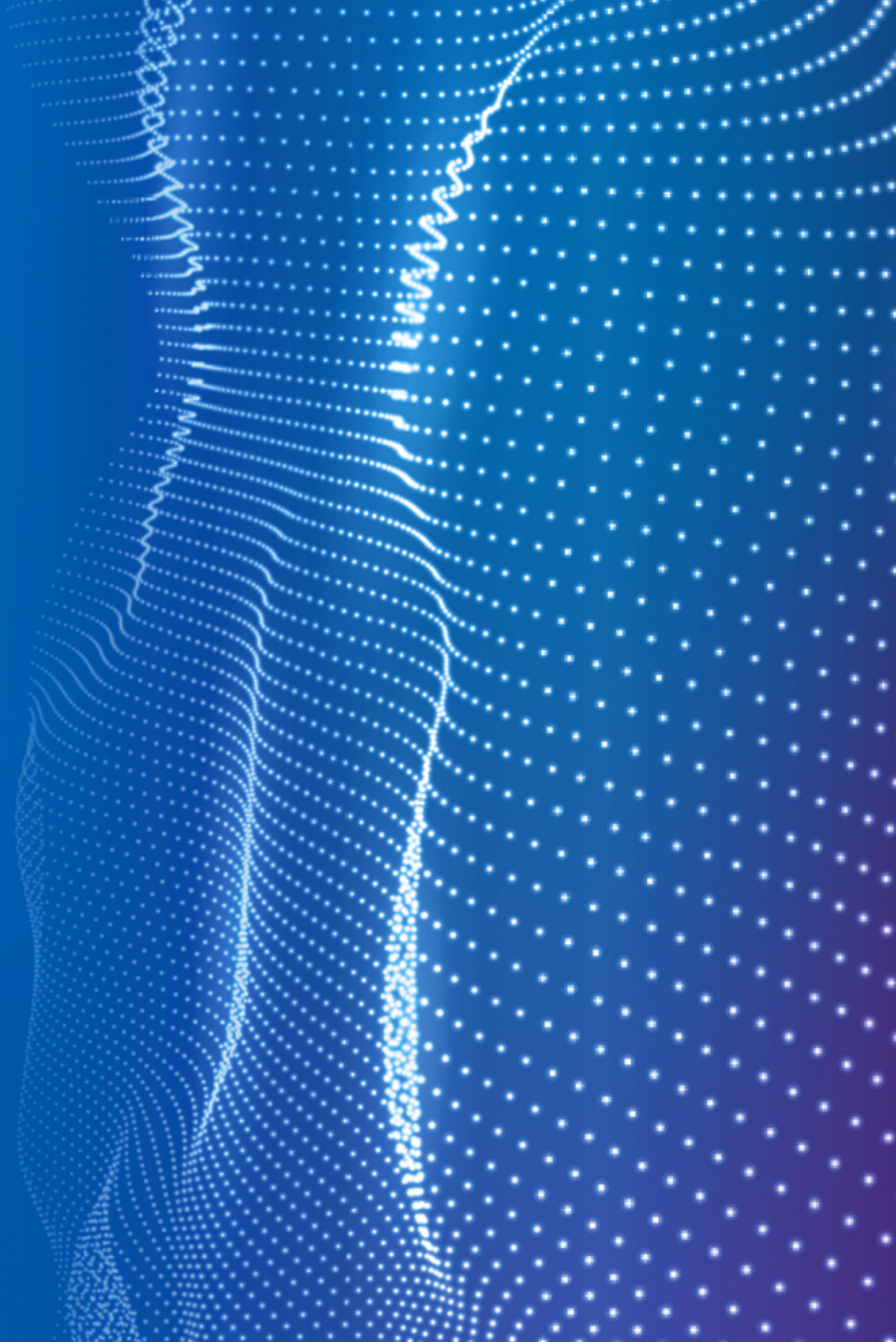
Los entornos analíticos y sus riesgos asociados

Enfoque de KPMG para la gestión de los riesgos derivados de los entornos de analítica avanzada

kpmg.es

2020



Índice

La era de los datos:

Ética y seguridad en los modelos algorítmicos

Un reciente informe de investigación muestra que el valor de los datos va a aumentar exponencialmente y que el volumen de los mismos se multiplicará por 5 entre 2020 y 2025*.

Los datos han sido cruciales desde los inicios de la era digital, desde los primeros sitios web de comercio electrónico al crecimiento explosivo de servicios en la nube y la información inicial obtenida de análisis de Big Data.

La adopción de tecnologías emergentes se está acelerando en todo tipo de organizaciones: el uso de **Inteligencia Artificial (IA), Machine Learning y Big Data son los grandes catalizadores** del cambio en estos tiempos. Por tanto, cada vez son más los entornos que procesan y analizan cantidades ingentes de datos para tomar decisiones automatizadas, cognitivas o inteligentes:

– El uso de algoritmos ayuda a crear y descubrir **patrones** dentro de grupos de datos **para ofrecer productos y/o servicios a clientes específicos** difíciles de detectar a simple vista.

– En caso de que una compañía quiera mejorar su rotura de stock o controlar cambios de tendencia, por ejemplo, el uso de algoritmos **optimizará su planificación y previsión de la demanda de sus clientes.**

– Otro uso habitual es el de los **chatbots inteligentes para resolver dudas o incidencias con clientes,** ahorrando así las compañías en soporte y atención al cliente.

Pero ante todo esto que se está desplegando y utilizando en tantas compañías, **los riesgos a los que se enfrentan** son, entre otros, la correcta utilización de estos entornos y la protección de los mismos. Además, los algoritmos que hay detrás pueden ser **destructivos** cuando producen resultados inexactos o sesgados, una preocupación inherente a la que se enfrenta cualquier organización que quiera confiar en su uso.

Por ello, el poder de este tipo de tecnologías transformadoras solo puede desbloquearse por completo mediante la **comprensión y control de los riesgos** que generan: saber identificarlos y tener la capacidad para la gestión de los mismos se ha convertido en un proceso necesario en cada organización.

* Splunk, TRUE Global Intelligence. (2020)."The Data Age Is Here. Are You Ready?", Recuperado de https://www.splunk.com/en_us/campaigns/data-age.html

La era de los datos:

Ética y seguridad en los modelos algorítmicos

Los reguladores y supervisores se están preocupando en cómo las tecnologías emergentes afectan las competencias centrales de la gobernanza del riesgo de identificar, administrar, medir y controlar los riesgos en toda empresa, así como en la importancia de los recursos, las habilidades y la experiencia adecuada para entregar esto de manera efectiva.

Analítica Avanzada

Usar de manera precisa los datos de las distintas fuentes que tengamos para predecir posibles eventos y/o comportamientos que nos ayuden a afrontar cambios en el negocio.

Inteligencia Artificial (IA)

Combinar algoritmos con la finalidad de crear máquinas que presenten las mismas capacidades que el ser humano.

Machine Learning

Crear y adaptar modelos con el propósito de permitir a los programas aprender a través de la experiencia.

RPA: Robotic Process Automation

Replicar las acciones de un ser humano real que interactúa con una aplicación de software para realizar tareas.

La era de los datos:

¿Qué es la ética de los algoritmos?

Todas las tecnologías emergentes mencionadas en la página anterior tienen una cosa en común: **el uso de algoritmos.** Por supuesto, estos algoritmos están diseñados de alguna forma para **intervenir, en mayor o menor medida, en la toma de decisiones del ser humano,** cada uno con su objetivo específico explicado anteriormente. Un algoritmo, por tanto, puede procesar en cuestión de segundos una cantidad ingente de información que contiene una compañía y ofrecerle una propuesta aparentemente objetiva.

Por ello, lo primero que nos preguntamos es, ¿cuál es el criterio a la hora de generar un algoritmo? El principal problema no radica en qué se tiene en cuenta a la hora de diseñar los algoritmos (que también), sino en cómo se utilizan, cómo se filtran, **cómo han sido entrenados y las eventuales correlaciones y dependencias con otras variables y modelos.** Y es aquí donde se debería contemplar la ética algorítmica que, básicamente, consiste en considerar la ética a la hora de desarrollar algoritmos para la IA y el Machine Learning, entre otros.

Una empresa de paquetería, a través del análisis de los datos, **rediseñó las rutas de sus conductores y redujo los kilómetros** recorridos y reconfiguró y estructuró de nuevo sus mapas.

Ciertas compañías consiguen **personalizar el hábito de compra de sus usuarios,** destacando los intereses de los mismos en la página inicial de la web.

Es destacable que, a la hora de diseñar y emplear algoritmos, las compañías tengan en cuenta esta dimensión para **evitar los sesgos** que se establecen y se reproducen en los propios algoritmos. Como indicamos, en última instancia, **afectan a las libertados e igualdades** de los usuarios.

El riesgo, por tanto, está en la falta de vigilancia del algoritmo, por muy sofisticado que sea. **Las compañías se deben comprometer a analizar desde la perspectiva de la ética los algoritmos** para que garanticen la transparencia y calidad de los datos, que sean confiables y que no generen abusos. Asimismo, una **supervisión y/o auditoría de los mismos** cada cierto tiempo es necesaria.

Como estamos ante una sociedad cada vez más gobernada por algoritmos, todos estos factores están forzando a la industria e instituciones públicas a **buscar alianzas para crear una gobernanza transparente, ética y justa** respecto a este tema.

Hay compañías que calculan a partir de un historial crediticio, nivel de ingresos y otros datos la probabilidad de que un ciudadano de EUU devuelva un préstamo. Además, hay compañías que se benefician de esos datos para no contratar empleados que estén endeudados.

Se investigó que en un buscador se muestran fotos de mujeres al emplear palabras como ”sensible” o “emocional”. Por el contrario, si se busca la palabra “inteligente” o “racional”, las fotos de hombres están más representados.

Estrategia Europea

Estrategia digital Europea

Esta Estrategia Global De Cooperación Digital de la UE podrá impulsar un enfoque europeo de la transformación digital que se basa en una larga historia de tecnología, innovación e ingenio, investidos en valores europeos.

Esta estrategia, además, se proyectará en el escenario internacional.

La **economía ágil de datos y su enorme potencial** en transformación nos ha afectado a todos nosotros y **Europa,** por su parte, parece ser que está lista para aprovechar al máximo las ventajas que traerá este tipo de prácticas: la **Comisión Europea,** durante los próximos cinco años, se centrará en los siguientes **tres objetivos clave** que mostramos a continuación para garantizar que las soluciones digitales ayuden a Europa a seguir su propio camino hacia una transformación que trabaja en beneficio de las personas respetando sus valores:

– **Tecnología que funciona para las personas:** Una fuerte y competitiva economía que domina y da forma a la tecnología de una manera que respeta los valores europeos.

– **Una economía justa y competitiva:** El objetivo es que empresas de todos los tamaños y de cualquier sector puedan competir en igualdad de condiciones, desarrollando, comercializando y utilizando tecnologías digitales a una escala que impulse su productividad y competitividad global, y que los consumidores, al mismo tiempo, puedan estar seguros de que sus derechos son respetados.

– **Una sociedad abierta, democrática y sostenible:** Un entorno de confianza en el que los ciudadanos tienen el poder de actuar e interactuar sobre los datos que proporcionan tanto en línea como *offline.*

Sin embargo, para que esa transformación digital sea completamente exitosa, la Comisión Europea indica que **se necesita crear un marco de derecho para garantizar una tecnología confiable y para dar a las empresas la confianza, las competencias y los medios para digitalizarse.**

Por tanto, la coordinación de esfuerzos entre la UE, los Estados miembros, las regiones, la sociedad civil y el sector privado son clave para lograr y fortalecer un liderazgo digital europeo.

Estrategia Europea

…La Comisión Europea, además, se ha pronunciado en detalle sobre dos objetivos:

La estrategia europea para los datos, que acompaña al **Libro Blanco sobre IA,** tiene como objetivo permitir que Europa se convierta en la economía ágil de datos más atractiva, segura y dinámica del mundo, dotando a Europa de datos para mejorar las decisiones y mejorar la vida de todos sus ciudadanos.

La estrategia establece una serie de medidas políticas, incluida la movilización de inversiones públicas y privadas, necesarias para lograr este objetivo.

1 Una estrategia europea para los datos

El objetivo de la UE es crear un espacio único de datos europeo, un verdadero **mercado único de datos,** abierto a datos de todo el mundo, donde los datos personales y no personales, incluidos los datos comerciales confidenciales, sean totalmente seguros y que las empresas también tengan **fácil acceso** a una cantidad casi infinita de datos industriales de alta calidad, que impulse el crecimiento y cree valor.

Debería ser un **espacio en el que la legislación de la UE pueda aplicarse de forma eficaz** y en el que todos los productos y servicios basados en datos cumplan las normas pertinentes del mercado único de la UE.

2 Enfoque europeo sobre la IA

La Comisión Europea también se ha pronunciado al respecto de la IA, señalando que Europa puede combinar sus puntos fuertes tecnológicos e industriales con una infraestructura digital de alta calidad y un marco regulador basado en sus valores fundamentales para **convertirse en un líder mundial en innovación en la economía de datos y sus aplicaciones,** tal como se establece en la estrategia europea de datos.

Sobre esa base, puede desarrollar un **ecosistema de IA que lleve los beneficios de la tecnología a toda la sociedad y a las economías europeas.**

Desafíos y riesgos para las compañías

Como bien hemos explicado al inicio del documento, el crecimiento que estamos viviendo de los datos es una realidad y supone un reto hasta ahora desconocido por las compañías.

Se deberá trabajar en garantizar que los algoritmos y modelos son desarrollados sin sesgos y que, ante una misma entrada, generan una misma salida. Todo esto supone un **claro desafío** para las compañías **dentro de sus procesos de gestión de riesgos, operativos, financieros, de marketing o de atención al cliente.** Como ejemplo, derivado del uso de los datos, la calidad de los mismos es clave no solo para poder obtener ventajas competitivas en el mercado sino también para impedir que incurran en graves errores estratégicos y operacionales basándose en datos erróneos.

Dada la magnitud de este desafío, es necesario **conocer muy bien sus virtudes y desventajas,** analizar de forma racional todos los posibles riesgos que este tipo de tecnologías pueden tener, no solo **en los entornos en los que se despliega,** sino también, dada la ingente cantidad de datos que este tipo de tecnología usa para entrenar algoritmos y modelos, en **cómo puede afectar** esto en la salvaguarda de los derechos de los interesados.

Además, la **Comisión Europea** menciona específicamente que un marco regulatorio debería **concentrarse en cómo minimizar los diversos riesgos de daño potencial.** Los principales riesgos están relacionados con:

- La aplicación de normas diseñadas para **proteger los derechos fundamentales** (incluida la protección de los datos personales y la privacidad). Al analizar grandes cantidades de datos, la inteligencia artificial también puede usarse para rastrear y des-anonimizar datos sobre personas, creando nuevos riesgos de protección de datos personales incluso con respecto a conjuntos de datos que per se no incluyen datos personales.
- Las cuestiones relacionadas con la **seguridad y la responsabilidad** (estos riesgos pueden ser causados por fallos en el diseño de la tecnología, estar relacionados con problemas con la disponibilidad y calidad de los datos u otros problemas derivados del aprendizaje automático).

Desafíos y riesgos para las compañías

La importancia de una adecuada gestión de riesgos en los entornos analíticos

En definitiva, es necesario establecer mecanismos de gestión del riesgo que se adecuen a la aparición de estos riesgos emergentes. Como hemos expuesto anteriormente, una de las problemáticas que surge es la validación de los resultados obtenidos de los análisis de los datos o las decisiones tomadas por estos sistemas. El desafío será, por tanto, el cómo demostrar a terceros que dichos resultados son correctos y apropiados.

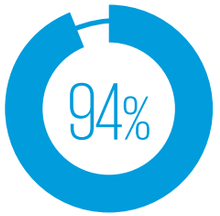
Por ello, debemos reconocer de forma urgente los nuevos perfiles de riesgo y adaptar nuestros enfoques de una manera estructurada. Estas tecnologías requieren implicaciones y replanteamientos en los modelos de gobierno y de control implantados previamente por estas compañías que pueden entrar en conflicto con los anteriores modelos establecidos.

Es vital replantearse el alcance de los objetivos de negocio evitando el conflicto con el cumplimiento, la seguridad de la información y la privacidad de los interesados cuyos datos son explotados. También será importante el aseguramiento de los activos, no de manera individual sino atendiendo también a los entornos, que en muchos casos se encuentran alojados en la nube.

Tener un control sobre los riesgos, unos procesos adaptados y maduros, programas de auditoría y un cuerpo normativo robusto que soporte los entornos de analítica avanzada va a permitir generar confianza en clientes y usuarios, garantizando una mayor y mejor adaptación y aprovechamiento de la tecnología para el beneficio propio.

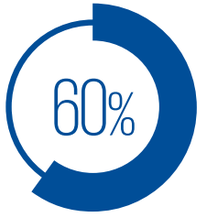
tienen un alto nivel de **confianza** en los análisis de su propia organización.

- KPMG's Guardians of Trust report



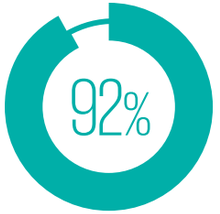
de las empresas creen que los **algoritmos de IA son clave** para obtener una ventaja competitiva.

- IDC



ven **restricciones regulatorias** como una barrera para implementar algoritmos de IA.

- BM IBV AI 2018



cuestionan la **fiabilidad** de los datos, la analítica... se preocupan por el impacto en la **reputación.**

- KPMG's Guardians of Trust report

Enfoque de KPMG

Desde KPMG conocemos bien esta situación a la que miles de compañías se enfrentan día a día, por ello, hemos definido una **estrategia global en la gestión de riesgos,** con la cual venimos ayudando a nuestros clientes.

En este sentido, hemos creado un Marco de Control o **Framework y una Metodología para la gestión del riesgo en este tipo de entornos,** basado en las mejores prácticas y principales estándares de mercado y apoyado en las herramientas que ponen a nuestra disposición las distintas Agencias y Organizaciones especialistas en materia de Protección de Datos y Seguridad de la Información, lo que nos va a permitir un adecuado tratamiento del riesgo para garantizar unos niveles de protección adecuados.

Este Framework ha contado para su desarrollo con las **fuentes de datos más fiables en la materia,** con herramientas y documentación adicional de entidades expertas en su campo de actuación como puede ser la **Agencia Española de Protección de Datos (AEPD)** en aspectos de Privacidad, o la **Enisa** en materia de Seguridad de la Información, sin excluir a otras Organizaciones con gran peso en ambos ámbitos.

Framework de Control

El Marco de Control o Framework que KPMG ha diseñado para la gestión del riesgo en este tipo de entornos contiene **una serie de controles a realizar en cada fase** de un entorno analítico.

Por tanto, **KPMG revisará la seguridad y privacidad en los entornos analíticos en todo el ciclo de vida de los mismos *(end-to-end),*** el cual es el siguiente:

Entornos analíticos

1. Análisis

Primera fase de análisis para valorar los aspectos a los que debe dar respuesta nuestra solución. Durante esta fase se ponen los **cimientos de la Estrategia y el Gobierno** que acompañarán a nuestro proceso durante todo su ciclo de vida.

No solo es necesario establecer un buen gobierno en la solución, también es el momento de **definir los requisitos funcionales y de Seguridad y Privacidad.**

2. Desarrollo

Durante la fase de Desarrollo, se empiezan a **elaborar los modelos y algoritmos necesarios para el tratamiento de la información.** Estos modelos deben desarrollarse en base a metodologías de **Desarrollo Seguro** y en base a las mejores prácticas de mercado.

Modelado de los datos **y entornos no preproductivos.**

Identificación de flujos de datos entre capas de la solución.

3. Retirada

Durante la fase de explotación, hay que garantizar que tanto la solución, algoritmos y modelos se usan para los fines para los que fueron desarrollados, así como que la **arquitectura sobre la que se despliega la solución es correctamente operada,** garantizando en todo momento la confidencialidad, integridad y disponibilidad de la información.

4. Explotación

Una vez se decide no dar continuidad al proceso del entorno analítico, debe hacerse un correcto tratamiento de los soportes y fuentes de datos que se han usado para entrenar y modelar la solución.

Es necesario garantizar **un correcto borrado de los soportes y de la información alojado en ellos,** de tal manera que se cumpla con la legislación vigente en protección de datos.

Enfoque metodológico

Para nuestro enfoque metodológico, es muy importante ir de la mano del equipo conocedor del entorno desde sus inicios, por ello, nuestros **expertos en analítica de datos** forman parte del equipo en todas las fases de nuestro trabajo.

Por todo esto, el enfoque integral para la gestión de riesgos en entornos tecnológicos desarrollado, engloba **los 3 diferentes ámbitos en los que un sistema o proceso puede verse comprometido:**

Marco de Gobierno

- El desarrollo de algoritmos en los últimos años ha avanzado mucho más rápido que el control de los mismos.
- Además de extender el marco de gobierno habitual de la compañía de aquellos procesos más tradicionales, es necesario considerar nuevos riesgos y retos.
- El control de los algoritmos exige nuevos skills y nuevas técnicas.

Modelos matemáticos y algoritmos

El perfil de riesgo de los modelos marca el nivel de control requerido para cada uno de ellos para responder a cuestiones como:

- Sobreajuste de datos
- Métricas inexactas
- Datos de entrenamiento erróneos o comprometidos
- Precisión de los modelos y su evolución
- Variables significativas de los modelos
- What if escenarios

Seguridad y privacidad

Los legisladores, los tecnólogos y las empresas se enfrentan al reto de garantizar que los consumidores tengan el suficiente control sobre sus datos para prevenir el uso indiscriminado de estos a la vez que se mantiene su utilidad para extraer conocimiento, patrones y, en resumen, valor.

- Seguridad del entorno
- Privacidad desde el diseño
- Cumplimiento RGPD
- Análisis de vulnerabilidades del entorno

Fases del trabajo

El equipo de expertos de KPMG ha definido un **enfoque ágil y estructurado para la evaluación de la Seguridad y la Privacidad en entornos de analítica avanzada,** que se adapta de manera flexible a las necesidades y grado de madurez de cualquier compañía en el punto de partida.

Esta metodología consta de **5 fases** en los que se evaluará la situación en la que se encuentra la compañía y cómo deberá alcanzar el "To-Be" deseado:

1. Inicio

Identificación de stakeholders, obtención de un **entendimiento de alto nivel,** definición de expectativas y responsabilidades y definición del **plan de proyecto.**

2. Entendimiento 'as-is'

Revisión de capacidades

Comprender la **estrategia analítica** y el portfolio digital de la empresa, revisar la **gobernanza de datos** y evaluación de capacidades internas en términos de habilidades y tecnología.

Revisión de datos y modelos

Revisión detallada de **calidad de datos, algoritmos utilizados** y el modelo de despliegue analítico utilizado, respaldado por herramientas.

3. Definición de datos y modelos

(Re) definición de las **prioridades estratégicas** y el estado "futuro" para las áreas de gobierno, datos, habilidades, procesos, tecnología. Documentación y cuantificación de **gaps.**

4. Plan de acción y road map

Priorizar el plan de acción en función de viabilidad y valor; Validación de la **hoja de ruta** con las partes interesadas.

5. Close the gap

Apoyo en la implementación

Según necesidades; a modo de ejemplo: apoyo en la definición del **plan de implementación** o ayudar a modificar la solución analítica para cumplir con los requisitos definidos.

Servicios gestionados

Proporcionar un servicio gestionado para el total o parte de la solución analítica o un servicio de **monitorización continua** para verificar su efectividad y cumplimiento.

KPMG: Experiencia y Garantía

¿Qué te aportamos?

Gracias a KPMG y a su amplia experiencia en este tipo de proyectos, podrás obtener los siguientes beneficios:

- **Credibilidad en el uso de analítica de datos.**
- **Control en la Seguridad y Governance de los datos.**
- **Reputación positiva en el mercado.**
- **Prevención de brechas de seguridad.**
- **Control sobre el diseño, verificando que los algoritmos se alinean a los principios y estándares de referencia.**
- **Mayor control / gestión del riesgo.**
- **Precisión de modelos y procesos.**
- **Servicio de monitorización continua para verificar efectividad y cumplimiento.**
- **Seguridad y Privacidad desde el Diseño.**

Control del riesgo en entornos analíticos

KPMG: Experiencia y Garantía

¿Qué te aportamos?

Contamos con la experiencia suficiente para darte la confianza y confortabilidad a la hora de acompañarte durante todo el proceso de gestión de riesgos:

Nuestras recomendaciones se basan siempre en un análisis de las necesidades de nuestros clientes para recomendar las soluciones que mejor se puedan adaptar.

Contamos con una larga historia y experiencia en auditoria y evaluación de riesgos para implementar un modelo de gobierno adecuado.

Contamos con un equipo de profesionales especializados en seguridad de aplicaciones, protección de entornos, accesos, privacidad y en analítica de datos que pueden acompañarlos en todo el proceso.

Proporcionamos la gama completa de servicios: marcos de gobierno generales, análisis en profundidad de algoritmos y seguridad y privacidad.

Numerosas certificaciones y referencias de empresas líderes en el mundo.

Utilizamos un enfoque comercial y de negocio para evaluar la calidad y adecuación de las decisiones de los algoritmos.

Foco en la transformación de las funciones de auditoría y control interno, riesgos y compliance a través de herramientas tecnológicas de última generación.

Contacta con nosotros

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

Rafael Tejedor
Director, Gobierno, Riesgo y Cumplimiento
KPMG en España
T: +34 686 39 27 90
E: rtejedor@kpmg.es

Jose Luis Palermo
Director Lighthouse
KPMG en España
T: +34 690 92 19 07
E: joseluispalermo@kpmg.es

kpmg.es