La privacidad en la nueva realidad

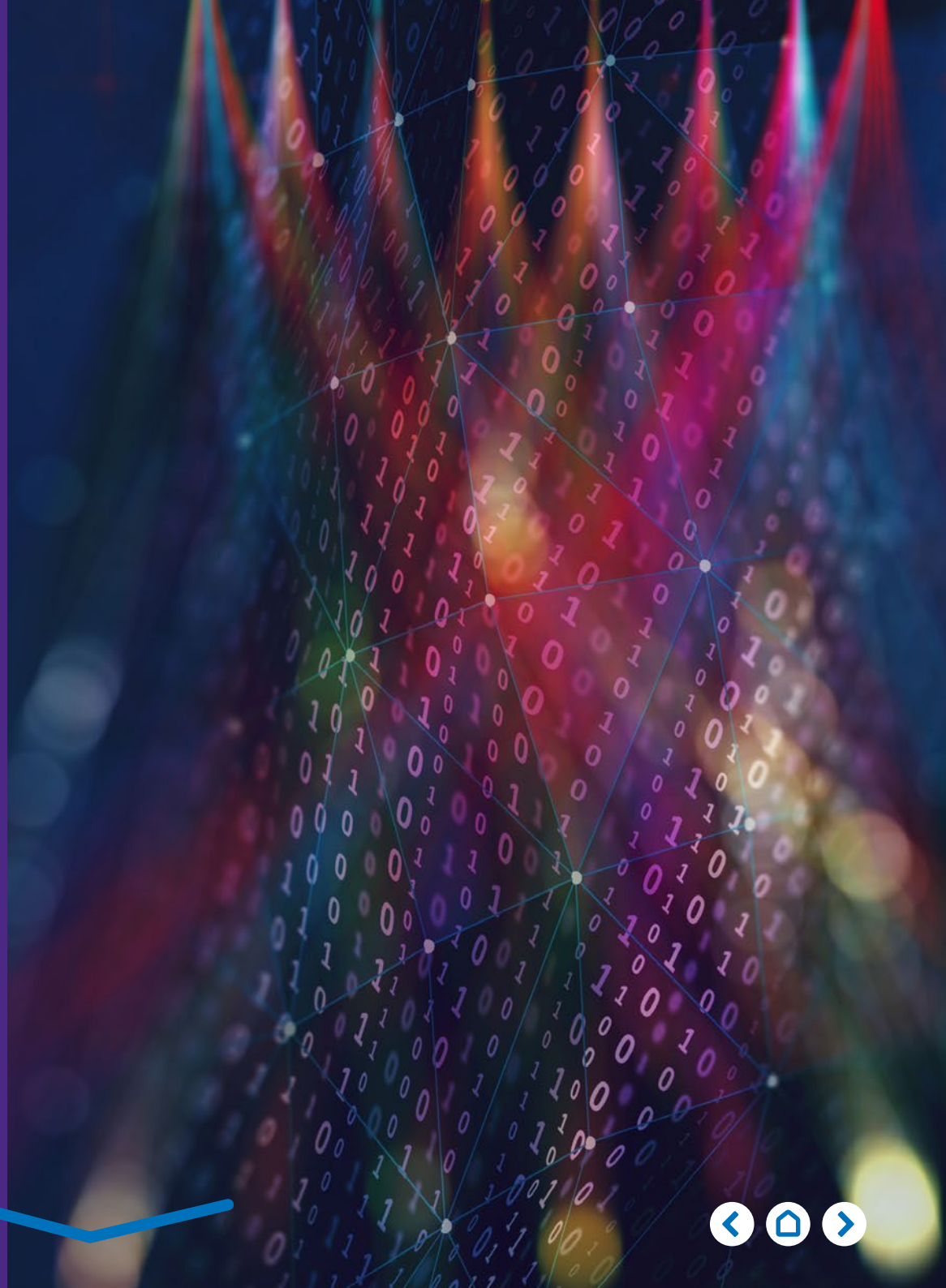
Análisis y enfoque de servicios profesionales de KPMG post COVID-19

Mayo 2020

kpmg.es

Contenido

KPMG



01. Contexto

Como consecuencia de la crisis sanitaria causada por el COVID-19, el uso de la tecnología está siendo un factor clave para adaptar la realización de las actividades habituales a esta nueva forma de vida.

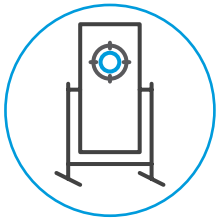
A priori, esta transformación digital proporciona ventajas y beneficios en el desarrollo de dichas actividades. En cambio, puede conllevar una serie de riesgos en la privacidad si no se realizan adecuadamente, impidiendo garantizar el derecho a la protección de los datos personales.

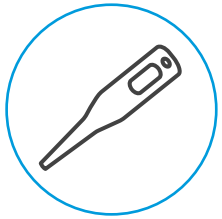
Para asegurar que las actividades se realizan de forma proporcional y que se establece un balance apropiado entre el beneficio obtenido por las mismas y el impacto causado en los interesados, es necesario analizarlas con mayor precisión desde un punto de vista de protección de datos.

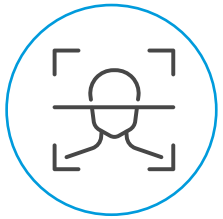
El presente documento pretende ser un punto de partida para analizar los principales riesgos e implicaciones de privacidad derivados del uso de tecnologías disruptivas que están emergiendo durante los últimos años, y algunas de ellas en especial frente a la crisis del Covid-19. En particular, se analizarán 10 actividades específicas que se consideran relevantes en el contexto de la nueva realidad actual.

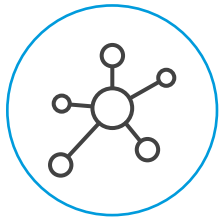
- En base a los riesgos identificados, se proponen una serie de recomendaciones y aspectos a tener en cuenta desde el punto de vista de privacidad para la gestión de los mismos, a fin de realizar un tratamiento adecuado de los datos personales.
- En este contexto de nueva realidad, donde la implicación de la tecnología en la privacidad es más relevante que nunca, desde KPMG seguimos poniendo foco en el desarrollo y adaptación de nuestros servicios para acompañar a nuestros clientes en el escenario que se plantea.

Decálogo de actividades en la nueva normalidad

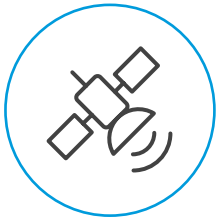

Probadores virtuales


Lectura de temperatura


Reconocimiento facial

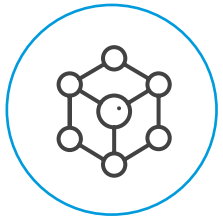

Apps de seguimiento de contagios

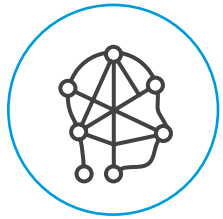

Vehículos conectados


Tecnología 5G


Drones


Smart cities


Smart contracts


Privacidad en entornos IA

Probadores virtuales (2/2)

Principales recomendaciones

1. Medidas de transparencia e información:

El deber de informar de una forma clara y concisa, y que permita al interesado entender las necesidades y limitaciones del tratamiento, es especialmente crítico teniendo en cuenta la tipología de datos tratados y las posibles acciones comerciales que podrían derivarse de la realización de perfilados para recomendar prendas o compras futuras en base a la información recabada durante el tratamiento. Por ello, se deberá indicar las finalidades concretas para el tratamiento de este tipo de datos.

2. Análisis de riesgos y evaluación de impacto en protección de datos:

Teniendo en cuenta la sensibilidad de los datos que van a ser tratados, el uso de tecnologías poco conocidas para el interesado y el potencial uso de los datos para realizar perfilados, es necesario analizar los riesgos e implicaciones de este tipo de tratamientos mediante la realización de una Evaluación de Impacto en Protección de Datos (EIPD).

3. Privacidad desde el diseño:

Elevar el concepto de probador tradicional a la implementación de probadores virtuales requiere de la aplicación de medidas de privacidad desde el diseño para asegurar la protección de datos a lo largo de todo el ciclo de vida del tratamiento. En este ámbito, es recomendable contar con un marco de control fiable que permita identificar y gestionar riesgos desde las fases iniciales y analizar las implicaciones en privacidad de las tecnologías utilizadas para el desarrollo de los probadores virtuales.

4. Medidas para asegurar la correcta aplicación del principio de minimización y conservación de datos:

- Minimización: es necesario ajustar la cantidad de datos recabados a los mínimos necesarios para ofrecer el servicio de probador virtual. Aspectos como el uso de avatares virtuales, la anonimización de las imágenes o la limitación de las imágenes almacenadas pueden ser soluciones que ayuden a mantener la confidencialidad de los datos del interesado sin penalizar la calidad del servicio ofrecido.
- Conservación: acogiéndonos a lo establecido en el RGPD, los datos deberán ser conservados durante no más tiempo del estrictamente necesario para los fines del tratamiento, por lo que siempre que sea posible se deberá optar por la no conservación de los datos.


36.3°C

Lectura de la temperatura (2/2)

Principales recomendaciones

1. Análisis de la base jurídica para tratamiento de categorías especiales de datos:

En primer lugar, es necesario analizar con precisión la base legitimadora de este tipo de tratamiento, especialmente en los casos en que negarse a la toma de temperatura impidiera la realización de la actividad o servicio. Dadas las posibles implicaciones del tratamiento, las medidas de transparencia y métodos para informar al individuo cobran también gran relevancia.

2. Análisis de riesgos y evaluación de impacto en protección de datos:

Este tipo de actividad responde a varios de los criterios de riesgo alto identificados por la AEPD, en particular: categorías especiales de datos, impedimento del uso de un servicio, efecto significativo sobre la persona y el uso de nuevas tecnologías.

Debido al potencial alto riesgo de estos supuestos para los interesados, es necesario realizar una Evaluación de Impacto en Protección de Datos (EIPD), con el fin de establecer garantías y medidas adecuadas para el tratamiento de los datos.

3. Medidas para asegurar la correcta aplicación de los principios de limitación de la finalidad, exactitud y conservación de los datos personales:

- **Finalidad:** ciertos sistemas o dispositivos de medición de la temperatura ofrecen la posibilidad de registrar o incluso tratar información adicional (cámaras térmicas), es por ello que se deberán aplicar las medidas necesarias para asegurar que los datos únicamente se usarán para la finalidad de detectar posibles contagios y evitar el acceso y contacto con otros individuos.
- **Conservación**: dadas las finalidades del tratamiento, a priori, no sería necesario registrar ni conservar los datos de temperatura. En caso de que se requiera, se deberán justificar suficientemente los plazos y criterios de conservación.
- **Exactitud:** debido al impacto que este tipo de tratamientos pueden tener en el individuo, se deberá garantizar la fiabilidad de esas mediciones y el uso de criterios objetivos para determinar la temperatura del individuo.

4. Protección contra la divulgación no justificada de datos a terceros:

Se deberán aplicar medidas para impedir que la información referente a la salud de los individuos sea accesible por personas no autorizadas. Este aspecto es de gran importancia cuando las mediciones se realizan en lugares públicos, lo que supondría un gran impacto para la privacidad del individuo.

Reconocimiento facial (2/2)

Principales recomendaciones

1. Análisis de la base jurídica para tratamiento de categorías especiales de datos:

Se deberá realizar un análisis de las posibles bases legales aplicables en función de las posibilidades que ofrece la AEPD a este respecto. Por ejemplo, el consentimiento del alumno debería ser libre, ofreciendo la universidad una alternativa equivalente (como la posibilidad de realizar la prueba presencialmente respetando las medidas de seguridad o la monitorización en remoto por parte del profesorado) y siendo capaz de acreditar igualdad entre alumnos que consientan o no.

2. Medidas para garantizar la proporcionalidad del tratamiento:

En base a los estudios realizados por la comunidad universitaria, se incide en la posibilidad de realizar las evaluaciones de los alumnos con medios menos intrusivos en protección de datos como exámenes orales por videoconferencia, videos explicativos del alumnado, etc. Dada esta casuística, se deberá analizar en profundidad y previamente al desarrollo del tratamiento, los medios para llevarlo a cabo y la proporcionalidad del mismo, valorando la implantación de medidas alternativas habilitadas para realizar la evaluación de los alumnos en el contexto actual (privacidad desde el diseño).

3. Análisis de riesgos y evaluación de impacto en protección de datos:

El uso de tecnologías como el reconocimiento facial requiere un análisis de los riesgos vinculados al tratamiento de las imágenes y otros posibles datos recopilados (como pulsaciones en el teclado, grabación del entorno del alumno, etc.) y una valoración de su impacto relativa a protección de datos. Al tratarse de un tratamiento de datos biométricos, se deberán definir garantías y medidas técnicas y organizativas más rigurosas para asegurar la protección y seguridad de los datos personales tratados.

4. Medidas para asegurar la correcta aplicación del principio de minimización de datos:

Debido a la sensibilidad de los datos recabados, se deberá poner especial foco en el volumen de datos biométricos que este tipo de sistemas pueden recoger y en la limitación de los mismos a los estrictamente necesarios para cumplir con la finalidad del tratamiento.

5. Medidas de garantía adecuadas con terceras partes involucradas:

En caso de que se requiera la participación de terceros para la implantación de las técnicas de reconocimiento facial o visionado, dicho encargado deberá ofrecer garantías suficientes para asegurar un nivel adecuado de protección de los datos. Este aspecto se deberá tener en cuenta a lo largo de todo el ciclo de vida del proveedor, incluyendo una homologación inicial para definir y establecer las medidas contractuales necesarias así como la realización de revisiones periódicas de cumplimiento.

Apps de seguimiento (2/2)

Principales recomendaciones

1. Análisis de riesgos y evaluación de impacto en protección de datos:

Debido a la tipología de datos tratados referentes a la salud de los individuos, el uso de tecnologías poco conocidas para los mismos y la potencial recogida masiva de datos por la aplicación, se recomienda realizar una Evaluación de Impacto en Protección de Datos (EIPD) con el fin de establecer las medidas técnicas y organizativas necesarias que garanticen un nivel de seguridad adecuado de los datos personales.

2. Protocolos de anonimización fiables y robustos:

Uno de los principales riesgos de estas aplicaciones es la posible identificación de los individuos que forman parte de la red. Por ello, las técnicas de anonimización utilizadas deberán responder a una serie de criterios robustos que impidan relacionar el identificador generado con el número de teléfono al que pertenece y, por tanto, directamente con el individuo. En este aspecto, se recomienda el uso de identificadores únicos y pseudoaleatorios, renovados regularmente y criptográficamente fuertes.

3. Medidas para garantizar que los datos se tratan únicamente para su finalidad:

La finalidad de este tipo de aplicaciones se centra en la identificación y alerta de los individuos que han estado en contacto con un caso positivo en COVID-19. Propósitos más allá del rastreo de contactos como identificar dónde estuvo el individuo en un determinado momento, estudiar patrones de comportamiento o temas de vigilancia a gran escala deben ser evitados.

4. Medidas para asegurar la correcta aplicación del principio de minimización de datos:

En línea con la recomendación anterior, recopilar datos relativos a localización o movimientos de los individuos no cumpliría con el principio de minimización de datos e incluso podría tener implicaciones más graves para el interesado ya que pondría en riesgo la seguridad del mismo.

5. Proporcionar medidas de control sobre los datos:

Para facilitar el control de los individuos sobre sus datos, la instalación de la aplicación debería ser voluntaria, se debería evitar toda posible discriminación por sospecha de infección, ofrecer la capacidad de desinstalar o desactivar la aplicación de forma sencilla y es recomendable que los identificadores se almacenen en el dispositivo del usuario de forma descentralizada.

Vehículos conectados (2/2)

Principales recomendaciones

1. Mecanismos de transparencia e información:

Debido a que el vehículo puede ser conducido por diferentes individuos que no siempre sean el titular del mismo, la información proporcionada cuando se realiza la venta del vehículo puede no ser suficiente para cumplir con el principio de transparencia. Ciertas comunicaciones o funcionalidades del vehículo interconectado pueden ser activadas sin que los usuarios sean conscientes de ello. En este caso, es necesario establecer mecanismos de transparencia y control sobre los datos.

2. Análisis de la base jurídica para tratamiento de los datos almacenados en el vehículo:

El vehículo conectado puede ser considerado a priori como un equipo terminal en base al estudio realizado por el Comité Europeo de Protección de Datos y, por tanto, el acceso a los datos almacenados en el mismo puede estar supeditado a las condiciones definidas en la directiva ePrivacy, sin perjuicio de los posibles cambios que introduzca el nuevo borrador del reglamento ePrivacy.

3. Medidas técnicas y organizativas apropiadas para mantener un nivel adecuado de seguridad:

- Análisis de riesgos y evaluación de impacto en protección de datos: dentro del gran número de datos que estos vehículos recopilan, los datos referentes a localización del vehículo, datos biométricos y los datos relativos a posibles infracciones al volante son especialmente relevantes en el contexto de la privacidad. La tipología de datos tratada, el tratamiento masivo de los datos, la tecnología utilizada y el posible impacto que esta tecnología puede tener en los individuos hace necesaria la realización de un análisis más exhaustivo del riesgo e impacto en privacidad a fin de definir las medidas técnicas y organizativas adecuadas para garantizar la privacidad.
- Medidas de seguridad adecuadas: la implantación de medidas de seguridad fiables es una obligación en el contexto de los vehículos conectados, debido al impacto que la materialización de los riesgos referentes al acceso no autorizado y control de los sistemas del vehículo puede causar en la seguridad física de los pasajeros. Alarmas en caso de ataque a los sistemas, guardar un histórico o log de accesos o el uso de frecuencias seguras son ejemplos de estas medidas.

4. Divulgación de datos no autorizada a terceros:

Un ejemplo de esta situación puede ser el acceso no autorizado a los datos por parte de aseguradoras o terceros para ofrecer pólizas de seguro en base a los patrones de conducción. Es necesario aplicar medidas específicas para evitar el tratamiento no autorizado de los datos por terceros, en aquellos casos que el usuario no haya dado el consentimiento explícito.


5G

Tecnología 5G (2/2)

Principales recomendaciones

1. Transparencia y trazabilidad de los datos:

La información proporcionada al individuo referente al tratamiento de sus datos debe ser clara, precisa y en un lenguaje sencillo y comprensible para el interesado.

La trazabilidad e identificación de los flujos de datos cobra especial relevancia teniendo en cuenta las posibles implicaciones transfronterizas que requieran la aplicación de garantías adecuadas para las transferencias internacionales de datos.

2. Determinación de responsabilidades referentes al tratamiento de los datos:

Este aspecto cobra especial relevancia debido tanto a los numerosos flujos de datos como a la gran cantidad de partes implicadas que participan en la explotación de la tecnología 5G (desarrolladores, agentes, operadores, etc.). Se deberán definir los roles y responsabilidades de las partes involucradas así como delimitar las obligaciones de cada una en materia de protección de datos.

3. Medidas de control de los individuos sobre sus datos:

Se deberán facilitar medidas de control del individuo sobre sus datos, tanto de aquellos proporcionados por él mismo como de los inferidos en base a su actividad o la de otros dispositivos conectados a la red.

4. Medidas técnicas y organizativas apropiadas para mantener un nivel adecuado de seguridad:

- Análisis de riesgos y evaluación de impacto en protección de datos: los riesgos y las implicaciones en privacidad en la tecnología 5G deberán analizarse desde el punto de vista de protección de datos y tenerse en cuenta particularmente desde las primeras fases de diseño de los tratamientos.
- Medidas de seguridad en las comunicaciones: como consecuencia del incremento de la conectividad y puntos de entrada a la red, la exposición ante ciberataques aumenta considerablemente. Reforzar medidas como el cifrado de las comunicaciones de extremo a extremo y la segmentación segura de los datos en red puede evitar el filtrado de información.

5. Medidas para minimizar el volumen de datos recopilados acerca de los individuos:

Debido a los numerosos datos tratados en los servicios 5G, se deberá tener especial consideración con los datos referentes a la geolocalización y perfilado, tratando siempre de minimizar los mismos a los estrictamente necesarios para el tratamiento.

Drones (2/2)

Principales recomendaciones

1. Mecanismos de transparencia e información:

Para cumplir con los requisitos de transparencia e información a los individuos, y dada la dificultad para identificar o detectar los drones, se recomienda el desarrollo de mecanismos o canales informativos con la información referente al tratamiento de los datos, entre otras: tipo de datos recabados, finalidades para las que se están recabando y por parte de quién.

2. Privacidad desde el diseño:

Teniendo en cuenta el gran número de posibilidades y capacidades tecnológicas que pueden integrarse en los drones (cámaras de reconocimiento facial, radares, escáneres infrarrojos, GPS, etc.), la aplicación de medidas de privacidad desde el diseño para asegurar la protección de datos a lo largo de todo el ciclo de vida del tratamiento cobra especial relevancia. Ejemplos de estas medidas serían: ajustar la resolución de la imagen al mínimo posible si el tratamiento no requiere una identificación precisa del individuo y limitar la grabación de las imágenes para los casos estrictamente necesarios.

3. Análisis de riesgos y evaluación de impacto en protección de datos:

Como consecuencia del gran volumen de datos tratados por estos sistemas, la posible finalidad de monitorización continua del interesado, la tipología de los mismos y en función de la tecnología utilizada, se deberá realizar una evaluación de impacto en protección de datos a fin de determinar si el tratamiento es legítimo, necesario y proporcional al fin perseguido, así como definir y documentar las medidas adoptadas para abordar los riesgos identificados.

4. Medidas de seguridad para evitar el acceso no autorizado a los datos:

Se deberán aplicar medidas específicas para garantizar un nivel adecuado de seguridad y evitar amenazas como la manipulación a distancia de los drones y el acceso no autorizado a los datos durante su transmisión desde el dron a la estación base. Estas medidas recogen aspectos como:

- Anonimización de cualquier dato personal innecesario.
- Implantación de protocolos de comunicaciones seguros que impidan tanto el control del dispositivo como el acceso a las transmisiones de los datos capturados por terceros.
- Cifrado de los datos capturados y almacenados en el dron.

Smart cities (2/2)

Principales recomendaciones

1. Medidas para evitar el perfilado masivo de los individuos:

Los datos relativos a un mismo individuo pero recabados por diferentes fuentes pueden ser combinados y pueden mostrar patrones de comportamiento o preferencias específicas. Para las finalidades perseguidas por las ciudades inteligentes, a priori, basta con obtener información relativa a colectivos y comportamiento de la sociedad. Por ello, el tratamiento de los datos de forma anonimizada o agregada es una estrategia apropiada para dificultar la asociación de datos a individuos específicos y evitar perfilados innecesarios para las finalidades perseguidas.

2. Análisis de riesgos y evaluación de impacto en protección de datos:

Teniendo en cuenta el nivel de implicación tecnológica en las Smart Cities, la afectación que puede tener en los ciudadanos y el tratamiento masivo de datos personales, se debe optar por mecanismos que permitan analizar y definir medidas para gestionar el riesgo de manera preventiva y proactiva. Previamente a la realización de este tipo de actividades, se requiere la ejecución de una evaluación de impacto en privacidad a fin de definir medidas específicas que aseguren el derecho a la protección de datos de los ciudadanos.

3. Medidas para asegurar un nivel adecuado de seguridad:

La interconexión supone una mayor exposición de los dispositivos conectados a la red, ya que aumenta el número de puntos de acceso a los mismos. Como consecuencia, se deberá poner especial foco en la definición de un plan de detección y respuesta ante posibles brechas de seguridad para evitar el posible filtrado o acceso no autorizado a esta información que tendría como resultado una elevada exposición de datos relativos a hábitos y actividades cotidianas de los individuos.

4. Medidas de garantía adecuadas con terceras partes involucradas:

La seguridad y privacidad debe ser desplegada e integrada a lo largo de toda la cadena de suministro en las Smart Cities. En concreto, se deberá analizar cuidadosamente a los proveedores y terceras partes implicadas, e invertir en integrar seguridad y privacidad a lo largo de todo el ecosistema. Este aspecto debería incluir una homologación inicial del proveedor para asegurarse que dispone de las garantías suficientes, formalizar las medidas contractuales necesarias así como la realización de revisiones periódicas de cumplimiento.

Smart contracts (2/2)

Principales recomendaciones

1. Medidas para garantizar el ejercicio de derechos por parte de los interesados:

Uno de los aspectos más característicos de la tecnología Blockchain es la inmutabilidad de los datos registrados en la cadena de bloques. Este aspecto afecta del mismo modo a los contratos inteligentes, en caso de no poder modificar el contrato cualquier cambio en leyes, negocio o similar podría ser difícil de implementar, suponiendo del mismo modo un reto para rectificar, actualizar o suprimir los datos personales incluidos en el contrato. Evitar almacenar datos de carácter personal por defecto y el uso de técnicas de que impidan identificar directamente a los individuos como la ofuscación, anonimización o agregación de datos permitirían implementar una solución más conciliadora con la privacidad.

2. Medidas para garantizar la aplicación de los plazos de conservación:

En línea con lo explicado previamente, los datos personales almacenados en una cadena de Blockchain no pueden ser alterados o borrados, se almacenan de forma permanente. El principio de conservación establece que los datos no deben ser mantenidos de forma que se permita la identificación de los individuos por más tiempo del necesario. En este ámbito, podemos volver a recurrir a técnicas de anonimización de datos personales como medida para asegurar que no se conservan por más tiempo del necesario.

3. Garantías adecuadas en transferencias internacionales de datos:

En ciertas soluciones, debido a la descentralización de los datos en la tecnología Blockchain, puede resultar difícil determinar qué jurisdicciones aplican para cada caso en cuestión, no hay un control real sobre la ubicación de los usuarios. La identificación de transferencias internacionales y la aplicación de salvaguardias apropiadas son aspectos que se ven afectados por esta funcionalidad del Blockchain. Cifrar las transacciones de modo que únicamente las partes involucradas puedan acceder a toda la información ayudaría a identificar en mayor medida los flujos del tratamiento de datos personales.

Privacidad en entornos de IA (2/2)

Principales recomendaciones

1. Medidas de transparencia e información:

En este tipo de desarrollos tecnológicos, especialmente cuando nos referimos a los algoritmos de IA, el derecho a ser informado se convierte en un punto crítico debido a la confidencialidad a la que está sometida esta información. La necesidad de ofrecer información que permita comprender el funcionamiento de la solución es más crítica en casos en los que se puedan realizar decisiones automatizadas y/o perfilado (patrones utilizados, valores de precisión, supervisión humana, etc.).

2. Análisis de riesgos y evaluación de impacto en protección de datos:

Las soluciones basadas en IA suelen conllevar un nivel de riesgo alto, por la tecnología utilizada, el volumen de datos tratados y la tipología de tratamiento. Para analizar los riesgos e implicaciones en privacidad es necesaria la realización de una Evaluación de Impacto en Protección de Datos (EIPD). Para que dicha evaluación sea completa, se recomienda tener en cuenta riesgos y amenazas específicos para los entornos de IA, entre los que podemos encontrar ataques por adversarial machine learning, imitación de patrones, manipulación de la API de usuario, etc.

3. Medidas para asegurar la correcta aplicación de los principios de minimización y exactitud:

- Minimización: especialmente en tratamientos basados en entornos de IA es necesario establecer un equilibrio entre el desarrollo y precisión de la solución y el número de datos que se requieren para el tratamiento. Aspectos como la fiabilidad, robustez, actualidad y relevancia de los datos favorecen notablemente a la hora de limitar el volumen de datos utilizados para conseguir la precisión deseada de la solución IA. Existen además numerosas técnicas de minimización de datos para este tipo de tecnología que deben tenerse en cuenta, como son: técnicas de validación cruzada, modelos de aprendizaje federado, agregación de datos, etc.

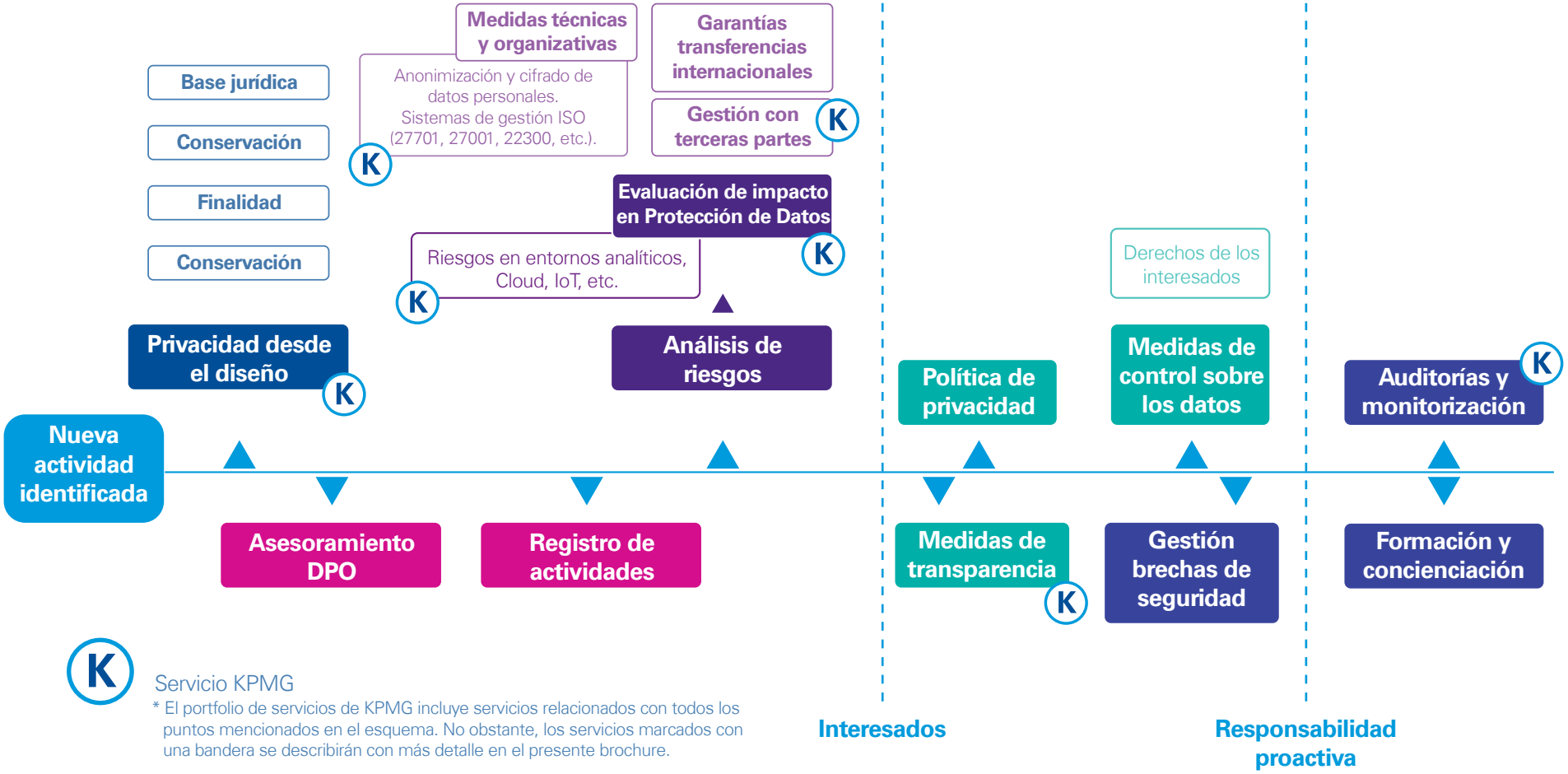
- Exactitud: este principio es particularmente relevante si el tratamiento está basado en datos biométricos (huella, reconocimiento facial, etc.) evitando así falsos positivos u otros factores relacionados. El uso de algoritmos estables y precisos, y la verificación y validación de los componentes de IA, son ejemplos de medidas para garantizar la exactitud de los datos personales.

4. Garantías suficientes en transferencias internacionales de datos:

Especialmente si la solución se basa en servicios en la nube o en casos en que se requiere mejorar o evolucionar el modelo por parte de terceros, es posible que se identifiquen transferencias internacionales de datos, siendo necesario establecer las garantías definidas en el RGPD.

02. Consideraciones generales

Adicionalmente a las recomendaciones específicas en materia de protección de datos identificadas para cada actividad, el siguiente esquema presenta de un modo más genérico los principales pasos a tener en cuenta en el desarrollo de cualquier nueva actividad que implique el tratamiento de datos personales.



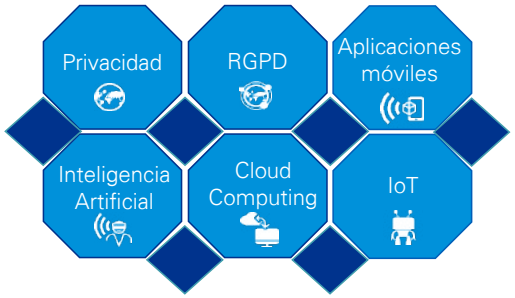
03. Servicios KPMG

Framework de Privacidad desde el Diseño (PbD)

Marco de control PbD enfocado a identificar, prevenir y evitar potenciales riesgos derivados del tratamiento de datos personales desde las fases iniciales del desarrollo de nuevos proyectos o modificación de los existentes.

Beneficios

- Aseguramiento con respecto al **principio de privacidad desde el diseño y por defecto**.
- Identificación de riesgos en privacidad desde las **fases iniciales** de los proyectos y previamente a su materialización.
- **Marco de control bien** definido en base a los **7 principios fundamentales de PbD***.
- **Customización del marco PbD** en base a la tipología de actividades de tratamiento y tecnología utilizada.



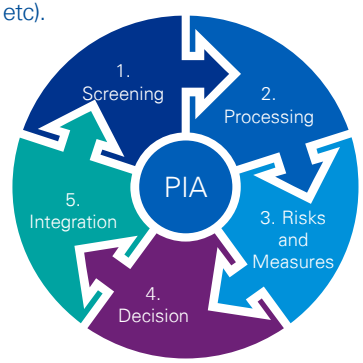
(*) Principios desarrollados por el Instituto de Privacidad y Big Data dirigido por la Dr. Ann Cavoukian.

Privacy Impact Assessment Tool

Herramienta desarrollada por KPMG para realizar las Evaluaciones de Impacto en Protección de Datos (PIAs en inglés). La evaluación se divide en dos partes diferenciadas: sistemas de información y principios fundamentales del tratamiento.

Beneficios

- Identificación de los procesos o tratamientos de **alto riesgo**.
- **Evaluación del impacto y probabilidad de los riesgos de privacidad** asociados con una **tecnología** o un **nuevo proyecto** de alto riesgo que involucre datos personales.
- Identificación de **medidas técnicas y organizativas adecuadas** para garantizar un nivel adecuado de seguridad.
- **Personalización del catálogo de amenazas y controles** para diferentes tecnologías (IA, Cloud, IoT, etc).



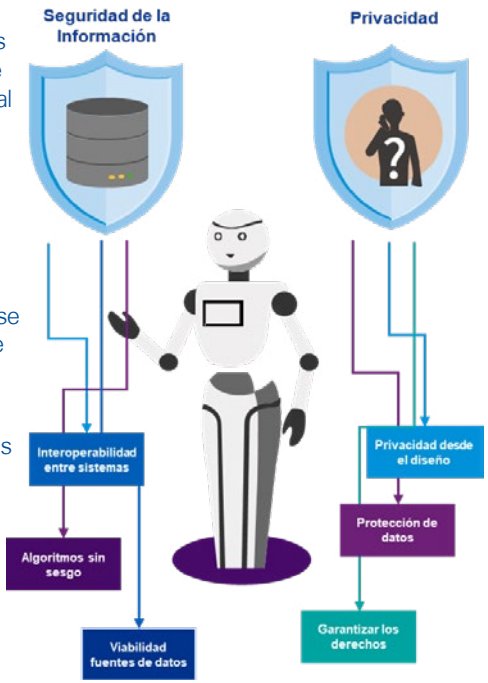
Privacidad y Seguridad para entornos analíticos

Herramienta desarrollada por KPMG para realizar las Evaluaciones de Impacto en Protección de Datos (PIAs en inglés).

Framework para la gestión del riesgo en este tipo de entornos, basado en los principales estándares del mercado.

Beneficios

- **Identificar los riesgos** expuestos por la adopción de inteligencia artificial relacionados con la tecnología, seguridad y privacidad.
- Revisión de **modelos y algoritmos** en base a metodologías de desarrollo seguro.
- Revisión de modelado de datos y entornos no preproductivos.
- Revisión **arquitectura** de despliegue.
- **Análisis** de la **criptografía**.



03. Servicios KPMG

Third-Party Risk Management (TPRM)

Enfoque para la gestión del ciclo de vida de los proveedores en relación al riesgo tecnológico.

Beneficios

- **Identificación de proveedores y servicios** en función de su criticidad para aplicar medidas específicas **en base a riesgo**.
- Homogenización del proceso de **contratación y revisión** de proveedores.
- Enfoque holístico, que cubre el ciclo de **riesgo del proveedor end to end**.
- Mejora en las **garantías a las áreas de negocio respecto a la seguridad y privacidad** de los servicios en cuestión

Anonimización

Análisis de soluciones de anonimización o seudonimización de datos personales con una metodología y un marco de gestión propio basado en las guías publicadas por diferentes autoridades de control.

Beneficios

- Aseguramiento, tanto **técnico y jurídico**, de que la posible **solución de anonimización o seudonimización** cumple con los criterios del RGPD.
- Identificación de **deficiencias y fortalezas** de la solución y proposición de **medidas correctoras** o complementarias a adoptar con carácter previo a su potencial implementación.
- Análisis de **requerimientos de roles, claves, algoritmos y permisos de la solución**.

ISO 27701 - PIMS

Enfoque para la gestión eficaz y continuada de un sistema de gestión para la seguridad y la privacidad basado en el estándar internacional ISO 27701. Se trata de una extensión de las ISOS 27001 y 27002.

Beneficios

- Proteger la **confidencialidad, disponibilidad e integridad** de la información personal, mitigando posibles riesgos de seguridad y promover una **cultura de privacidad en la organización**, fomentando un sistema de mejora continua y un sistema de gestión unificado.
- Demostrar **responsabilidad proactiva** con respecto al RGPD y otras leyes y/o estándares de privacidad.
- Construir y mantener la **confianza y satisfacción** de los **clientes**.

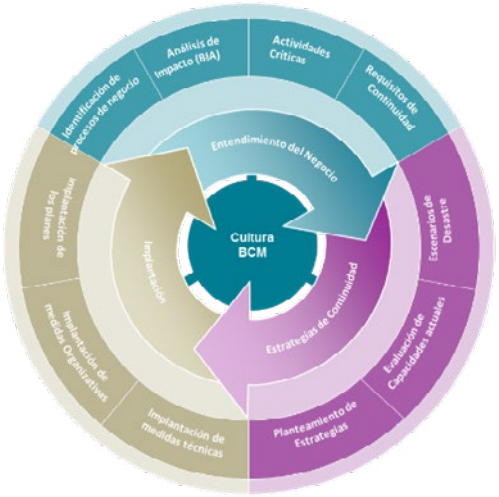
03. Servicios KPMG

Plan de Continuidad de Negocio

Creación y mantenimiento de Planes de Continuidad de Negocio, Recuperación frente a desastres y Planes de Contingencia con base a estándares internacionales tales como la ISO 22301.

Beneficios

- Garantizar la **disponibilidad** mínima necesaria de los procesos críticos de negocio en caso de sufrir una **contingencia**.
- Establecer **procesos de recuperación** necesarios para volver a una situación de normalidad de acuerdo a los niveles de servicio definidos.

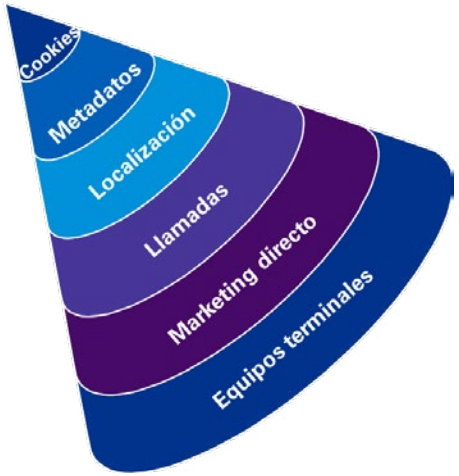


E-Privacy

Metodología para llevar a cabo los proyectos de transformación al Reglamento sobre la privacidad y las comunicaciones electrónicas (ePrivacy).

Beneficios

- **Evaluación** de cada uno de estos aspectos en función de su **grado de madurez**, de manera que se pueda concretar el nivel de partida respecto a su adecuación.
- Definición de **planes de acción.**
- **Implementación** de las **acciones propuestas**.



Privacy Health Check - PHC

Herramienta con metodología propia, basada en los principales marcos de referencia y mejores prácticas de la industria respecto de la protección de datos para realizar una revisión del grado de madurez de nuestro programa de privacidad – RGPD y/o LOPDGDD.

Beneficios

- Demostrar **responsabilidad proactiva** con respecto a las auditorías indicadas en el RGPD.
- **Mejorar el nivel de madurez** con respecto al programa de privacidad de la compañía.
- Identificar **deficiencias o aspectos de mejora** para subsanarlos a través de un plan de acción.

04. Bibliografía

1. Guías y publicaciones de la Agencia Española de Protección de Datos (AEPD):

- El uso de las tecnologías en la lucha contra el COVID19. Un análisis de costes y beneficios. https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf
- Informe acerca del uso de reconocimiento facial en exámenes. https://www.aepd.es/es/documento/2020-0036.pdf
- Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos
- Vehículos conectados. https://www.aepd.es/es/prensa-y-comunicacion/blog/vehiculos-conectados
- Introducción a las tecnologías 5G y sus riesgos para la privacidad. https://www.aepd.es/sites/default/files/2020-05/nota-tecnica-privacidad-5g.pdf
- Drones y protección de datos. https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf
- Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

2. Guías y publicaciones de l Comisión Europea:

- Comunicación de la Comisión Europea: orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020XC0417%2808%29
- Shaping Europe's digital future. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
- European data strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
- Excellence and trust in artificial intelligence. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en
- Smart cities. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_es#últimas-novedades

04. Bibliografía

1. Otras guías y publicaciones de interés:

- IAPP: DPA guidance on COVID-19. https://iapp.org/resources/article/dpa-guidance-on-covid-19/
- A socio-technical framework for digital contact tracing. https://arxiv.org/ftp/arxiv/papers/2005/2005.08370.pdf
- Comité Europeo de Protección de Datos: Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_es
- Autoridad Catalana de Protección de Datos (APDCAT): La protección de datos de carácter personal en las ciudades inteligentes ("Smart Cities"). https://apdcat.gencat.cat/es/documentacio/smart_cities/
- Protecting Personal Data using Smart Contracts. https://arxiv.org/pdf/1910.12298.pdf
- ENISA: Improving information security in the financial sector. https://www.enisa.europa.eu/publications/blockchain-security
- The European Union Blockchain Observatory and Forum: Legal and Regulatory framework of Blockchain and Smart Contracts. https://www.eublockchainforum.eu/reports
- Information Commissioner's Office: Guidance on the AI auditing framework. https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf

Contactos:

Javier Aznar
Director, Technology Risk
KPMG en España
T: +34 699 35 00 29
E: jaznar@kpmg.es

Juan Ignacio Ríos
Senior Manager, Technology Risk
KPMG en España
T: +34 683 66 38 39
E: juanignaciorios@kpmg.es