desde el diseño de terminales a sistemas operativos.

Solicitamos tanto a fabricantes de dispositivos como a proveedores de sistemas operativos:

- La inclusión de mecanismos de protección a niños, niñas y adolescentes (control parental, restricción por edades, sistemas de aprobación para la instalación de aplicaciones, sistemas de protección ante compras, límites de uso de aplicaciones y dispositivos, etc.).
- La incorporación de mecanismos de autocontrol, conocidos como de bienestar digital, que permitan hacer un mejor uso de los dispositivos y ofrezcan opciones al usuario para ayudarle a reducir una posible dependencia.
- Que ofrezcan actualizaciones de seguridad con regularidad para proteger a nuestros clientes frente a los nuevos riesgos y amenazas que aparecen constantemente y que ponen en peligro los datos y la privacidad de los usuarios a la vez que prolongan la vida útil de los dispositivos.
- Que incluyan funcionalidades que ayuden al usuario a reducir las distracciones por un mal uso del móvil al volante (uso por voz, silenciado de notificaciones, etc.).

Iniciativas de educación y sensibilización

Hablamos continuamente del reto que supone hoy en día estar al corriente de cada desarrollo tecnológico que aparece en el mercado, no por el simple hecho de conocer las versiones más modernas de *gadgets*, o de lo último en robótica e Inteligencia Artificial, sino porque cada avance nos pone a todos, grandes y pequeños, delante de un nuevo reto educativo que debemos saber aprovechar.

Telefónica, consciente de esta realidad, apuesta por el desarrollo de iniciativas formativas y de sensibilización para todos los públicos que faciliten la convivencia en una sociedad cada vez más digital.

El portal Dialogando es una muestra de ello. La iniciativa, implantada en 10 países de la Compañía, ayuda a la sociedad a reflexionar sobre el uso que hacemos de la tecnología en nuestro día a día gracias a los recursos que elabora un comité

de expertos en diferentes materias relacionadas con la vida digital.

Se han llevado a cabo un centenar de iniciativas de concienciación en las siguientes temáticas: uso de la tecnología durante la pandemia, *grooming*, *sexting*, ciberacoso, brecha digital, cibercontrol y violencia, tolerancia en Internet, bienestar digital, conducción responsable, fraude *online*, privacidad de datos, identidad digital, *fake news*, *eSports* y *gaming*, ocio digital, etc. con más de 166 millones de personas impactadas a través de estas acciones y de la mano de colaboradores como Club de Malasmadres, FAD, iWomanish, Gonvarri, Faro Digital, RedPapaz, Sin Trata A.C., Fundación Habla, CHS Alternativo, NSPCC, entre muchos otros.

2.4.6. Asuntos transversales de confianza digital

2.4.6.1. Control interno

Con el objetivo de atender y cumplir con las disposiciones legales de los países relacionadas con las leyes y regulaciones locales de protección y privacidad de datos, dentro del Plan Anual 2020 se realizaron un total de 10 trabajos de auditoría específicos para verificar su cumplimiento, así como la identificación de las mejores prácticas en temas de protección de datos.

El aspecto más relevante en las operadoras europeas, que están afectadas por la nueva legislación en materia de protección de datos (GDPR), ha sido revisar la implantación del Modelo de Gobierno. En el resto de países afectados por leyes locales de protección de datos, los aspectos más importantes revisados han sido: la verificación de la aplicación de las medidas de seguridad en el tratamiento de los datos personales, verificar que se aseguran la integridad y calidad de la información y revisar que se ha obtenido el consentimiento de los usuarios para el tratamiento de sus datos personales.

En el Plan Anual también se han potenciado trabajos de auditoría relacionados con la ciberseguridad y la seguridad en Redes y Sistemas, teniendo como objetivo validar el nivel de acceso lógico y la integridad de la información y contenidos almacenados en los elementos que conforman dichas Redes y Sistemas. Durante 2020 se realizaron 65 trabajos de esta naturaleza.

2.4.6.2. Formación y concienciación

Durante 2020, 80.222 asistentes completaron formación en materia de privacidad, protección de datos, seguridad y ciberseguridad. De estos cursos se han impartido un total de 105.700 horas de formación.

Adicionalmente se han reforzando los programas de comunicación y concienciación en esta materia, utilizando diferentes canales para garantizar la llegada de los mensajes a todos los niveles y geografías de la empresa.

2.4.6.3. Relación con los grupos de interés

Telefónica participa activamente en distintas organizaciones y foros internacionales, la mayor parte de ellos de naturaleza multipartita. En 2020 se destaca:

Internet Governance Forum (IGF)

Nuestro director de Políticas Públicas e Internet finalizó a término de 2020 el mandato máximo de tres años como miembro del Grupo Consultivo (MAG por sus siglas en inglés). Su principal objetivo es asesorar al secretario general sobre el programa y el calendario de las reuniones del Foro.

Este año hemos participado en la decimoquinta edición del IGF celebrado en la modalidad *online* por primera vez en su historia bajo la organización de las Naciones Unidas con el lema 'Internet para la resistencia y la solidaridad humana', en el que destacó la adopción de Internet como herramienta para afrontar la crisis asociada al COVID-19 y cómo abordar las barreras que limitan su adopción y han resultado en un incremento de las desigualdades de manera más evidente durante la pandemia. Entre otros, participamos en el *workshop* #128 Crisis globales y usos socialmente responsables de datos y en el Pre-event #30 De Principios a la implementación: Inteligencia Artificial y el papel del Sector Privado

Foro de Gobernanza de Internet en España

Con foco en el debate en la digitalización y la sostenibilidad en un mundo post-COVID, beneficios sociales del uso de datos, se han abordado el uso de la tecnología en la lucha contra el COVID-19, su impacto social y cómo avanzar en una digitalización y desarrollo sostenible, y la geopolítica de la tecnología entre otros.

Global Network Initiative (GNI)

Participamos desde el 2017 en esta organización multipartita para avanzar en la protección y promoción de la libertad de expresión y la privacidad en la industria de las TIC.

Para ello se acuerdan estrategias y posicionamientos conjuntos sobre los derechos de libertad de expresión y de privacidad. Durante este año se han organizado diversos eventos *online* con especial hincapié en el impacto del COVID-19 en el uso de tecnologías de rastreo y las solicitudes de los gobiernos sobre los derechos de libertad de expresión y privacidad en distintas regiones del mundo.

Consejo de Europa

Somos miembros del partenariado establecido en 2017 entre empresas digitales, operadoras, organizaciones sectoriales y el Consejo de Europa para la promoción de derechos digitales. En el 2020 hemos participado activamente en el grupo de trabajo establecido por el *Ad hoc Committee on Artificial Intelligence* (CAHAI) para la elaboración de un estudio preparatorio sobre la regulación de la Inteligencia Artificial en el ámbito de los derechos humanos, la democracia y el Estado de Derecho que servirá de base para la futura propuesta del Consejo de Europa en esta materia.

Internet & Jurisdiction
Cooperamos con esta organización *multistakeholder* que se centra en los problemas jurisdiccionales que plantea el carácter transfronterizo de Internet facilitando un proceso de diálogo estructurado entre sus miembros para permitir el desarrollo de estándares globales que facilite la cooperación transnacional y la coherencia de las políticas.

Durante el 2020 hemos participado activamente en la elaboración del informe de estatus regional de América Latina que se ha realizado con la Comisión Económica para América Latina y el Caribe (CEPAL) y con *Die Deutsche Gesellschaft für Internationale Zusammenarbeit* (GIZ). Es el primer y más amplio informe realizado en la región que identifica las diferentes tendencias de política que giran en torno al carácter transfronterizo de Internet y la forma en que afecta a los diferentes interesados, como los gobiernos, las empresas y la sociedad civil.

Cybersecurity Tech Accord
Telefónica es miembro fundador de esta iniciativa nacida del sector privado. Se trata de un esfuerzo conjunto de más de 140 empresas de todo el mundo cuyo objetivo principal es proteger a los usuarios de Internet frente a la creciente evolución de las ciber amenazas. La concienciación a los usuarios sobre la adopción de medidas de salud cibernética y a los gobiernos sobre la necesidad de adoptar medidas responsables en materia de ciberseguridad son otras de las principales tareas que se llevan a cabo desde la organización.

Iniciativa fAIr LAC
Telefónica, un año más, participa en la iniciativa FairLac, del Banco Interamericano de Desarrollo, junto a otros socios tecnológicos. El objetivo es promover el desarrollo de IA ética y transparente de los servicios públicos en la región latinoamericana.

En 2020, a pesar de la pandemia del COVID-19, se ha avanzado en el desarrollo de varios casos de uso de la IA responsable en salud, así como se ha inaugurado un nuevo HUB en Medellín, para promover la IA en políticas de diversidad de género.

Telefónica, además, participa con la promoción del uso de la IA en las políticas de empleo, aportando el caso de uso del Programa Destino Empleo de Fundación Telefónica en Chile.

OECD
Somos miembros de 'Business at the OCDE', donde nuestro director de políticas públicas e Internet es vicepresidente de la comisión de Economía Digital. Durante 2020 hemos continuado colaborando con el grupo de Inteligencia Artificial (AIGO), y en la revisión de recomendaciones de banda ancha y del mercado digital en Brasil.

EU Expert Group on B2G Data Sharing
Participamos en el grupo de expertos de la Comisión Europea sobre *Business-to-Government (B2G) data sharing.*

The European AI Alliance
Nuestro *Chief AI & Data Strategist* es miembro de la Alianza Europea de IA de la Comisión Europea, una plataforma para discutir abiertamente sobre temas de inteligencia artificial y su impacto.

Iniciativas de IA de GSMA & ETNO
Somos miembros de la *Task Force on IA for Impact* de GSMA (Global System for Mobile Communications) y de la *Task Force on Artificial Intelligence* de ETNO (European Telecommunications Network Operators' Association).

Pacto Digital

En Julio de 2020 publicamos nuestro Pacto Digital (https://www.telefonica.com/es/web/public-policy/pacto-digital-de-telefonica) para reconstruir mejor nuestras sociedades y economías después de la pandemia. En la senda del Manifiesto de 2018 (https://www.telefonica.com/manifiesto-digital/), el Pacto Digital promueve el establecimiento de unas reglas del juego adaptadas a la nueva realidad post-COVID para evitar las desigualdades en el mundo digital, fomentar el acceso a la conectividad de nueva generación y a la protección de los derechos humanos frente a las amenazas tecnológicas. Un Pacto Digital que, de nuevo, se centra en las personas y que está basado en el diálogo y el acuerdo entre Administraciones, sociedad y empresas, basado en cinco prioridades:

- **Impulsar la digitalización para una sociedad y economía más sostenible;**
- **Abordar las desigualdades invirtiendo en las aptitudes digitales y adaptando el Estado de bienestar;**
- **Construir una conectividad inclusiva y sostenible;**
- **Garantizar una competencia justa mediante la modernización de los marcos fiscales, regulatorios y de competencia; y**
- **Mejorar la confianza mediante un uso ético y responsable de la tecnología.**

2.4.7. Hitos 2020 y Retos 2021 GRI 418-1

> Hitos 2020:

En 2020 alcanzamos el 100% de cumplimiento en cada una de las siguientes metas fijadas:

- **Centros de privacidad locales en el 100% de los países.**
- **Digitalización de todo el proceso de gestión relacionado con los aspectos de seguridad a lo largo de todo el ciclo de vida de los proveedores.**
- **Implementación de los Principios de IA en la Compañía a través de un modelo de gobernanza global.**
- **Nuevas líneas de actuación que nos permitan abordar el uso responsable de la tecnología y la protección del menor en la Red.**
- **Colaboraciones/Alianzas que nos permitan profundizar el alcance de nuestras acciones de sensibilización en el ámbito del uso responsable del móvil al volante.**

Además, hemos alcanzado los siguientes hitos:

- **Publicación del Pacto Digital de Telefónica.**
- **Revisión y refuerzo de las medidas de seguridad relacionadas con el acceso remoto y el teletrabajo.**

> Retos 2021:

- **Actualización del Centro de Transparencia Global.**
- **Avance en la implementación de la digitalización de la privacidad.**
- **Digitalización de los procesos de gestión de la continuidad de negocio.**
- **Continuación de la implementación de los Principios de IA en la Compañía.**
- **Nuevos formatos y canales para comunicar los mensajes relacionados con la protección al menor y el uso responsable de la tecnología que nos permitan conectar más y mejor con los diferentes públicos**

Resumen de indicadores clave

Indicadores	2019	2020
Nº de asistentes a cursos de formación en Protección de Datos y Ciberseguridad	54.991	80.222
Nº de horas de formación en Protección de Datos y Ciberseguridad	104.558	105.700
Nº de procedimientos abiertos por temas Protección de Datos	66	61
Nº de multas por temas de Protección de Datos (*)	22	15
Cuantía de multas (euros) por temas de Protección de Datos (*)	243.595	328.594
Número de consultas/reclamaciones en temas de Protección de Datos/ Privacidad en el Canal de Negocio Responsable	6	15
Número de consultas/reclamaciones en temas de Libertad de Expresión en el Canal de Negocio Responsable	0	0
Nº de auditorías internas en Protección de Datos y Ciberseguridad	69	75
Número de auditorías externas en materia de Seguridad en Productos y Servicios (**)	13	10
Nº de incidentes/brechas de Seguridad de la Información o de Ciberseguridad con alto impacto que han afectado a datos de carácter personal de clientes	1	0
Alcance de las iniciativas de formación y concienciación sobre el uso responsable de la tecnología (personas)	223.725.282	166.470.613

(*)Tras la aplicación del criterio de "resolución firme " en materia de multas, una resolución/multa en Brasil se ha trasladado de 2019 a 2020.
(**) Productos y Servicios que están auditados: 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.