Asociación Española de Compliance

# Grupos de trabajo de ASCOM

## Protección de datos y nuevas tecnologías

Tecnologías innovadoras aplicadas al Compliance

Septiembre 2020

www.asociacioncompliance.com

# Tecnologías innovadoras aplicadas al Compliance

## 1. Objetivo del documento

El presente trabajo tiene como objetivo principal poner a disposición de la comunidad dedicada al Compliance, ya sea como prestadores de servicios relacionados con la materia, o bien a los Compliance Officers de organizaciones, unas nociones básicas respecto a tecnologías de la información que juegan un papel importante en el día a día del Compliance, ya sea como herramientas para su adecuada aplicación y gestión, o bien como herramientas de trabajo.

De esta forma, se pretende introducir los conocimientos básicos y esenciales relacionados con determinadas tecnologías de la información muy novedosas, que están siendo utilizadas en la actualidad para llevar a cabo procesos propios de las áreas de Compliance, o bien, respecto de las que en el día a día reciben requerimientos desde las diferentes áreas de negocio los Compliance Officers.

## 2. Tecnología de "blockchain" aplicada al compliance

### 2.1 Contexto normativo. Obligaciones en materia de información no financiera

Cuando hablamos de blockchain enseguida nos viene a la cabeza un producto: las criptomonedas y dentro de éstas, el caso de éxito más sonado, el Bitcoin.

Blockchain es una parte de una tecnología más amplia conocida como DLT (Distributed Ledger Technology), traducida como tecnología de registros distribuidos.

Al margen de la posibilidad de generar criptoactivos o criptomonedas (al inicio odiadas y poco a poco estudiadas por los bancos centrales, incluso como una posibilidad realizable) esta tecnología promete muchas mejoras, como incrementar la eficiencia en los procesos y dos cuestiones clave que siempre nos han preocupado en el Compliance: la transparencia y la trazabilidad.

Pero no todo son bondades, también existen riesgos, como en cualquier nueva tecnología que se implanta, y estos riesgos cada vez afectan más a una globalidad que a un único usuario.

Sin entrar en otros riesgos, como serían los tecnológicos o medioambientales y que no son objeto de este capítulo, podemos citar los que sí tienen una naturaleza más legal o de cumplimiento normativo: la firmeza de las transacciones, la gobernanza, la privacidad de la transacción o el registro y tratamiento de datos de carácter personal (incluyendo el borrado de datos).

## 2.2. Definición

Un registro distribuido (DLT) es una base de datos descentralizada que gestionan varios participantes y que se caracteriza por un proceso de validación consensuado y reglado entre las partes. Esta base de datos se actualiza de forma sincronizada por acuerdo de los participantes, generándose copias idénticas que están distribuidas entre los mismos.

Dentro del DLT, la tecnología de cadena de bloques (*blockchain) permite almacenar la información agrupando las transacciones por bloques en orden secuencial, conectándolos de forma cronológica para crear una cadena de bloques.*

*La integridad y la seguridad de los datos almacenados en la cadena se garantizaría mediante criptografía (técnica de cifrado que hace ininteligible un mensaje para aquel que no es su destinatario).*

## 2.3. Origen

En el año 2008, Satoshi Nakamoto, cuya identidad es aún desconocida, o incluso podría ser el pseudónimo de un grupo de personas, publicó un artículo que describe un sistema Peer to Peer (P2P) de dinero digital. Tan sólo un año más tarde, lanzó la popular moneda virtual, el bitcoin.

Con el bitcoin, sobre la base del blockchain se podrían hacer transacciones entre desconocidos sin la necesidad de requerir a un tercero de confianza y con cierta seguridad, al utilizar una solución criptográfica.

Durante todo este tiempo, poco a poco estas soluciones basadas en el blockchain han ido captando el interés de los distintos sectores, que han ido estudiando y desarrollando posibles aplicaciones para empresas tecnológicas, el sector financiero o incluso las propias autoridades supervisoras.

## 2.4. Cómo funciona, la nueva industria minera

La tecnología *DLT combina tres tecnologías ya existentes: (i) Las redes P2P (Peer to Peer, es decir, de consumidor a consumidor), con las que a principios de siglo compartimos de forma altruista nuestra música y películas con otros usuarios (napster, emule, Torrent, ares…); (ii) la criptografía, que permite el intercambio seguro de contenidos mediante un cifrado y que se usa por ejemplo en procesos tan comunes como la firma digital y (iii) los algoritmos de consenso, que permiten a participantes desconocidos que se pongan de acuerdo, es decir, garantizar que los registros de los participantes son idénticos, sin fraudes ni duplicidades.*

*De entre los algoritmos de consenso utilizados el más famoso es el "proceso de minado" (proof of work). En él, los participantes (mineros, coloquialmente) entran en redes públicas o privadas -a estas últimas, de acceso restringido- para validar y crear nuevos bloques de la cadena a través de complejas pruebas de trabajo criptográfico (minado). A cambio de este trabajo de validación y generación de bloques y criptografía, pueden recibir incentivos o recompensas, por eso que comúnmente se les denomina mineros.*

*El proceso de blockchain más famoso, el utilizado por los Bitcoin, utiliza redes públicas y abiertas, que plantean entre otros un problema relevante: ¿cómo mantener la privacidad de las transacciones? A este reto se le suman otros retos relevantes, ¿cómo se procede al borrado de esos datos? ¿bajo qué jurisdicción se encuentran? ¿cómo se protege la confidencialidad del usuario?*

## 2.5. Aplicaciones prácticas

Si esta tecnología ha conseguido hacerse un hueco entre los bienes más valiosos y probablemente el activo más utilizado a nivel global, como es el dinero, ¿dónde está el límite?

Curiosamente las divisas son elementos que tradicionalmente han requerido de un respaldo y una intervención de autoridades públicas que regulen su emisión, su valor, su contravalor, sus movimientos…, y no sólo como moneda de cambio, también de forma especulativa.

La irrupción de los criptoactivos o criptomonedas al principio se vio como una amenaza sobre el sistema financiero tradicional, desaconsejando su uso o generando advertencias de los propios supervisores. Sin embargo, recientemente el Banco Central Europeo ha urgido a su estudio como posible emisor.

Sin llegar a la emisión de criptomonedas, ¿dónde más está emergiendo esta tecnología?: en los pagos, en la contratación y custodia de valores, el comercio internacional… y también se puede utilizar en ámbito de cumplimiento normativo, dentro de las denominadas Fintech o Regtech, que aglutinan soluciones tecnológicas basadas en la nube, en el big data o en el blockchain.

Estas soluciones pueden mejorar la calidad y trazabilidad de los datos que utilizan, facilitando así cumplir con materias que históricamente han formado parte de nuestro mapa de riesgos de cumplimiento: el conocimiento del cliente (KYC, Know Your Customer), tan vinculado a la prevención del blanqueo de capitales y la financiación del terrorismo, la trazabilidad de las transacciones, el reporte a los reguladores, la calidad de datos en la presentación de declaraciones informativas, la mejora en transparencia o en la gestión de los riesgos.

## 2.6. Algunos ejemplos de uso

Cada vez más emerge como solución para proyectos de seguridad, salud, medioambientales, acción climática, energías renovables y proyectos globales que traspasan fronteras. Son los casos por ejemplo de las plataformas para el comercio de gases de efecto invernadero o de derechos de emisión de carbono, que requieren asegurar la trazabilidad, la transparencia y la verificación objetiva de la transacción.

Entre los casos de éxito, podemos citar algunos proyectos pilotos entre los que se encuentran las redes eléctricas inteligentes, en las que los particulares pueden acceder al mercado mediante la compra y venta entre particulares de energía eléctrica de origen renovable, fijando a través de tecnología blockchain el precio y la cantidad de energía que quieren poner en distribución a través de transacciones seguras entre particulares. Son los casos por ejemplo de plataformas como equigy (https://equigy.com/) o quartier strom (https://quartier-strom.ch/index.php/en/homepage/).

## 2.7. Riesgos y beneficios

Centrándonos en el ámbito de los riesgos y beneficios normativos simplemente y obviando otros riesgos y beneficios de índole más técnico o incluso estratégicos o medioambientales, destacamos los siguientes:

- El principal riesgo al que nos enfrentamos es su falta de madurez. Como toda nueva tecnología, no está carente de riesgo, por lo que con los años va ganando robustez confianza y seguridad. No en vano, el Reglamento General de Protección de Datos 679/2016 exige evaluaciones de impacto para aquellos tratamientos de datos que utilicen nuevas tecnologías, por lo que a buen seguro la utilización de blockchain en los procesos de la empresa requerirá de una evaluación de impacto, que analizará los riesgos y beneficios específicos de la solución tecnológica de cada negocio.
- También hay un riesgo relevante en la necesidad de tener conocimientos técnicos para su correcto entendimiento. El desconocimiento en sí, dentro del cumplimiento normativo, siempre ha sido un quebradero de cabeza cubierto con acciones formativas y de concienciación. La utilización cada vez más de elementos tecnológicos facilita la trazabilidad de los procesos y gana eficiencias, pero necesita de una acción constante de actualización de conocimientos.
- Además, todavía no existe un marco regulatorio claro en cuanto a los registros que se producen por los participantes, existen dudas acerca de la posibilidad de borrado de datos tras su uso o de cuándo se pueden entender firmes las transacciones.
- Por otro lado, el hecho de utilizar un ecosistema digital íntegramente y con múltiples nodos en los que se encuentra la información, hace que la ciberseguridad impacte mucho más en los riesgos de seguridad y confidencialidad, lo que podría ser objetivo y foco de atención de los atacantes.

- La gobernanza del sistema utilizado, la transparencia en los procesos y la identificación de sus responsables. Estos modelos serán más sencillos si se utilizan plataformas privadas, pero tampoco estará exento de riesgos.
- Entre los beneficios, tendremos:
- La posibilidad de mejora en el conocimiento del cliente, la utilización de la Regtech mejora el conocimiento de la transaccionalidad de los clientes, por lo que se mejora en el cumplimiento del tradicional Know your Customer (KYC).
- Fruto de la anterior, mejora en el cumplimiento de la prevención del blanqueo de capitales y financiación del terrorismo, a través de la citada mejora en el conocimiento de la transaccionalidad e inmediatez.
- También es posible la mejora el reporte regulatorio, al tener una calidad del dato superior y una trazabilidad más completa, disminuyendo las incoherencias en los datos archivados en diferentes repositorios.
- Podría mejorarse la adaptabilidad a normativas cada vez más tecnológicas, pero que nos afectan en nuestro día a día, la aplicación de la Directiva de Servicios de Pago (PSD2), con previsiones en cuanto a factores de autenticación o incluso el Reglamento de Protección de Datos -aquí en una doble vertiente, tanto por el riesgo, como por la adaptación al entorno digital-.

# 3. Internet de las cosas (iot) aplicada al compliance

## 3.1. Introducción

El Internet de las Cosas (en inglés IoT, *Internet of Things)* es un concepto que se refiere a la interconexión digital de objetos cotidianos con Internet, la conexión de Internet con más “cosas u objetos”, que personas.  IoT permite que se conecten “cosas” en cualquier momento (cualquier contexto), en cualquier lugar (en cualquier lugar) con cualquier cosa (cualquier dispositivo) y cualquier persona (cualquiera) que use cualquier ruta (cualquier red) y cualquier servicio o negocio.

Se trata de un concepto que nació en el Instituto de Tecnología de Massachusetts (MIT) en 1999 por Kevin Ashton, profesor del MIT en aquel entonces, inicialmente para promocionar la identificación por radiofrecuencia (RFID).

Encontramos IoT tanto a nivel consumidor como en a nivel empresarial e industrial y su aplicación abarca a multitud de diferentes sectores (automotriz, telecomunicaciones, energía, entre otros). Hablamos de ciudad inteligente, red inteligente, automóvil inteligente, hogar inteligente, etc. En cada uno de estos campos, las aplicaciones se desarrollan para permitir la interacción entre los propios objetos, transfiriendo información en tiempo real.

Por ejemplo, para controlar los electrodomésticos en un hogar inteligente disponemos de termostatos inteligentes, calefacción, iluminación y dispositivos electrónicos conectados se pueden controlar de forma remota a través de ordenadores, teléfonos inteligentes u otros dispositivos móviles, cámaras conectadas a Internet que permiten publicar imágenes en línea, dispositivos médicos implantables o la automatización de la ciudad mediante sistemas que pueden recopilar y analizar datos sobre los usuarios, que envían mensajes a otras tecnologías y permiten aumentar la calidad de vida de las personas.

## 3.2. Aplicaciones prácticas

El futuro de IOT pasa por "conectar" dispositivos. Por ello, las aplicaciones prácticas que pueden aparecer son variadas, ya que los modelos tradicionales de negocio pueden contar con nuevos cambios derivados de la interconexión masiva de dispositivos, herramientas o procesos. Algunos de los ejemplos de IOT que están adquiriendo protagonismo son:

A) **Coches autónomos:** los coches autónomos, entendiendo por esto los automóviles que prescinden de la figura del conductor, constituyen una realidad y un ejemplo de la aplicación de IOT al sector de la automoción. Equipados con decenas de sensores, estos vehículos recopilan y tratan grandes cantidades de datos de tráfico de otros vehículos interconectados, personas, condiciones de la carretera como limitaciones de velocidad, mapas de ciudades y carreteras, procesando dicha información a alta velocidad. Los beneficios de contar con coches autónomos son palmarios, ya que podría mejorar la logística empresarial, reducir el factor humano en los accidentes o aumentar la eficiencia durante la conducción, minimizando las emisiones contaminantes a la atmósfera.

B) **Carteras inteligentes:** las carteras inteligentes son una tecnología que están comenzando a desarrollar grandes empresas, cuyo objetivo es minimizar la intervención humana durante el proceso de compraventa en negocios físicos. La implementación de esta tecnología necesita una serie de elementos: sensores en los estantes de las tiendas, que permitan recoger información sobre los artículos depositados en ellos y sobre el momento en el cual un cliente lo incorpora a su cesta de la compra, sensores en las puertas de salida de las tiendas y una billetera online. Con estos elementos, la acción de realizar la compra puede sufrir grandes cambios; un cliente que realice esta modalidad de compra estará incorporando artículos a su propio carrito virtual cuando extraiga artículos de los mostradores, confirmando la compra de dichos artículos al salir del establecimiento, lo que conllevaría el cobro de los artículos a través de una billetera virtual propiedad del usuario.

C) **Dispositivos portátiles:** las gafas inteligentes, pulseras Fit y smartwatches, engloban un conjunto de dispositivos conocidos como dispositivos portátiles y que en la práctica suponen ejemplos de IOT con multitud de aplicaciones; las gafas inteligentes permiten facilitar información al usuario sobre determinados objetos sobre los que dirija su mirada, las pulseras Fit captan y proporcionan datos relativos a las constantes vitales como podrían ser las pulsaciones por minuto, tensión arterial, cambios en la temperatura corporal, etc… y por último, los “smarwatch” pueden proporcionar datos de interés sobre el entorno que nos rodea y que puedan satisfacer necesidades precisas del usuario.

D) **Hogares inteligentes:** posiblemente, este es uno de los ejemplos más populares dentro del IOT. La implantación de sensores y conexiones en los elementos que componen nuestros hogares, permiten la configuración y uso de los mismos de forma remota, por ejemplo, posibilitando la elevación de las persianas de forma remota, gestionar la temperatura de la vivienda, controlar el encendido de luces de forma que se dé la apariencia de que hay gente en la misma vivienda y hasta configurar el encendido de determinados aparatos con un consumo elevado de electricidad en las horas del día en las cuales la electricidad es más barata.

E) **Hoteles inteligentes:** en la actualidad, se está trabajando en el desarrollo e implementación de aplicaciones que puedan descargarse los clientes en sus teléfonos móviles y que permitan sustituir las tradicionales tarjetas magnéticas de los hoteles y que permitan gestionar la temperatura o iluminación de la habitación.

## 3.3. Riesgos y beneficios

Los posibles riesgos que pueden materializarse en la implementación o uso de dispositivos IoT son:

A) **Identificación de la información personal:** la información personal sólo se puede transmitir cuando el objeto está vinculado a una persona, con una conexión directa o indirecta. Se produce un enlace directo cuando el usuario es consciente y da su consentimiento para una posible transmisión de sus datos personales. O, cuando una persona compra algo y hay una etiqueta RFID u otra en el objeto, esto podría ser un riesgo para la privacidad, especialmente si la persona se vincula automáticamente al objeto durante el proceso de compra, como por ejemplo mediante el uso de un crédito o tarjeta de fidelidad. Alternativamente, la conexión es indirecta cuando el objeto está vinculado a una persona indirectamente a través del uso de información que pertenece a esa persona.

B) **Creación de perfiles:** si los objetos están vinculados a una persona, será posible obtener información personal sobre esa persona a través de la información transmitida a través de Internet por cada objeto. Una vez que las personas compran bienes o servicios utilizando métodos de pago electrónico, es simple vincular los tipos de productos comprados a su hábito y estilo de vida.

C) **Geolocalización:** mediante nuestros dispositivos (en primer lugar, los teléfonos inteligentes) es sencillo encontrar detalles precisos sobre la ubicación de una persona.

D) **Responsabilidad por violaciones de datos y pérdida de datos:** el IoT tiene efectos sobre la responsabilidad cuando los datos recopilados y transmitidos carecen de las medidas de seguridad adecuadas.

### 3.4. Medidas preventivas y controles

A la hora de llevar a cabo el diseño, desarrollo y despliegue de elementos de IoT, debemos tener presente que los riesgos para la privacidad de los usuarios aparecen durante todo el ciclo de vida de los datos que van a ser tratados. Por ello, desde el diseño, se debe tener en cuenta la privacidad como un principio rector a tener en cuenta.

Por tanto, existen una serie de medidas que necesariamente deben tomarse en cuenta.

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES |
|---|---|---|
| Identificación de la información personal | Análisis de riesgos del flujo de vida de los datos personales | Visado de proyectos que impliquen modificaciones en el flujo de vida de los datos |
| | Anonimizar datos personales | Revisión procedimientos de anonimización |
| | | Pruebas de reversing, OSINT |
| | Bastionado de apps y dispositivos donde se almacenen los datos personales | Procedimientos de actualización de medidas de seguridad de apps y dispositivos |
| Creación de perfiles | Protección de los datos en reposo y en tránsito | Pruebas de penetración |
| | Adecuada gestión derechos de acceso lógico | Revisión directorio activo |
| Geolocalización | Minimizar el tratamiento de datos personales | Auditoría periódica del Registro de Actividades de Tratamiento |
| | | Revisión permisos de apps |

# 4. Computación en la nube aplicada al Compliance

## 4.1. Introducción

Una primera aproximación para entender los sistemas Cloud o sistemas de informática en la nube, sería entender estos como el servicio mediante el cual se utilizan los sistemas informáticos de terceras empresas para fines propios. Para ello, estas empresas invierten capital en proporcionar una estructura de hardware, software y personal que permiten prestar este servicio tanto a personas físicas como a otras empresas.

Los servicios en la nube se pueden emplear para llevar a cabo el almacenamiento de datos o también para emplear la capacidad de computación que estas empresas proporcionan a sus clientes, para llevar a cabo operaciones informáticas y procesamientos de datos complejos. Por tanto, podríamos entender que los sistemas Cloud tienen dos vertientes, en atención a la finalidad del servicio que se vaya a contratar, pudiendo actuar como repositorios de datos o como procesamiento en la nube.

Las principales características la computación en la nube son:

A) **Rentabilidad:** El planteamiento de la informática en la nube parte de la base de convertirse en su servicio rentable para las empresas, por lo que se trata de proporcionar un modelo de precios de pago por uso, basándose en el consumo real que se vaya a llevar a cabo. Este tipo de servicio es rentable por tanto al permitir:

- Eliminar los costes iniciales de infraestructura, al no tener que disponerse de máquinas que funcionen como servidores internos ni el coste de la instalación asociada a los mismos.
- Eliminar los costes derivados de la gestión de la infraestructura.
- Pagar para obtener recursos adicionales, por lo que se puede ajustar el servicio contratado en función de las necesidades existentes.

B) **Escalabilidad:** la escalabilidad se define como la posibilidad de aumentar o disminuir los recursos y servicios en función de las necesidades, pudiendo encontrar escalabilidad horizontal o vertical:

- Escalabilidad vertical: Consistente en agregar más recursos para aumentar el rendimiento de un servidor contratado.
- Escalabilidad horizontal: Consistente en agregar más servidores al servicio contratado para que funcionen como una unidad.

C) **Elasticidad:** la elasticidad es la propiedad de que los sistemas incorporen o disminuyan automáticamente los recursos que se emplean en función de las necesidades existentes. De esta forma, el empleo de recursos siempre se puede ajustar a las necesidades reales, ajustando mejor el coste del servicio.

D) **Confiabilidad:** los servicios Cloud proporcionan servicios de alta disponibilidad permitiendo que los datos estén siempre disponibles, basándose en la redundancia de las arquitecturas de red, de forma que, si un componente que interviene en la red falla, otro elemento de similares características entra en funcionamiento, asegurando la disponibilidad de la información.

E) **Acceso global:** los proveedores de estos servicios pueden disponer de centros de procesamiento de datos repartidos por diferentes regiones, de forma que permiten adaptar el servicio prestado a los requisitos locales existentes en materia de procesamiento de datos.

## 4.2. Aplicaciones prácticas

Si tenemos en cuenta los diferentes modelos de implementación de servicios en la nube, podemos diferenciar entre tres modelos de servicio en la nube:

A) **Nube pública:** en este modelo, una empresa nos proporciona un entorno en el cual todos los procesos que queremos llevar a cabo se ejecutan en sus centros de procesamiento de datos. Un ejemplo sería mediante la contratación de servicios de nube pública para alojar en ella una página web, lo que conllevaría el ahorro en la instalación y mantenimiento de los servidores donde se hospede pero que también implicaría un menor control sobre las medidas de seguridad implementadas.

B) **Nube privada:** en este modelo, se implementa un entorno virtualizado dentro del centro de procesamiento de datos propio. Esto permite llevar a cabo la asignación de recursos a actividades concretas con las características de elasticidad y escalabilidad. Sin embargo y a diferencia de la nube pública, los costes de instalación y mantenimiento de infraestructura perdurarían. Un ejemplo de empleo de nube privada podrían ser determinados sistemas que por legislación deban permanecer en un territorio determinado o que requieran la implementación de una serie medidas de seguridad concretas que la nube pública no pueda proporcionar.

C) **Nube híbrida:** mediante este modelo se combinan ambos tipos de nubes, permitiendo por ejemplo contar con una página web o un blog hospedada en una nube pública que conecta con una base de datos alojada en una nube privada. Este supuesto es especialmente eficaz cuando tenemos en cuenta la regulación en protección de datos.

En atención al tipo de servicio, las nubes pueden proporcionar servicios IaaS, PaaS y SaaS:

A) **IaaS:** infraestructura como servicio o IaaS (*Infrastructure as a Service)* es el servicio que permite ofrecer el mayor nivel de control posible sobre el hardware al suponer la contratación del mismo exclusivamente, prescindiendo de sistemas operativos y software. Este servicio se utiliza principalmente cuando se tienen que llevar a cabo la migración de cargas de trabajo, o para realizar el almacenamiento de copias de seguridad y recuperación.

B) **PaaS:** plataforma como servicio o PaaS (*Platform as a Service)* es el servicio que además del hardware proporciona el entorno donde probar programas informáticos, reduciendo los costes de desarrollo de aplicaciones informáticas o páginas web, al no tener que gestionar la instalación de sistemas operativos o preocuparse por el mantenimiento y actualización del mismo.

C) **SaaS:** software como servicio o SaaS (*Software as a Service)* es el servicio mediante el cual el software es administrado en la nube por un tercero para un cliente final, como por ejemplo Office365.

### 4.3. Riesgos y beneficios

El principal beneficio radica en que se este tipo de tecnología permite emplear hardware o software sin tener que incurrir en grandes inversiones para ello, configurando un importe ahorro en costes para empresas no tecnológicas.

Sin embargo, la computación en la nube tiene una serie de riesgos derivados de su propia naturaleza que se deben tener en cuenta desde el punto de vista del cumplimiento normativo:

A) **Accesos no autorizados:** El tratamiento de datos personales desde fuera de las oficinas conlleva aumentar la probabilidad de que se produzcan accesos no autorizados por terceros, lo que podría llegar a provocar una brecha de seguridad, en atención a la base de datos que pueda ser vulnerada.

B) **Tratamiento de datos en países que no aportan un nivel adecuado de protección al tratamiento de los datos:** el empleo de nubes públicas puede dificultar conocer con exactitud en qué país se alojan los datos. Por tanto, se pueden estar llevando a cabo transferencias internacionales de datos a países que no cuentan con un nivel adecuado desde el punto de vista de la protección de datos.

C) **Aislamiento de datos:** El almacenamiento de datos en la nube pública hace que se comparta la infraestructura con otros clientes, por lo que una ineficiente arquitectura de red puede llevar a accesos no autorizados de datos.

D) **Pérdida de los datos:** Al procesar o almacenar los datos en la infraestructura de terceros dependemos de ellos y de sus medidas para evitar la pérdida de datos personales. Los proveedores de servicio deben tener una política de recuperación de datos en caso de desastre. Asimismo, es muy recomendable que

los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general. Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar.

### 4.4. Medidas preventivas y controles

Algunas de las medidas preventivas y controles que se pueden implementar para reducir los riesgos asociados al uso de servicios Cloud son:

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES |
|---|---|---|
| Accesos no autorizados | Formación a administradores y usuarios del sistema | Revisión y mejora acciones de formación llevadas a cabo |
| | Gestión adecuada de derechos de acceso lógico | Revisión directorio activo |
| | Diseño de arquitectura de red segura que incluya segmentación de entornos Cloud | Pruebas de penetración |
| Transferencias internacionales a países no adecuados | Auditoría previa a encargados de tratamiento | Revisión resultados auditoría |
| | Introducir SLAs en contratos con terceros | Revisión KPIs asociados a los SLAs |
| Pérdida de los datos | Diseñar sistemas de alta disponibilidad y redundancia | Auditorías de seguridad |
| | Plan de Continuidad de Negocio | Pruebas de recuperación |

## 5. Big data aplicado al Compliance

### 5.1. Introducción/Definición/Origen

El Big Data es el conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que proporcione valor.

En la definición del Big Data, también se acepta comúnmente su caracterización a través de las denominadas “las 3 uves”: volumen, variedad y velocidad:

A) **Volumen:** es la característica más obvia y que recoge el propio nombre de Big Data. Se pasa de manejar magnitudes de megabytes, gigabytes, como mucho Terabytes, a manejar Petabytes de forma cada vez más frecuente.

B) **Variedad:** tanto por la tipología de datos como por sus fuentes. Se ha pasado de manejar datos estructurados en bases de datos procedentes, en su mayoría, de fuentes internas, a tratar datos estructurados, semiestructurados y desestructurados; de ser datos cuasi estáticos a datos dinámicos o en continuo cambio; de originarse en un número de fuentes limitadas a proceder

de personas, máquinas, sensores, etc. Esta variedad y volumen, requieren un tratamiento diferente para poder convertirse en información.

C) **Velocidad:** La captura, movimiento y proceso de los datos se hace a gran velocidad, llegando a ser en tiempo real en algunos casos.

Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos. No es una tecnología en sí misma, sino más bien un planteamiento de trabajo para la obtención de valor y de beneficios como consecuencia del tratamiento de los grandes volúmenes de datos que se están generando día a día.

El Big Data no hay que entenderlo únicamente como el almacenamiento y procesamiento de muchos datos que se transmiten a gran velocidad. Juega un papel muy importante la analítica descriptiva y sobre todo la predictiva. Es decir, convertir esos datos en bruto en información que tenga una aplicación.

El objetivo del Big Data es aportar y descubrir un conocimiento oculto a partir de grandes volúmenes de datos. No es relevante el volumen de datos o su naturaleza. Lo importante es su valor potencial que solo las tecnologías especializadas pueden explotar.

## 5.2. Aplicaciones prácticas

La gran mayoría de proyectos Big Data se pueden clasificar según sus objetivos en:

- **Mejor conocimiento del cliente:** la información permite ofrecer un mejor servicio y atención al cliente.
- **Mejor conocimiento del mercado para la captación de nuevos clientes.**
- **Personalización de productos y servicios:** la información permite personalizar el servicio ofreciendo una mejor experiencia de cliente, incrementando la fidelización y satisfacción.
- **Mejora y rapidez en la toma de decisiones:** la información permite a las organizaciones públicas y

privadas tomar mejores decisiones, optimizando la gestión de procesos y, por tanto, reduciendo costes aumentando la competitividad.

- **Previsión del comportamiento:** un análisis adecuado permite obtener una mejor visión de qué puede pasar, ampliar la visión estratégica y de negocio, crear nuevos servicios y productos, y obtener nuevos ingresos.
- **Monetización:** la propia información puede ser monetizada, por ejemplo, a través de una mejor publicidad o compartiendo estos datos con otras compañías (eso sí, asegurando el cumplimiento del marco legal).
- **Riesgos:** La disponibilidad y el almacenamiento de datos, la potencia de procesamiento y las técnicas de modelado predictivo han aumentado las capacidades de cuantificación del riesgo de negocio y de Compliance.

## 5.3. Riesgos y beneficio

### 5.3.1. Riesgos

A) **La discriminación predictiva:** el análisis predictivo puede ser utilizado para tomar decisiones sobre la adecuación de un usuario para, por ejemplo, acceder a un determinado trabajo, un préstamo o una tarjeta de crédito. Es decir, para tomar decisiones por asociación que afecten negativamente a las personas.

   El riesgo no está en los datos en sí, sino en la interpretación y/o asociación que pueden llegar a hacer las empresas, y en la toma de decisiones automática o basada en criterios poco lícitos. ¿Pueden llegar a discriminarse usuarios por una predicción hecha por un algoritmo? En este sentido, las empresas tendrán que llevar a cabo un esfuerzo para evitar despersonalizar las decisiones, y equilibrar el análisis predictivo con la atención personalizada.

B) **La pérdida de anonimato:** cada vez es más difícil, para el usuario común, llevar a cabo una acción online sin asociarla a su identidad. Necesitamos identificarnos para prácticamente cualquier cosa. De hecho, cada vez es más difícil para las empresas anonimizar los datos de forma que no se pueda re-identificar a las personas, ya que generamos una ingente cantidad de información que se pueden cruzar y conectar.

   La clave para las empresas será la implementación de sistemas de seguridad que garanticen la privacidad y seguridad de los datos, y la capacidad para generar confianza en los usuarios. Por parte de los usuarios, cada vez se educa más en limitar la cantidad de información personal que se vuelcan en la red.

C) **El negocio de los datos:** el Big Data ha generado nuevos modelos de negocio, algunos de ética discutible, como el negocio de la compraventa de datos. Cada vez más empresas venden datos segmentados enlazados al perfil del usuario, con lo que la empresa compradora puede ofrecer productos altamente personalizados. Así, un embarazo, las tendencias sexuales de la persona o una enfermedad pueden quedar revelados por la publicidad a la que someten a la persona, aunque esta no lo desee y dejándole poco margen para la privacidad.

Aunque hay grandes empresas que intentan implementar políticas publicitarias que frenen estas prácticas, el hecho es que cada vez estamos más expuestos, tanto como lo están nuestros datos.

D) **Los ciberataques:** aunque, no es el único riesgo, lo cierto es que sigue estando entre los primeros puestos de la lista. La cada vez mayor interconectividad y tráfico de datos hace que incremente también el riesgo de un robo, pérdida, suplantación de identidad

### 5.3.2. Beneficios

- Análisis de grandes volúmenes de datos a una velocidad inimaginable.
- Herramienta eficaz y útil para realizar predicciones.
- Su valor en sectores clave como en el sanitario, donde existen ya muchos ejemplos de su eficacia para reducir el tiempo de ingreso hospitalario o predecir futuras enfermedades y riesgos sanitarios.
- Su utilización en las Smart Cities como herramienta para prevenir, por ejemplo, colapsos de tráfico y excesos de contaminación.
- En el sector de la distribución permite anticiparse al consumidor evitando situaciones de desabastecimiento de productos y falta de suministro. La identidad digital hace visibles a billones de personas que permanecían en el anonimato y las hace menos vulnerables a abusos y explotación.
- Motor económico y de desarrollo con un potencial del que solo hemos explorado una parte.

## 5.4. Medidas Preventivas, Organizativas y Seguridad.

A continuación, se deberán desarrollar una serie de políticas preventivas controles por el Delegado de Protección de Datos (DPO) que contemplen los siguientes riesgos más relevantes derivados de las técnicas Big Data (según Análisis de Riesgos y Evaluación de Impacto realizados).

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES |
|---|---|---|
| La discriminación predictiva | Transparencia en la información y consentimiento | • Muestreo: verificar a través de un muestreo que se está informando y que existe base de legitimación para el tratamiento.<br>• Cuestionarios cumplimiento. |
| | Cumplimiento de principios de tratamiento y conservación | • Muestreo: verificar que se está cumpliendo con los principios.<br>• Cuestionarios de cumplimiento. |
| | Hacer efectivos los derechos de los interesados | • Verificar si los datos están organizados de manera que se pueden hacer efectivos los derechos de los interesados.<br>• Verificar si se ha informado al interesado.<br>• Verificar si se contestan los derechos en plazo. |
| | Decisiones individuales automatizadas: uso de técnicas de anonimización. | Auditorías de seguridad: verificar que no es posible la reidentificación. |
| | Adopción de medidas técnicas. | Auditoría de Seguridad. |
| | Formación y Concienciación. | Registros de Formación |
| La pérdida del anonimato | Uso de técnicas de anonimización. | Auditorías de seguridad: verificar que no es posible la reidentificación. |
| | Adopción de medidas técnicas: implementar sistemas de seguridad que garanticen la privacidad y seguridad de los datos. | Auditorías de seguridad. |
| | Formación y concienciación. | Registros de Formación. |
| El negocio de los datos | Transparencia en la información y consentimiento explícito. | • Muestreo: verificar a través de un muestreo que se está informando y que existe base de legitimación para el tratamiento.<br>• Cuestionarios cumplimiento |
| | Cumplimiento de principios de tratamiento y conservación. | • Muestreo: verificar que se está cumpliendo con los principios.<br>• Cuestionarios de cumplimiento. |
| Ciberataques | Medidas Técnicas | Auditoría de Seguridad |

# 6. Deep learning y machine learning

## 6.1. Introducción/Definición/Origen

Machine Learning o Aprendizaje Automático es una técnica de Inteligencia Artificial que desarrolla computadoras con la habilidad de aprender de los datos sin ser programadas explícitamente para ello. Son algoritmos capaces de crear soluciones aprendiendo de ejemplos sin necesidad de recibir instrucciones del ser humano.

Se empezó a hablar de Inteligencia Artificial por primera vez en 1956 en la Conferencia de Dartmouth. Las primeras investigaciones de Inteligencia Artificial trabajaron en programas para la resolución general de problemas. En los años 60, se comenzó a entrenar ordenadores para imitar el razonamiento humano básico de manera que pudieran aprender de los datos, por ejemplo, el reconocimiento de imágenes, dando lugar al nacimiento del Machine Learning. En las décadas posteriores, con la creación de internet, la utilización de cantidades masivas de datos y la mejora de la capacidad de procesamiento de los ordenadores se dio un paso más, consiguiendo que las máquinas además de aprender de la experiencia, se entrenaran a sí mismas mediante redes neuronales artificiales de algoritmos. Estos están interconectados en diferentes capas simulando el funcionamiento de las neuronas en el cerebro humano, es lo que se conoce como Deep Learning.

Machine Learning son técnicas de aprendizaje que permiten a un sistema de Inteligencia Artificial aprender a resolver problemas que no se pueden especificar de manera precisa o cuyo método de resolución no se pueda describir mediante reglas de razonamiento simbólicas. Generalmente se refiere a la Inteligencia Artificial centrada en desarrollar sistemas predictivos que aprenden de los datos. Son algoritmos que identifican patrones en los datos disponibles y aplican el conocimiento adquirido a nuevos datos. Utiliza la comparación de patrones estadísticos para estudiar los datos e inferir reglas generales para las aplicaciones.

Existen varios tipos de Machine Learning, siendo los más extendidos:

- **El Aprendizaje Automático supervisado:** Los algoritmos trabajan con datos etiquetados. Se facilitan al sistema ejemplos variados y representativos de la mayoría de las situaciones, de manera que el algoritmo es capaz de generalizar y saber interpretar los datos de entrada, asignarles una etiqueta de salida y comportarse adecuadamente en situaciones no descritas en esos ejemplos, es decir, aprende de los datos y predice el valor de salida.
- **El Aprendizaje Automático no supervisado:** no existe información de clasificación ni de evento. El algoritmo parte de datos no etiquetados, extrae la información significativa, sin variables de salida conocidas mediante la exploración de la estructura de dichos datos.
- **El Aprendizaje por refuerzo:** se deja libertad al sistema de Inteligencia Artificial para tomar sus decisiones a lo largo del tiempo, y cada vez que adopta una decisión se le proporciona una señal de recompensa que informa al sistema si la decisión fue acertada o no. El sistema aprende en base prueba-error. Se utiliza en sistemas de formulación de recomendaciones en el mundo del marketing (por ejemplo sugerir en internet a los usuarios productos), video juegos y juegos de mesa.
- **El Aprendizaje Automático profundo o Deep Learning:** adopta algoritmos basados en el concepto de redes neuronales, en el sentido de que cuenta con una red de unidades de procesamiento de pequeño tamaño con numerosas conexiones ponderadas entre ellas. La red neuronal cuenta con varias capas entre la entrada y salida, que le permiten aprender la relación general entre ellas en pasos sucesivos. Es más preciso y requiere un menor grado de orientación humana.

El Deep Learning ha supuesto un punto de inflexión pues ha transformado la forma en que los algoritmos logran un rendimiento al nivel del de los seres humanos y, en algunos casos, con una precisión superior en tareas como el reconocimiento de imágenes o de la voz o la traducción automática. Requiere una mayor cantidad de datos y capacidad de los ordenadores.

## 6.2. Aplicaciones prácticas

Machine Learning y Deep Learning se vuelven extremadamente útiles al combinarlas con el juicio humano. Sus posibles aplicaciones en los sistemas de gestión de Compliance son las siguientes:

- **Gestión de riesgos mediante la automatización de procesos** reduciendo las posibilidades de error y aportando una mayor objetividad. Por ejemplo, en los procesos de selección; en los servicios financieros, para evaluar la

solvencia y reducir los costes de servicio al cliente, en particular, para la suscripción de préstamos en la banca minorista; en la prevención del blanqueo de capitales, para analizar información de diferentes fuentes y generar informes de manera automática.

- **El diseño de controles para prevenir y detectar los comportamientos fraudulentos**, analizando datos masivos que detectan actividades sospechosas.
- **Revisión de documentos automáticamente:** con el Machine Learning no supervisado, se procesan gran cantidad de contratos, se identifican y categorizan cláusulas repetidas. De aplicación en el sector financiero con cierto tipo de contratos crediticios por su escasa variabilidad y el volumen de contratos.
- **Prevención y detección del fraude:** estas tecnologías permiten identificar patrones de actividades fraudulentas y detectar incumplimientos.
- **Ciberseguridad:** automatización de la detección y la respuesta a las amenazas, cada vez más en tiempo real.
- **Formación:** permite diseñar planes de formación personalizados.

### 6.3. Riesgos y beneficios

Los beneficios de utilizar Machine Learning y Deep Learning en los sistemas de gestión de Compliance son los siguientes:

- **Facilitan un sistema de gestión de Compliance más eficiente,** a través de herramientas que minimizan el riesgo a la vez que facilitan procesos y optimizan resultados, reduciendo la posibilidad de errores y mejorando su rendimiento con una mejor gestión del tiempo y ahorro de costes.
- **Los procesos automatizados mediante estas técnicas facilitan el cumplimiento de la normativa aplicable, así como de los valores y principios éticos de la organización.** Ayudan a prestar mejores servicios y crear productos seguros y fiables en diferentes sectores.

- Mejora la forma de tomar decisiones de la organización.
- Reduce los riesgos de brechas de seguridad de la información.
- **Impulsa la cultura de cumplimiento** alineada con los valores de la organización a través de la formación impartida con estas técnicas más amenas, accesibles y amigables (por ejemplo video juegos).

A pesar del potencial de estas tecnologías, debemos tener presente los posibles riesgos asociados a su utilización:

- **Incumplimiento de la normativa de protección de datos y privacidad:** Los algoritmos de Machine Learning y Deep Learning requieren una gran cantidad de datos para mejorar su capacidad de predicción. Cuando se trate de datos personales se debe velar por el cumplimiento de la normativa de protección de datos y privacidad teniendo en cuenta las diferentes legislaciones de los países en los que se opere.
- **Prejuicio y discriminación:** la mayoría de los algoritmos actuales se entrenan a través de un "aprendizaje supervisado", que requiere que los humanos etiqueten y categoricen los datos subyacentes. Se pueden introducir sesgos no intencionales en los datos de entrenamiento que generen resultados discriminatorios o injustos. Los modelos se deben entrenar y analizar sus resultados para erradicar los posibles sesgos antes de su implantación y posteriormente, en su revisión.
- **Puede producir efectos adversos debido a asimetrías de poder** o de información entre la organización y sus trabajadores o entre consumidores y plataformas de proveedores y vendedores.
- **Opacidad del algoritmo:** podría impedir la transparencia respecto a cómo se tomó una decisión errónea o inadecuada adoptada por los modelos de Machine Learning y Deep Learning y las personas que los manejan impidiendo a los afectados su impugnación. Esto puede suceder con los algoritmos de "caja negra" en los que no se puede explicar por qué se ha generado ese resultado ni los factores que contribuyeron a ello. Sin esta información no se puede impugnar adecuadamente la decisión. Los modelos deben ser transparentes, disponer de explicaciones sobre la medida en que estas técnicas condicionan e influyen en la toma de decisiones y utilizar técnicas de explicabilidad para garantizar la comprensión de las decisiones, el cumplimiento de la normativa, el respeto de los derechos de los afectados y su alineación con los valores de la organización.
- **Falta de fiabilidad de los algoritmos:** si no son entrenados lo suficiente o no son ajustados, revisados y mejorados periódicamente pueden llevar a decisiones erróneas con el consiguiente daño para los afectados y la reputación de la organización.

- **Riesgos de seguridad:** pueden sufrir ataques malintencionados que afecten a los datos y al comportamiento de los modelos de Machine Learning y Deep Learning de manera que adopten decisiones erróneas. Las organizaciones deberán adoptar medidas de seguridad de forma proactiva.
- **Falta de precisión de los modelos** para adoptar decisiones correctas si las organizaciones no protegen la calidad, la forma y la cantidad de los datos que se procesen para evitar que sean excesivos o insuficientes.

### 6.4. Medidas preventivas y controles

Las organizaciones se enfrentan al desafío de utilizar esta tecnología de forma efectiva y responsable. Una cultura ética en la organización resulta esencial para garantizar que los modelos de Machine Learning y Deep Learning no provoquen daños involuntarios o efectos adversos y comprometan el enorme potencial de estas tecnologías. Para asegurar la aplicación responsable, las organizaciones deberán:

- A la hora de diseñar los modelos de Machine Learning y Deep Learning, tener en cuenta las normas de cumplimiento y establecer políticas claras que definan los valores y puntos de referencia para desarrollar y utilizar estas tecnologías de manera responsable.
- Velar por que los algoritmos estén alineados con los valores, directrices y normas de cumplimiento de la organización revisando los modelos y realizando auditorías.
- Comprobar que los datos utilizados en los entrenamientos de los algoritmos sean fiables y no se introduzcan sesgos en los algoritmos para que sean justos.
- Facilitar la acción y supervisión humana para poder juzgar y en su caso descartar una decisión.
- Diseñar algoritmos transparentes, explicables y auditables.

- Fomentar equipos diversos, interdisciplinares, involucrando a la dirección al más alto nivel, capaces de utilizar el poder analítico de esta tecnología, potenciando la transformación continua, y la agilidad del aprendizaje.

# 7. Chatbot aplicados al Compliance

## 7.1. Introducción/Definición/Origen

El origen del chatbot se remonta a 1950, cuando el científico Alan Turing empezó a estudiar si los ordenadores podían mantener una conversación con humanos, esto es, conversaciones máquina-humano.

Antes de los chatbots existieron los bots. Los bots son softwares creados para automatizar procesos que se ejecutan sin la necesidad de una intervención humana, como por ejemplo reservar una habitación en un hotel o un restaurante.

Un chatbot es un bot especializado y creado para mantener conversaciones y ofrecer respuestas preconcebidas. es un software de inteligencia artificial.

Los chatbot  son programas informáticos diseñados para simular conversaciones con personas a través del teclado (chat) o mediante reconocimiento de voz.

Podemos diferenciar dos tipos de chatbots:

- Dumb chatbot: de funcionamiento sencillo, que consiste en asociar respuestas a preguntas predeterminadas, esto supone que solo puede responder palabras o frases que tenga previamente registradas.
- Smart Chatbots: funcionan con sistemas de inteligencia artificial, es un sistema que aprende de su propio funcionamiento para mejorar las respuestas, lo que permite conversaciones mucho más fluidas simulando el comportamiento humano.

Los chatbots surgieron en los años 60 con “Eliza”, el primer chatbot desarrollado por Josep Weizenbaum en el Instituto de Tecnología de Massachusetts en 1966, cuyo objetivo era mantener una conversación muy sencilla en inglés con un usuario sobre cualquier tema. Para ello, su programación se basaba en la identificación de palabras claves para entender los textos y respondía con frases predefinidas que estaban asignadas a las palabras identificadas, hasta la reciente aparición de Watson (IBM, 2006), Siri (Apple 2010), Google Now (2012) o Alexa (Amazon, 2014), estando todos ellos sometidos a una evolución permanente en la actualidad.

## 7.2. Aplicaciones prácticas

El chatbot se puede desplegar en diversos canales, como web, WhatsApp, Facebook, u otros entornos, implicando distinto tiempo de desarrollo, tecnología, y coste.

### 7.2.1. Atención al cliente

Llevamos años siendo testigos del auge de los chatbots en atención al cliente. Se ha pasado de los asistentes virtuales basados en repositorios de preguntas frecuentes (FAQs) hasta ver un mismo chatbot ofreciendo varios procesos transaccionales distintos. Esto significa que, a día de hoy, los chatbots no sólo brindan contenidos informativos y no sólo son capaces de redireccionar al usuario hacia la sección de la web o de la app donde pueda efectivamente llevar a cabo su operación. Pueden hacer mucho más.

Los chatbots de ahora saben recibir información del usuario, siempre que haya accedido a su área privada, desde el CRM. Esta capacidad permite personalizar la atención al usuario, por ejemplo, llamándolo por su nombre, haciendo referencia a los productos que tiene contratados o bien retomando una incidencia que haya abierto previamente. También saben recolectar información empleada durante la conversación o bien solicitarla proactivamente en caso de que sea necesaria.

Gracias a la gestión de estas variables o parámetros, la conversación está siempre contextualizada y al mismo tiempo hace posible disponer de estadísticas filtradas por cualquiera de las variables utilizadas. El usuario no tiene que repetir informaciones ya comunicadas o implícitas, se siente atendido de forma personalizada y la conversación resulta rápida y eficiente. Las variables sirven de base para que el chatbot pase de ser un mero canal de comunicación explicativa a convertirse en una aplicación transaccional integrada.

En la actualidad los casos de uso que incluyen procesos transaccionales son tan diversificados como las necesidades de las empresas: reserva de sala de reunión, localización del cajero más cercano, recuperación de contraseña, seguimiento de pedidos, consulta de saldo, estado de un vuelo, duplicado de factura, etc. Todos tienen en común haber simplificado el acceso a operativas que hasta entonces sólo se podían gestionar desde el Contact Center y mediante un agente humano.

### 7.2.2. Compliance

Un chatbot puede ayudar a las empresas a fomentar una cultura de compliance entre los empleados. De esta manera, el Compliance Officer se puede dedicar a otras tareas y la compañía tendría una evidencia que muestra su diligencia en el cumplimiento normativo.

Se podría configurar un chatbot con preguntas y respuestas (FAQ) relativas a compliance (como por ejemplo, dudas acerca de conflicto de interés). Así, la respuesta sería inmediata y disponible a cualquier hora. Además se puede responder a varios empleados a la vez.

El chatbot también podría servir como canal de denuncias (whistleblowing) adicional a otros, como un proveedor específico, el correo electrónico o postal o el teléfono.

Mediante el chatbot también se podrían hacer encuestas acerca del grado de conocimiento relativo a compliance de los empleados. Convendría que el/la Compliance Officer monitorice las conversaciones para analizar el grado de conocimiento y también para ajustar las respuestas.

Otra función del chatbot podría ser el avisar o recordar a los empleados alguna tarea, algún plazo que tengan que cumplir o un próximo evento (como una formación).

El chatbot también podría guiar al empleado en una formación.

## 7.3. Riesgos y beneficios

El principal riesgo del chatbot es garantizar la privacidad de los datos de los clientes y la seguridad. Respecto a la privacidad, lo primero que debemos plantear es la finalidad del chatbot y la determinación de la base legitimadora de los datos (consentimiento, cumplimiento de una relación contractual, interés legítimo,...) y cumplir con el deber de informar el tratamiento de los datos informando sobre responsable, finalidad y posibilidad de ejercer los derechos.

También dentro de la responsabilidad proactiva, debemos analizar la privacidad desde el diseño, definiendo todos los requisitos necesarios para mitigar los riesgos de privacidad. Así, por ejemplo, debemos evaluar si el chatbot requiere profiling, tratamientos de datos a gran escala, uso de bases de datos externas, uso de tecnologías innovadoras en cuyo caso debemos realizar un análisis de impacto de privacidad (PIA).

Además, el enlace entre el chatbot y las aplicaciones internas de la compañía tiene que ser realizado de conformidad con las políticas de seguridad y evitando que un fallo en una transacción pueda afectar el funcionamiento del chatbot en general.

En cuanto a seguridad, también cabe destacar que el chatbot no debe manipular ninguna información sensible, sólo la remite y/o la enseña en la interfaz.

Hay diversas técnicas para mitigar el riesgo de falta de seguridad, como distintas capas de seguridad adicional o un enmascarador de variables y de logs.

Dependiendo de la configuración, puede ser necesario incluir una política de privacidad y/o una política de cookies. Asimismo, si se presta un servicio mediante el chatbot, hay que facilitar los términos y condiciones de uso.

Riesgo es dotar al chatbot de la suficiente inteligencia para poder interpretar toda la variedad de preguntas sobre un tema y el entrenamiento del modelo para poder responder de la forma adecuada. En este sentido, los chatbots son programas informáticos y por tanto sujetos a la regulación de propiedad intelectual. Normalmente para la creación de chatbot se utilizan códigos abiertos para entendimiento del lenguaje o para entrenar los modelos. Es necesario analizar correctamente la forma de construcción de los programas para determinar riesgos de propiedad intelectual.

Otro posible riesgo es la posibilidad de afectar al derecho al honor, a la intimidad y la propia imagen por el uso de inteligencia artificial que impacten en los derechos personalísimos de los usuarios si el programa utiliza expresiones racistas, ofensivas o injuriosas.

En cuanto a los beneficios del chatbot, mejora la experiencia de los usuarios, que tienen a disposición una aplicación sencilla, conversacional y personalizada, que puede integrarse además en sus canales favoritos (Whatsapp, messenger, web, etc). Se benefician de un buen nivel de servicio y de calidad. Por otro lado, las empresas sacan mayor provecho de sus procesos ya digitalizados a la par que alivian a sus departamentos de atención al cliente de las operativas más frecuentes y repetitivas. Asimismo, las empresas pueden obtener bases de datos cualificadas enriquecidas con el análisis de la psicografía de sus usuarios/as, abriendo la puerta del big data como herramienta de marketing. Se puede segmentar a los usuarios.

## 7.4. Medidas preventivas y controles

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES |
|---|---|---|
| Garantizar privacidad | Privacidad desde el diseño | Comprobación de la implementación correcta de los requisitos de privacidad: cláusula informativa, confidencialidad, controles de acceso a datos, asegurar las finalidades de los datos... |
| | Política de minimización de datos | Definir los datos personales imprescindibles para la finalidad |
| | política de privacidad y cookies | definir la política de privacidad y cookies cuando sea necesario |
| Seguridad | Política de seguridad | Revisión de medidas de integridad y confidencialidad aplicadas |
| | Definición de requisitos de seguridad de las infraestructuras y entornos de desarrollo | Pruebas Pentest para garantizar la seguridad de los programas<br><br>Comprobación de cifrado de datos cuando sea necesario |
| | Definición de medidas organizativas de aplicación | Control de aplicación de las medidas necesarias: control de acceso segmentado, planes de recuperación de datos, otras medidas. |
| Pérdida de los datos | Medidas para asegurar la protección de datos | Auditorías de seguridad |
| | Plan de Continuidad de Negocio | Pruebas de recuperación de actividades críticas |
| Propiedad intelectual | Definir reglas de uso de códigos abiertos y APIS | Auditorías informáticas para comprobar uso de códigos abiertos de acuerdo a los procedimientos definidos |
| Lesión de derechos fundamentales | Definición de respuestas posibles por equipos multidisciplinares: informáticos, negocio, legal... | Control humano en el diseño del sistema y seguimiento de su funcionamiento<br><br>Supervisión de modelos<br><br>Auditorías independientes para comprobar que no impactan en derechos fundamentales |

# 8. Robótica aplicada al compliance

## 8.1. Introducción

El término “robot” fue acuñado por primera vez por el escritor de origen checo Karel Čapek en su primera obra teatral titulada ‘R.U.R.’ (*Robots Universales Rossum)* publicada en el año 1920[1]. La pieza plantea una sociedad distópica en la que los robots, configurados inicialmente como una ayuda para las personas, terminan por destruir a los seres humanos y tomando el control del mundo. Afortunadamente, la quimera planteada por Čapek se circunscribe a su obra y hoy en día la robótica goza de una mejor prensa en círculos jurídicos y empresariales.

También resulta interesante, destacar la publicación del relato titulado “Círculo Vicioso” por Isaac Asimov en 1942 donde enunció las tres leyes de la robótica[2]. Asimov se preguntaba qué podría pasar si los robots se rebelaran contra los humanos, por eso formuló una serie de normas éticas para controlar su comportamiento. Estas tres leyes pretender limitar las actuaciones de los robots: solo pueden actuar bajo las órdenes de humanos y en ningún caso pueden atacar o hacer daño a las personas.

En términos académicos, el Diccionario de la Real Academia Española (DRAE) define a un robot como una “máquina o ingenio programable que es capaz de manipular objetos y realizar diversas operaciones”.

## 8.2. Regulación y marco normativo de aplicación

En el mundo del derecho es sabido que la ley suele ir por detrás de la realidad. Los continuos avances tecnológicos, entre los que se incluye la robótica, han acreditado la lentitud del legislador a la hora de diseñar un marco regulatorio acorde a una realidad en la que los robots y la inteligencia artificial ya no pertenecen al mundo de la ciencia ficción. Aunque por ahora no existe una normativa específica que regule la utilización y desarrollo de los robots, sí contamos con algunas bases con marchamo europeo que sirven para definir los contornos jurídicos en los que se ubica actualmente la robótica.

En primer lugar, cabe apuntar al marco de responsabilidad y seguridad para la inteligencia artificial, el internet de las cosas y la robótica establecido en la Directiva de Máquinas 2006/42/CE/ y en la Directiva 85/374/CEE sobre productos defectuosos. El Parlamento Europeo ya ha puesto de manifiesto que dicho marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento.

Por otro lado, la tendencia hacia la automatización requiere que los implicados en el desarrollo y comercialización de aplicaciones de inteligencia artificial incorporen desde el principio características de seguridad y ética. A este respecto, en el año 2016 el Comité de Asuntos Jurídicos del Parlamento Europeo encargó la elaboración de un estudio que fue publicado bajo el título "European Civil Law Rules in Robotics[1]". Este documento tiene la finalidad de evaluar y analizar, desde una perspectiva legal y ética, la industria robótica y establecer nuevas reglas de derecho civil europeo.

Más recientemente, en fecha 16 de febrero de 2017, el Parlamento Europeo emitió junto con el estudio anterior una serie de recomendaciones en materia de regulación sobre los derechos civiles de los robots que dirige a la Comisión Europea[2]. Las citadas recomendaciones no deben entenderse como un borrador de iniciativa legislativa, sino que son unas meras indicaciones para instar a la Comisión Europea al desarrollo de nueva legislación europea para regular estas cuestiones. Asimismo, en estas recomendaciones el Parlamento Europeo solicita a la Comisión Europea que presente una propuesta de Directiva relativa a las normas de legislación civil en materia de robótica en línea con las recomendaciones propuestas.

Más recientemente, en el año 2018, más de 200 expertos de varios Estados Miembros remitieron una carta abierta a la Comisión Europea titulada "Robotics, Open Letter[3]" en la que recomendaban el desarrollo de la industria de la inteligencia artificial y la robótica en aras de limitar los riesgos que puedan producir sobre los seres humanos.

Tras esta petición de la comunidad científica, en el mes de abril del año 2019 el Grupo de Expertos de alto nivel sobre Inteligencia Artificial de la Comisión Europea publicó unas directrices éticas para el desarrollo de la inteligencia artificial (EU Guidelines on Ethics in Artificial Intelligence: Context and implementation[4] centrándose principalmente en recomendaciones enfocadas al desarrollo de la innovación

1. Acceso al documento completo en ingés: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf
2. Acceso al documento completo: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf
3. Acceso al texto completo en inglés: http://www.robotics-openletter.eu/
4. Acceso al texto completo en inglés: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf

partiendo desde una robustez técnica aplicando criterios éticos y alentando a una competitividad responsable en este sentido.

En conclusión, parece evidente que, aunque todavía no se dispone de un marco normativo específico aplicable a la regulación y funcionamiento de los robots, sí contamos con una serie de recomendaciones y directrices publicadas por los organismos europeos y otras normas generales que deben ser de aplicación como es el Reglamento General de Protección de Datos (RGPD).

Desde el punto de vista técnico, la Asociación Española de Normalización (ISO por sus siglas en inglés) publicó la ISO 13482 sobre requisitos de seguridad para robots no industriales y la ISO 10218 (dividida en dos partes ISO 10218-1 y 10218-2) relativa a la seguridad de robots industriales.

No obstante, está previsto que ésta última sea revisada por el grupo de trabajo correspondiente (WG 3 “Industrial safety”) del Comité ISO encargado de la normalización de robots siendo el mes de mayo de 2021 el plazo límite para la publicación de una nueva versión.

## 8.3. Aplicaciones prácticas

### 8.3.1. RPA y programas de cumplimiento normativo

La automatización de procesos mediante robots (*Robotic Process Automation o RPA por sus siglas en inglés)* es toda tecnología enfocada a disminuir la intervención humana en ciertas actividades repetitivas o automáticas que varían poco en cada iteración.

La RPA presenta grandes ventajas, tanto desde un aumento de la productividad como de la escalabilidad en la utilización de recursos o en la implementación de programas de cumplimiento normativo. Con ello, se aumenta la capacidad de trabajo de un sistema sin comprometer el funcionamiento y calidad de este.

En el seno de la implementación de programas de cumplimiento normativo, los robots de software pueden utilizarse en distintas fases o para distintas tareas como pueden ser las siguientes:

- **Identificación de clientes para evitar el fraude y blanqueo de capitales:** entre las más populares se encuentran los softwares denominados como *Know Your Customer (KYC) o Customer Due Diligence (CDD).*
- **Evaluación de riesgos penales:** se realiza el mapa de riesgos penales contestando a una serie de cuestiones que arrojan los resultados de dicha evaluación.
- **Gestión de riesgos y políticas internas de cumplimiento:** permite establecer un control exhaustivo de las reglas a seguir, una reducción del contacto humano con datos de carácter sensible y, en último término, una disminución de las probabilidades de que tenga lugar un fraude o una actitud negligente.
- **Digitalización del canal de denuncias:** se recomienda utilizar canales de denuncias digitalizados y externalizados. Tal y como indicó la Fiscalía General del Estado en su Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas, esta fórmula ofrece una mayor garantía de confidencialidad y aporta más confianza a los trabajadores que teman posibles represalias.
- **Cumplimiento del registro de la jornada horaria:** monitorización y seguimiento del horario laboral de los trabajadores y posibilidad de elaboración de informes semanales con esta información. Asimismo, estos datos pueden ser útiles para la confección de horarios de trabajo y evitar que se solapen días de vacaciones u otras ausencias que perjudiquen el normal funcionamiento de la empresa.

De las anteriormente nombradas, quizás una de las herramientas más interesantes, sea el robot de software denominado como KYC ya utilizado en multitud de entidades financieras, que permite definir los controles y procedimientos de supervisión de forma automatizada para la validación de identidad de sus clientes, con el objetivo de evitar operaciones fraudulentas y delitos de blanqueo de capitales, financiación del terrorismo y otros negocios delictivos.

## 8.4. Riesgos y beneficios

### 8.4.1. Riesgos

El uso de aplicaciones robóticas de RPA conlleva una serie de riesgos:

- **Posibles brechas de seguridad de información confidencial y datos personales** si los sistemas de seguridad no están configurados siguiendo los estándares más altos y, en todo caso, asegurando la protección de la privacidad y la intimidad en las comunicaciones entre los seres humanos y los robots.
- **Vulnerabilidades derivadas del desarrollo de los sistemas en materia de seguridad** como falta de preparación de planes de continuidad de negocio,

implementación deficiente de la gestión de la identidad o en la gobernabilidad de los RPA.

- **Control de accesos y administración de los sistemas para evitar comportamientos no autorizados** llevados a cabo por los robots que pueden mitigarse monitoreando la actividad de los robots asignando esta responsabilidad a humanos, en aras de que las acciones sean restringidas gestionado los privilegios de acceso procurando que sean los mínimos indispensables.
- **Riesgos reputacionales, incumplimiento normativo y conductas contrarias al derecho de defensa de la competencia** cuando los algoritmos de aprendizaje automático recogen patrones o toman decisiones que podrían ser problemáticas desde el punto de vista ético, suponer una conducta contraria a las normas de competencia o derivar en el incumplimiento de otra normativa de aplicación.

### 8.4.2. Beneficios

Las principales ventajas que aportan las aplicaciones robóticas de RPA son las siguientes:

- **Ejecución de tareas de forma precisa y con un alto estándar de calidad** sin horarios ni limitación de tiempo, lo que ofrece máxima flexibilidad para adaptarse y cubrir el alto volumen de operaciones en situaciones concretas de aumento del trabajo o la producción.
- **Escalabilidad y estandarización de procesos automáticos** que hacen que los costes sean más reducidos y eficientes, mejorando la calidad y la precisión de las tareas automatizadas. Esto implica una redistribución de tareas que favorece que los humanos se centren en actividades que aportan valor añadido o en el desarrollo de nuevas competencias.
- **Minimización de riesgos ya que las actividades ejecutadas** por un robot pueden ser monitoreadas y grabadas, lo cual genera información útil que puede ser utilizada para la mejora de la eficiencia de procesos, así como para el cumplimiento de requerimientos de auditoría.

En relación con los beneficios que supone automatizar procesos en el curso de la implementación y desarrollo de los programas de cumplimiento, teniendo en cuenta que es fundamental el previo *input* humano para programar los sistemas de conformidad con la normativa vigente de aplicación, podrían destacarse los siguientes:

- Gestión de todas las áreas de cumplimiento desde un amplio espectro como objetivos corporativos, control de riesgos y evaluación continua de cumplimiento normativo.
- Facilita el seguimiento de acciones por incumplimiento.
- Acredita las gestiones y actuaciones realizadas puesto que se puede constatar la trazabilidad y mostrar evidencias.
- Detección automática de no cumplimientos.
- Generación de reportes automáticos y facilitación de procesos de auditoría y certificación interna.
- Aumenta la confianza de terceros puesto que se puede interpretar como una medida de transparencia.

## 8.5. Medidas preventivas y controles

<table>
<tr><th>RIESGOS</th><th>MEDIDAS PREVENTIVAS</th><th>CONTROLES</th></tr>
<tr><td>Brechas de seguridad de información confidencial y datos personales</td><td>Establecer protocolos de reporte de incidencias</td><td rowspan="3">Auditorías internas periódicamente para detectar posibles riesgos y deficiencias</td></tr>
<tr><td>Vulnerabilidades del desarrollo de los sistemas</td><td>Desarrollo desde la privacidad por defecto y por diseño</td></tr>
<tr><td>Control de accesos y administración de sistemas</td><td>Establecer controles de acceso a usuarios autorizados</td></tr>
<tr><td rowspan="2">Riesgos reputacionales, incumplimiento normativo y conductas contrarias al derecho de defensa de la competencia</td><td rowspan="2">Adaptar las políticas internas a la implementación de sistemas de RPA y procedimientos de automatización</td><td>Mantener un reporte actualizado de verificación de los criterios de cumplimiento normativo</td></tr>
<tr><td>Revisiones anuales de los algoritmos de automatización para comprobar que están alineados con los objetivos del negocio</td></tr>
</table>

# 9. Anonimización vs seudonimización

## 9.1. Introducción/Definición/Origen

La Anonimización o disociación de datos personales es aquel tratamiento que produce la ruptura total de los datos, de tal forma que no se pueda volver asociar al titular de estos, y por tanto sea imposible identificar a esa persona posteriormente.

La antigua Ley Orgánica de Protección de Datos de 15/1999, de 13 de diciembre, aunque no hacía referencia en su redacción a la palabra anonimización, se entiende, que la misma se reflejaba, en su artículo 3 apartado f), donde definía el Procedimiento de disociación como *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable."*

En el ámbito de la normativa europea de protección de datos, la Directiva 95/46/CE considera la anonimización como *"el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación".* En virtud de este, tratar los datos de tal manera que no puedan usarse para identificar a una persona física mediante *"el conjunto de los medios que puedan ser razonablemente utilizados"* por el responsable del tratamiento o por terceros.

Es en el año 2014 cuando el Grupo de Trabajo sobre protección de datos del Artículo 29 de la Comisión Europea, publicó el "Dictamen 05/2014 sobre Técnicas de la Anonimización."

En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».

En cuanto a la Seudonimización, podría definirse como aquel tratamiento que produce la modificación de los datos identificativos del interesado, pero sin suprimir la vinculación entre los datos que consigan identificar al titular de estos.

El RGPD en su artículo 4 apartado 5 define la seudonimización como “el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.”; y en su artículo 32, sobre la seguridad del tratamiento, incluye la seudonimización como una medida apropiada para garantizar el nivel de seguridad.

Es importante destacar, que el resultado de aplicar la anonimización o la seudonimización a un dato personal, arroja un resultado totalmente distinto. Un dato anonimizado es irreversible, no siendo posible la vinculación o identificación de la persona titular del dato. Por el contrario, un dato seudonimizado es reversible, dado que a tal efecto su limitación es transversal, pudiendo vincular a la persona titular del dato.

## 9.2. Aplicaciones prácticas.

En palabras sencillas, en el proceso de anonimización se eliminarán aquellos datos susceptibles de identificar directa o indirectamente a personas concretas, permaneciendo solo aquella tipología de datos que de ninguna manera podría asociarse con el titular de estos.

Por ejemplo, si una empresa recoge datos sobre los desplazamientos de personas, los patrones de viaje individuales a nivel de evento seguirán considerándose datos personales (*excluido monitorización de los desplazamientos de personas con COVID19/ Tratamiento de datos personales como consecuencia del COVID 19, Proximity tracing),* aun en el caso de que se hayan eliminado los identificadores directos del conjunto entregado a terceros. Por el contrario, si el responsable del tratamiento borra los datos no tratados y entrega únicamente estadísticas agregadas a terceros a un nivel general (por ejemplo, «los lunes, en el trayecto X, hay un 160 % más de pasajeros que los martes»), entonces estaríamos hablando de datos anónimos.

Por lo tanto, para conseguir referida finalidad (imposibilidad de asociar los datos que se han anonimizado con los datos identificativos de la persona afectada), es necesario la aplicación práctica de un proceso adecuado al contexto que se quiere anonimizar, la solución óptima requerirá la combinación de diversas técnicas, aunque no existen un catálogo de las mismas, deberán respetarse las recomendaciones prácticas que se formulan en el Dictamen (Anexo Manual de técnicas de anonimización).

En cuanto a la seudonimización lo fundamental es proteger la información adicional, ya que es esa información la que podría identificar al interesado. En la práctica,

está podría realizarse de diversas formas, entre ellas, mediante la sustitución de cifras y códigos de palabras, codificación de la información, códigos con clave de desencriptación, intercalado aleatorio por conjunto de datos, etc.

Un ejemplo concreto sería el envío de una muestra biológica -sangre- a un laboratorio para que realicen su análisis. En este supuesto, el laboratorio, solamente, tiene acceso a dichas muestras, en ningún caso podría acceder a los datos identificativos de la persona titular de las muestras.

En el Dictamen del Grupo del Artículo 29, existen diversas técnicas, las cuales son dinámicas y van evolucionando tecnológicamente, pero todas ellas cuentan con los siguientes extremos:

- <Singling out>: aislamiento de alguno de los datos personales del conjunto perteneciente a un individuo.
- < Linkability >: identificación por sistema grupal, no individual.
- < Inference >: identificación a partir de ciertas premisas que pueden concluir el dato personal identificativo.

Ejemplos aplicaciones prácticas:

| DISEÑO CRIPTOGRÁFICO | CAMBIOS DE IDENTIFICADOR | AÑADIR PREVIAMENTE VALORES <SAL> O VALOR CONSTANTE |
|---|---|---|
| Hash como técnica de seudonimización o anonimización | Algoritmo de cifrado | Disociación de identificadores |
| Microagreagación | Amnesia | Combinación subida de datos falsos |
| Cifrado por sustitución numérica | Combinación subida de datos falsos/ Permutación | Generalización y eliminación |

## 9.3. Riesgos y beneficios/ Medidas preventivas y Controles

Ambas técnicas implican riesgos, tales como, posibilidad de extraer registros que identifiquen personas, capacidad de vincular distintos registros que vinculen a un grupo de personas y posibilidad de deducir un valor de un atributo a partir de otro.

Sin embargo, cuando un conjunto de datos se anonimiza realmente y no es posible ya identificar a las personas, no existiría dato personal, y por ello se entiende que no estaría dentro de la Ley de Protección de datos, siendo el riesgo residual inherente de reidentificación menor que si el dato hubiera sido seudonimizado.

En definitiva, la irreversibilidad que ofrece la anonimización garantiza la información sin incumplir la normativa de protección de datos.

En la seudonimización, por el contrario, nunca se elimina toda la información, existiendo información adicional y personal que puede dar lugar a su identificación, por ello la probabilidad de que el seudoanonimato admita la identificabilidad es alta, siendo el riesgo residual inherente de reidentificación mayor dentro del ámbito de aplicación del régimen jurídico de protección de datos.

No obstante, cabe destacar que, en ambos supuestos, la falta de protocolo y falta de diligencia por parte de quien realiza el proceso de anonimización o seudonimización, generaría los mismos efectos, siendo un grado de riesgo muy elevado, con efectos legales, en los que sería irrelevante la intención del responsable del tratamiento o del destinatario, aplicándose la normativa sancionadora de protección de datos.

En relación con los beneficios, la existencia de unos «datos visibles» pueden aportar beneficios a la sociedad, empresas, personas y organizaciones, sólo si se respetan los derechos de protección privada, tales como aquellos utilizados en estadísticas, sanitarias, comerciales o de cualquier otra índole que no viole la protección de datos personales.

La innovación en el mundo tecnológico, no debe ser sinónimo de pérdida de confidencialidad. La implantación de las medidas preventivas y controles deben ir siempre encaminados a generar un equilibrio entre el interés legítimo del responsable y los derechos y libertades fundamentales de los interesados. El riesgo residual siempre va existir al aplicar una técnica de anonimización o seudonimización, por ello,  es necesario implementar controles y evaluar si son suficiente

Podemos destacar, varios riesgos, medidas de prevención, controles y beneficios que se producen como consecuencia de la aplicación de técnicas de anonimización o seudonimización, entre otros, los siguientes:

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES | BENEFICIOS |
|---|---|---|---|
| Pérdida de datos anonimizados o seudonimizados | Evaluaciones previas a la anonimización o seudonimización. Elección de la mejor técnica atendiendo a las características del dato a tratar | Revisión y análisis de las diferentes técnicas aplicadas transversalmente. | Portabilidad de datos. La anonimización o seudonimización, habilita la transacción de datos entre distintas soluciones informáticas y software |
| | Diseño de sistemas de alta protección | Auditorías de seguridad en los datos personales | Reducción del riesgo de fuga de datos personales |
| | | Protocolos y procedimientos de anonimización y seudonimización | |
| | Business continuity Plan | Plan de contingencia en la trazabilidad de los datos | Cloud hosting. Posibilidad de almacenar los datos en diversos lugares. |
| Reidentificación | Supervisión del tráfico entrante y saliente del firewall | Asegurar que el equipo de anonimización/seudonimización de una empresa no depende de alertas para identificar una actividad peligrosa. El equipo de anonimización debe comprender el sistema de anonimización y estar preparado para tomar las medidas necesarias en caso de que se produzca una brecha de seguridad tecnológica. | Desarrollo de los conocimientos de los empleados. Valor añadido para la Compañía. |
| | Actualización periódica de nuevas amenazas tecnologías | Realizar un seguimiento actual de las amenazas, estando siempre atento en la medida que se detectan o publiquen amenazas no deseadas, que pueden robar datos confidenciales y reidentificar los titulares personales. | Información estratégica para realizar estudios estadísticos, sin utilizar los datos personales, mediante la trazabilidad de estos. |
| Reutilización | Formación de empleados | Formar a los empleados de manera continua para que comprendan cualquier cambio en la política de uso aceptable de la empresa. | Ahorro de costes, minimizando los riesgos |
| | Fomentar la vigilancia entre empleados | "Vigilancia vecinal" de la seguridad. Si un empleado nota algo sospechoso, debe notificarlo a la persona adecuada de IT inmediatamente | |
| | Desarrollo de nuevas metodologías de anonimización / seudonimización | Soluciones de seguridad adicionales que protejan aún más la red y amplié las capacidades de protección en una empresa. Reconstruir el dato original si no puede ser imposible, debe ser extremadamente costosos para quien intente reconstruirlo. | Aplicación de técnicas Open data/ Big Data en la explotación de la información |

[1] Fuentes normativas:

Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, así como la Directiva 2002/58/CE sobre la protección de la intimidad en las comunicaciones electrónicas

Grupo de Trabajo sobre Protección de Datos Artículo 29 (WP29) de la Comisión Europea que publicó el documento "Dictamen 05/2014 sobre Técnicas de la Anonimización."

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

La Directiva sobre la protección de la intimidad en las comunicaciones electrónicas (Directiva 2002/58/CE)

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Informes Agencia Española de Protección de Datos

# 10. Identificación mediante sistemas biométricos

Según lo establecido en el artículo 4.14) del RGPD se entenderá por datos biométricos aquellos *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".*

En consecuencia, serán considerados como datos biométricos aquellos permitan identificar a una persona y/o confirmar quién es mediante la realización de tratamientos técnicos que recojan datos relativos al aspecto físico, corporales o conductuales, como puede ser su huella digital.

Ya a comienzo de los años 70, Shearson Hamil, una empresa de Wall Street, instaló Identimat, un sistema de identificación automática basado en huella dactilar que se utilizó para el control de acceso físico a instalaciones, siendo la primera solución biométrica de uso comercial. Desde entonces se ha investigado mucho en el campo de la biometría, aplicándose a otros rasgos biométricos diferentes de la huella dactilar.

A día de hoy, el avance en el conocimiento de dichos rasgos y sus correspondientes ventajas e inconvenientes, unido a las posibilidades que ofrece la tecnología, hacen que la biometría se considere uno de los elementos clave en cuanto a técnicas de identificación y seguridad en el futuro.

Dependiendo de la técnica biométrica empleada, los parámetros considerados son diferentes: los surcos de la huella dactilar, la geometría de la mano, la voz, la imagen facial, etc.

De estos parámetros se extrae un patrón único para cada persona, que será el que se utilice para posteriores comparaciones.

Las características biométricas empleadas deben tener las siguientes propiedades:

- Universalidad
- Singularidad
- Permanencia en el tiempo y en distintas condiciones ambientales
- Medibles de forma cuantitativa

Y las tecnologías para medir estas características deben proporcionar:

- Rendimiento
- Aceptación por parte del usuario
- Resistencia al fraude y usurpación

Las tecnologías biométricas se aplican en dos **fases:**

1) **Registro:** el proceso de registro se compone de tres fases distintas:
   - Captura de los parámetros biométricos.
   - Procesamiento creando una plantilla con las características personales de los parámetros capturados.
   - Inscripción de la plantilla procesada guardándola en un medio de almacenamiento adecuado.
2) **Autenticación:** mediante el proceso de autenticación se captura una muestra biométrica del individuo que se comparará con las plantillas ya registradas. Esta autenticación puede realizarse de dos modos diferentes:
   - Identificación: consiste en la comparación de la muestra recogida del usuario frente a una base de datos de rasgos biométricos registrados previamente.
   - Verificación: aquí, sin embargo, el primer paso del proceso es la identificación del usuario mediante algún nombre de usuario, tarjeta o algún otro método. De este modo se selecciona de la base de datos el patrón que anteriormente se ha registrado para dicho usuario. Posteriormente, el sistema recoge la característica biométrica y la compara con la que tiene almacenada. Es un proceso simple, al tener que comparar únicamente dos muestras, en el que el resultado es positivo o negativo.

Se distinguen dos grupos de tecnologías biométricas **en función de la metodología utilizada:**

1) Las que analizan **características fisiológicas** de las personas.
   - Huella dactilar.
   - Reconocimiento facial.
   - Reconocimiento de iris.
   - Reconocimiento de la geometría de la mano.
   - Reconocimiento de retina.
   - Reconocimiento vascular.
   - Líneas de las palmas de la mano.

- Forma de las orejas.
- Piel, textura de la superficie dérmica.
- ADN
- Composición química del olor personal

2) Las que analizan su **comportamiento:**
   - Reconocimiento de firma.
   - Reconocimiento de escritor.
   - Reconocimiento de voz.
   - Reconocimiento de escritura de teclado.
   - Reconocimiento de la forma de andar.

Por otra parte, **dependiendo de qué tecnologías** utilizan los sistemas de identificación biométrica se dividen en:

- Dinámicos: Utilizan tecnologías de comportamiento que comparan acciones o movimientos
- Estáticos: Utilizan tecnologías fisiológicas que miden y comparan rasgos físicos.
- Mutimodales: Combinan técnicas estáticas y dinámicas.

## 10.1. Aplicaciones prácticas

Entre las principales aplicaciones, cabe destacar las siguientes:

- Control de accesos físicos y lógicos.
- Control de presencia.
- Lucha contra el fraude.
- Call centers.
- Medios de Pago.
- Control de navegación.
- Vigilancia.

Adicionalmente, cabe la aplicación en combinación con otras tecnologías

1) Combinación biometría con NFC: con la tecnología NFC (Near Field Communication) integrada en los smartphones se pueden realizar pagos y existen aplicaciones que combinan esta tecnología con la biometría para comprobar la identidad del usuario. Otra aplicación que combina ambas tecnologías es en entornos hospitalarios para administrar medicamentos. Con NFC, en una pulsera o similar, se determina qué medicamentos administrar y con biometría se identifica al paciente para evitar errores.

2) Match on card: Tes una combinación de la biometría y las tarjetas inteligentes para proporcionar una autenticación de doble factor (algo que tienes y algo que eres). En el chip de la tarjeta inteligente se almacena de forma segura el patrón biométrico (generalmente la huella dactilar) y también tiene lugar la comparación. El sistema de autenticación debe proporcionar el dispositivo de captura (lector de huella).

3) Dispositivos móviles:
   - Reconocimiento de huella dactilar.
   - Reconocimiento facial.
   - Reconocimiento de escritura.
   - Reconocimiento de voz.
   - Reconocimiento de manos.
   - Reconocimiento de oreja.
   - Reconocimiento de iris.

## 10.2. Riesgos y beneficios

| RIESGOS | BENEFICIOS |
|---|---|
| Pérdida o robo de información biométrica. | Reducción de costes de mantenimiento de los sistemas de autenticación. |
| Suplantación de Identidad. | Aumento de la eficiencia. |
| Sabotaje. | Control horario. |
| Incumplimiento de la normativa de protección de datos personales | Mejora de la imagen corporativa. |
| Idoneidad de la implantación. | Aumento de la seguridad en el control de accesos. |
| Calidad de la tecnología. | Posibilidad de tramitaciones remotas. |
| Incidencias con el sistema. | Aumento de la Privacidad. |
| Indisponibilidad de sensor. | |
| Variación involuntaria en los rasgos biométricos. | |
| Experiencia de uso negativa. | |
| Falta de aceptación cultural. | |

## 10.3. Medidas preventivas y controles

| RIESGOS | MEDIDAS PREVENTIVAS | CONTROLES |
|---|---|---|
| Pérdida o robo de información biométrica. | • Reforzar la seguridad del Sistema: Garantizar la privacidad y evitar accesos no autorizados.<br>• Política de Seguridad. | Control de accesos. Registros log.<br>Cifrado.<br>Auditoría de Sistemas. |
| Suplantación de Identidad. | Reforzar la seguridad del Sistema: Garantizar la privacidad y evitar accesos no autorizados.<br>Política de Seguridad. | Control de accesos. Registros log.<br>Cifrado.<br>Auditoría de Sistemas. |
| Sabotaje. | Firewall y antivirus | Plan de contingencia. |
| Incumplimiento de la normativa de protección de datos personales[5] | Cumplir con la normativa de protección de datos: información, base de legitimación, minimización de datos y limitación de la finalidad. | Controles periódicos de verificación. |
| Idoneidad de la implantación. | Realizar una buena adaptación. | Verificar que la adaptación se ajusta a las circunstancias concretas. |
| Calidad de la tecnología. | Adquisición de Tecnología de calidad. | • Inventario de Activos Intangibles y Recursos Tecnológicos.<br>• Proceso de Homologación de Proveedores eficaz. |
| Incidencias con el sistema. | Registro de Incidencias. | Plan de Contingencia. |
| Indisponibilidad de sensor. | Registro de Incidencias. | Plan de Contingencia. |
| Variación involuntaria en los rasgos biométricos. | Actualización periódica de muestras. | Verificar que existen procesos automáticos de actualización de muestras. |
| Experiencia de uso negativa. | Canal de Comunicación con clientes efectivo. | Encuestas de satisfacción/experiencia de usuario. |
| Falta de aceptación cultural. | Formación y concienciación | • Plan de Formación.<br>• Registros de Formación. |

5. El artículo 9.1 del RGPD establece que los datos biométricos van a ser considerados como una categoría especial de datos personales y que, como regla general, estará prohibido su tratamiento, en particular, con una finalidad destinada a identificar de manera unívoca a una persona física. La regulación de dicho artículo dispone:
Principio general: *"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física".*
Excepciones: (i) que el interesado por dicho tratamiento hubiera otorgado su consentimiento explícito para dicho tratamiento con uno o más de los fines especificados, excepto que existiera una prohibición legal a nivel europeo o estatal sobre ello; (ii) cuando el tratamiento fuera necesario para el cumplimiento de obligaciones y ejercicio de derechos específicos del responsable del tratamiento o del propio interesado, con relación a aspectos relativos al derecho laboral, seguridad y protección social.
Asimismo, debemos de atender a lo dicho en los considerandos del RGPD:
Considerando 51: *"Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales."*
Considerando 52: "Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial."

## Participantes en el grupo de trabajo que han elaborado este documento:

Coordinador del grupo de trabajo:

- Hurtado, Alonso

Participantes (por orden alfabético):

- Díaz, Carlos
- Díaz-Varela, Nuria
- Estrada, Carolina
- Garzón, Fuencisla
- Heras, Isabel
- Hernández, José María
- Navarro, Vicente
- Romero, Patricia
- Zarzalejos, María


Asociación
Española
de Compliance