PwC Digital Trust Insights 2024: Conclusiones de la encuesta mundial sobre el presente y futuro de la ciberseguridad

PwC Digital Trust Insights 2024 es una encuesta realizada por PwC entre junio y julio de 2023 en 71 países, incluyendo España, que recoge las respuestas de 3.876 CISOs, CEOs y ejecutivos del C-Suite en los ámbitos de Seguridad, IT y Negocio. El 67% de los ejecutivos encuestados pertenecen a grandes compañías con ingresos mayores de 1.000 millones de euros. Del total de participantes, 1.250 forman parte de empresas europeas, siendo 143 de ellos, miembros de compañías ubicadas en España.

Nos encontramos inmersos en un escenario de reinvención y transformación de los negocios, originado en gran parte por el desarrollo de nuevas capacidades soportadas en tecnologías disruptivas. Al mismo tiempo, el incremento masivo y dependencia de soluciones tecnológicas están transformando el perfil de ciberriesgo de las organizaciones.

Los resultados de nuestra encuesta 'PwC Global Digital Trust Insights 2024', muestran que la ciberseguridad continúa siendo, ahora más que nunca, una prioridad para los líderes de las organizaciones. Las amenazas e incidentes de seguridad continúan en aumento con respecto a años anteriores, al igual que siguen creciendo las inversiones en ciberprotección. No obstante, aún queda trabajo por delante para abordar los retos actuales, donde la involucración y coordinación de la Alta Dirección y el C-suite para integrar la ciberseguridad en el modus operandi de las organizaciones, resulta clave para afrontar las amenazas presentes y futuras.

¿EN QUÉ PUNTO NOS ENCONTRAMOS?

Aún queda un largo camino por recorrer

Según los directivos encuestados, aunque las expectativas e inversiones en ciberseguridad aumentan, su percepción es que la mejora real de la seguridad tiene aún mucho camino por delante. Un escenario de transformación digital como el actual, en el que la tecnología ya forma parte del *core* del negocio, requiere que, para protegerlo, la ciberseguridad progrese y evolucione de forma efectiva en consonancia a la adopción de nuevas capacidades e infraestructuras tecnológicas y las amenazas crecientes que llevan aparejadas.

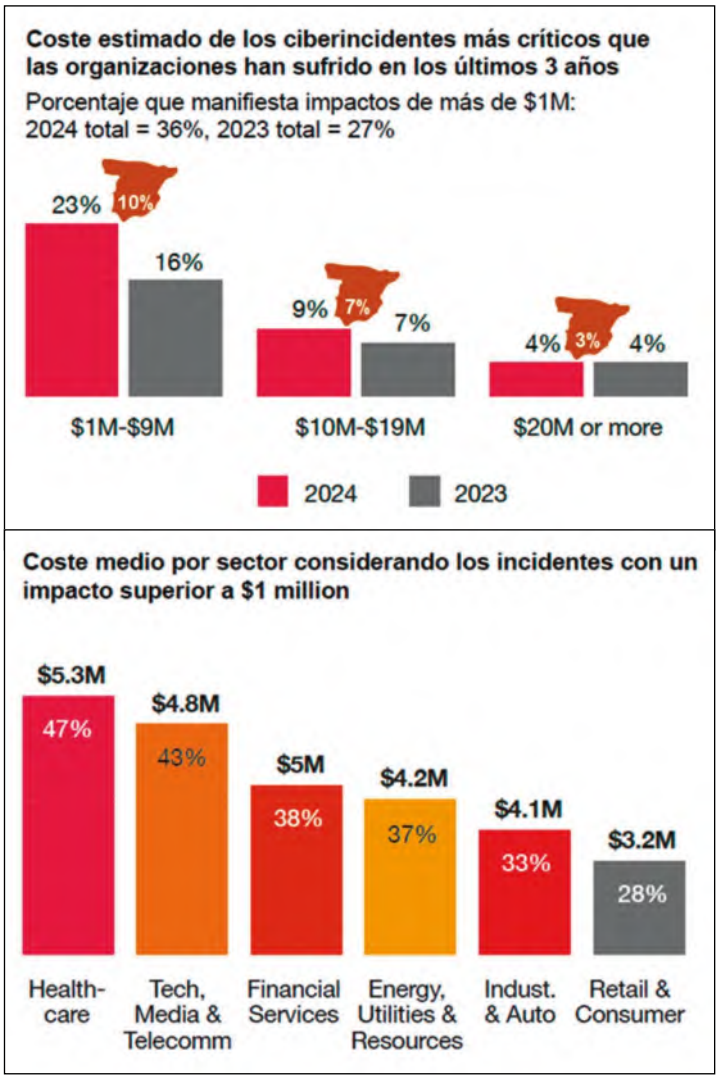

Figura 1.- Coste estimado originado por ciberincidentes en los últimos 3 años.

Los ciberincidentes siguen aumentando en volumen, sofisticación e impacto...

Tanto el número de ciberincidentes como el impacto económico que ocasionan a las organizaciones ha vuelto a crecer un año más, con ataques sofisticados en los que una vez que el atacante penetra en el entorno de la organización, suelen causar estragos de todas las formas posibles. Es decir, lo que puede comenzar como una brecha en la nube podría convertirse en una amenaza persistente avanzada, incluso si se paga el rescate.

El porcentaje de los encuestados que manifiesta haber sufrido ciberataques con impacto económico superior al millón de dólares en los últimos 3 años se ha incrementado al 36% (20% en España), desde el 27% del año pasado.

...Pese a presupuestos, inversiones en ciberseguridad en aumento...

Los ejecutivos de nuestro estudio manifiestan no estar frenando el gasto en ciberseguridad, sino que la inversión está aumentando en ratios superiores a los de años anteriores. De hecho, tal y como se detalla en la **Figura 2**, el 81% de los encuestados (82% en España) afirman que incrementarán su inversión en ciberseguridad en 2024 (frente al 64% del año pasado).

Las partidas a las que más organizaciones dedican sus inversiones se orientan a la modernización y optimización tecnológica, si bien en España, las organizaciones también consideran como área de inversión prioritaria la mejora de su postura ante el ciberriesgo, así como el cumplimiento regulatorio.

En relación con la proporción de la inversión en ciberseguridad respecto a la de tecnología, las inversiones en ciberseguridad también representan este año una mayor proporción respecto al presupuesto total de IT y OT, con un aumento medio global del 14% en 2024 frente al 11% de 2023.

...Pero con planes de ciberresiliencia aún insuficientes

Un aspecto clave como es la definición y puesta en marcha de un adecuado plan de resiliencia y respuesta ante incidentes es otro de los puntos destacados que actualmente se considera que no está avanzando con la velocidad que debería, dado el contexto presente. Actualmente, sólo el 2% de las organizaciones manifiesta estar en fase de optimización y mejora continua de su plan de resiliencia en todos los ámbitos clave del mismo.

Muchas organizaciones abordan aún la gestión del riesgo con una perspectiva basada en

silos, que trata el perfil de riesgo de cada unidad de negocio. La gestión de riesgos interrelacionados y complejos como los ciberriesgos, requiere que la Alta Dirección aborde la resiliencia y gestión del riesgo con una visión integral, tal y como ya vienen proponiendo los nuevos requerimientos de regulaciones como DORA (*Digital Operational Resilience Act*).

LA NECESIDAD DE EVOLUCIONAR EL 'CYBER AS USUAL'

¿Por dónde empezar?

Al igual que los negocios se encuentran en plena evolución y transformación, los resultados analizados de la encuesta *Global Digital Trust Insights 2024,* evidencian que una gran parte de las organizaciones siguen atrapadas en el *cyber as usual*.

Iniciativas fragmentadas y poco cohesionadas, complejidades tecnológicas en constante expansión, proyectos que no se traducen en mejoras reales y planes de gestión de riesgos que suponen, en ocasiones, un riesgo en sí mismo, son algunos de los escollos que siguen obstaculizando el camino hacia una ciberseguridad realmente confiable.

En la **Figura 4**, se muestran las principales iniciativas que, según la visión de los directivos encuestados, podrían suponer un cambio a la hora de hacer ciberseguridad, y servir de referencia junto a las siguientes para dar un paso más allá del *cyber as usual*:

- **Llegada al negocio con el uso de lenguaje común.** Es preciso llegar a los responsables de los negocios eliminando barreras mediante el uso de un lenguaje común que informe, atraiga y sea capaz de trasladar los riesgos que conlleva el uso de la tecnología y sus impactos.
- **Diseño de nuevas iniciativas para la gestión del ciberriesgo** con la búsqueda de amenazas específicas para el sector, la visión y la estrategia de la organización, planes para que la organización sea capaz de identificar el ciberriesgo de forma proactiva contribuyendo a generar una cultura del riesgo, así como nuevas formas de encontrar y reforzar puntos débiles, con iniciativas de recompensa por la identificación de fallos de seguridad.
- **Involucración desde la estrategia** que permita a la organización involucrarse con el regulador o grupos de trabajo en la generación de normas y requerimientos en ámbitos disruptivos (IA, metaverso, criptomonedas, etc.) de forma que impulsen y no obstaculicen la evolución del negocio.
- **Asignación a los equipos de tareas de valor,** liberando a los equipos de ciberseguridad de las tareas más rutinarias y automáticas mediante procesos automáticos o servicios gestionados con el objetivo de centrar su actividad en tareas de valor con el conocimiento de la organización (análisis de amenazas, desarrollo de técnicas de protección innovadoras, etc.)
- **Incorporación de la ciberseguridad en la agenda del Consejo de forma regular.** La ciberseguridad y gestión del ciberriesgo encabezan la lista de mayores preocupaciones de los Consejos, pero tan solo el 56% de los encuestados (52% en España) reconoce que la Alta Dirección de su organización es informada con frecuencia de la evolución de la exposición al ciberriesgo y cómo este es mitigado. La transformación del negocio va unida a la transformación de la ciberseguridad, que involucra a toda la organización y puede resultar un aspecto diferencial para el crecimiento del negocio. La consideración del ciberriesgo como un riesgo más del negocio y la atribución de la responsabilidad del ciberriesgo a la Alta Dirección, resultan claves para llevar la ciberseguridad y ciberriesgo a la agenda del Consejo.

	Global (3876)	Western Europe (1250)	España (143)
Net Crecimiento	80%	80%	83%
Net Disminución	5%	6%	4%
Crecimiento 15% o más	10%	9%	8%
Crecimiento 11-14%	16%	16%	19%
Crecimiento 6-10%	31%	30%	29%
Crecimiento 5% o menos	24%	25%	26%
Sin cambios	9%	9%	10%
Disminución 5% o menos	2%	3%	1%
Decrease by 6-10%	2%	2%	3%
Decrease by 11-14%	1%	1%	0%
Decrease by 15% or more	0%	0%	0%
Cannot determine at this time	3%	3%	3%
I don't know	2%	2%	1%

Figura 2.- Previsión de crecimiento del presupuesto de ciberseguridad de las organizaciones para 2024.

	GLOBAL	EUROPA OCCIDENTAL	ESPAÑA
Evolución/Actualización de la tecnología incluyendo infraestructura ciber	49%	53%	42%
Optimización de la tecnología e inversiones actuales	45%	46%	44%
Mejoras en la gestión de ciberriesgos basadas en el roadmap de ciberseguridad	42%	43%	44%
Formación en ciberseguridad	40%	41%	36%
Cumplimiento normativo y regulatorio	31%	32%	44%

Figura 3.- (Respuesta múltiple) Principales partidas del presupuesto de ciberseguridad.

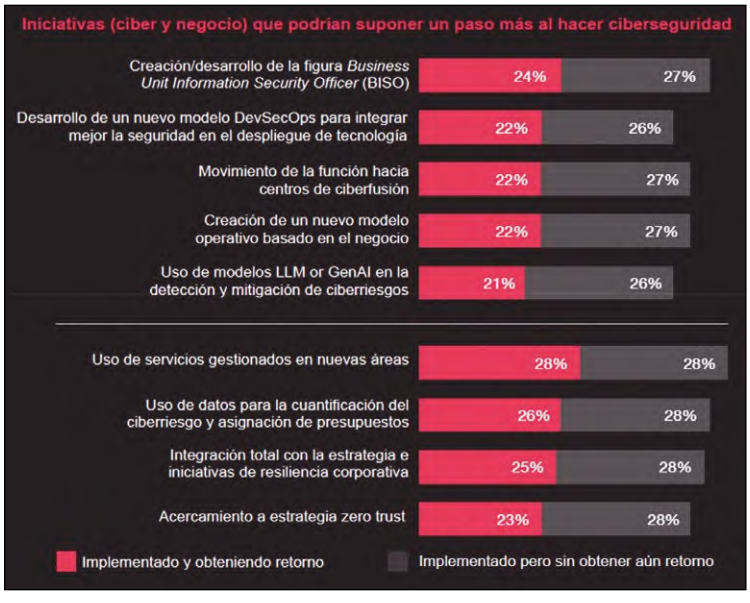

Figura 4.- (Respuesta múltiple) Propuesta de iniciativas que podrían suponer una evolución del cyber as usual.

¿Cómo están trabajando los alumnos aventajados?

Aunque nos encontramos lejos de que las organizaciones sitúen la seguridad en el epicentro de la innovación, 'Global Digital Trust 2024' ha querido poner de manifiesto las iniciativas de ciberseguridad, en las que está trabajando el 5% de los encuestados (*top performers*) que sí lo hacen y que, por sus respuestas, obtienen un mejor valor y retorno de la ciberseguridad al ir más allá del *cyber as usual*. La función de ciberseguridad de estos *top performers*, es capaz de:

- Detectar, responder rápidamente y salir fortalecidos ante las amenazas.
- Incorporar la seguridad y privacidad en productos, servicios y relaciones con terceros.
- Establecer controles de ciberseguridad en toda la organización.
- Asignar el presupuesto de ciberseguridad a la mitigación de los principales ciberriesgos, los cuales han tenido que ser previamente evaluados para su priorización.
- Mantener la relación con organismos públicos para aumentar la resiliencia y mejorar la respuesta ante incidentes.
- Colaborar con áreas del negocio cuyo trabajo afecta a la postura ante el ciberriesgo de la organización (por ejemplo, ingeniería de software, adquisiciones, etc.).
- Comunicar la estrategia y prácticas de ciberseguridad para ga-

narse la confianza de clientes, accionistas y socios comerciales.
• Acelerar la transformación digital y el diseño de la seguridad y la privacidad *by design* en nuevos procesos, productos y servicios.
• Aportar a la Alta Dirección el entendimiento y evaluación sobre la exposición al ciberriesgo, anticipar futuros ciberriesgos y proporcionar el soporte con las medidas para su mitigación.

PRINCIPALES PUNTOS DE ATENCIÓN PARA 2024

Del análisis de las respuestas obtenidas en nuestro estudio, a continuación, se destacan de forma agrupada, los cinco ámbitos clave en los que las organizaciones deberían poner foco para afrontar de manera exitosa la gestión de ciberriesgos y su ciberseguridad:

1. Focalización en la gestión del ciberriesgo y riesgos tecnológicos. Una adecuada gestión del ciberriesgo, trasciende más allá del ámbito puramente técnico e involucra como responsables al Consejo, Comité de Dirección y a las direcciones de los diferentes negocios, soportadas por las áreas de IT y Seguridad.

De entre los riesgos prioritarios a los que se enfrentan las organizaciones a todos los niveles, el 43% de los encuestados (56% en España) posiciona los ciberriesgos entre las principales prioridades para 2024, solo por detrás de los riesgos tecnológicos (51% de los encuestados a nivel global y 53% en España), ligados a su vez al ciberriesgo. Para su mitigación, una adecuada gestión, tiene que saber evaluar los riesgos para abordar prioritariamente los más relevantes.

En el contexto actual, la reinvención del negocio o transformación digital no se entiende sin considerar conjuntamente la ciberseguridad. Los ataques a la nube y a los dispositivos conectados son las ciberamenazas que más preocupan a nuestros encuestados, dos tecnologías que se encuentran en el centro de la transformación actual de los negocios, y que, como nuevas amenazas, deben ser incorporadas en el marco de gestión del riesgo junto a los procesos de tratamiento de sus riesgos y responsables.

2. Gestión de la seguridad en la nube: preocupa ¿y ocupa?

La masiva adopción de operativas y plataformas *cloud* está permitiendo abordar nuevos modelos de negocio, nuevas formas de trabajar en las que la ubicación geográfica ya no es un impedimento o conectar tecnologías en favor de mejores servicios a clientes y usuarios, operativa o capacidad de gestión, etc.

Figura 5.- (Respuesta múltiple) Ciberamenazas que más preocupan en las organizaciones en los próximos 12 meses.

Figura 6. Abordaje de retos cloud - proveedor de servicios cloud.

Consecuentemente, la seguridad en la nube, es para el 47% de los participantes en el estudio (43% en España), la principal preocupación en materia de ciberriesgos (54% en el caso del 42% de organizaciones con entornos *cloud* híbridos). Esto es así dado los numerosos vectores de ataque posibles, que obligan a las organizaciones a establecer controles en múltiples ámbitos: identidad y acceso, movimientos laterales, cuentas de correo electrónico, portales web, aplicaciones, información protegida, interacciones con los clientes, sistemas operativos, dispositivos conectados, y un largo etcétera. Igualmente, el *cloud security* se posiciona para el 33% (35% en España) como uno de los principales ámbitos de inversión para el próximo año.

Pese a ello, casi todas las organizaciones encuestadas (97%) reconocen contar con importantes aspectos de mejora en su plan de gestión de riesgos de la nube, de tal forma que tan sólo el 3% mantiene implementado y actualizado un plan integral de gestión de seguridad *cloud* que aborde las nueve áreas de seguridad de la nube incluidas en el gráfico de la *figura 6*. En dicho gráfico se puede apreciar el elevado porcentaje de organizaciones que aún no han abordado los principales retos de seguridad en la nube.

3. Uso de la IA generativa en ciberdefensa. El 69% de los participantes (61% en el caso de España) en el *Digital Trust Insights 2024*, afirma que su organización prevé utilizar IA generativa (GenAI) en el próximo año enfocada a ciberdefensa, con el objetivo de ayudar en la gestión de la ciberseguridad ante el aumento del número y complejidad de los ciberataques.

Muchas plataformas están ofreciendo sus LLM (*Large Language Models*) con sus soluciones tecnológicas de ciberseguridad, si bien **podría** pasar algún tiempo antes de que veamos un uso eficaz a gran escala de las GPT (*Generative Pre-trained Transformer*) en términos de ciberdefensa. Mientras tanto, destacamos los tres ámbitos de aplicación más prometedores para el uso de GenAI en ciberdefensa, según nuestros encuestados.

• **Detección y análisis de amenazas**. La GenAI puede resultar muy valiosa para la detección proactiva de vulnerabilidades, la rápida evaluación de su alcance (qué está en riesgo, qué está ya comprometido y cuáles son los daños) y la

posterior presentación de diferentes alternativas probadas para la defensa y la remediación. GenAI puede ayudar a identificar patrones, anomalías e indicadores de compromiso que eluden los sistemas tradicionales de detección.

• **Generación de informes sobre ciberriesgos e incidentes**. GenAI también podría simplificar la notificación y reporting de incidentes y ciberriesgos. Con la ayuda de NLP (*Natural Language Processing*), puede convertir datos técnicos en contenidos concisos que resulten entendibles incluso para personas sin conocimientos técnicos y ayudar a elaborar informes de respuesta a incidentes, inteligencia sobre amenazas, evaluaciones de riesgos, auditorías y cumplimiento normativo, presentando recomendaciones en términos que cualquiera pueda entender.

• **Aplicación y actualización de controles**. La seguridad de la nube y los sistemas de la cadena de suministro requieren de constantes actualizaciones en las políticas y controles de seguridad. Los algoritmos de aprendizaje automático y las herramientas GenAI pronto podrían recomendar, validar y perfilar políticas de seguridad, así como automatizar la configuración y actualización de controles adaptados al perfil de amenazas, tecnologías y apetito al riesgo de la organización.

El reto ahora para los directivos es cómo adoptar estas herramientas de forma ética y responsable y controlar a su vez los riesgos subyacentes. La GenIA aporta al mismo tiempo capacidades en el lado defensivo, pero también supone una amenaza empleada desde la posición del atacante. De hecho, el 52% de los encuestados considera que la IA contribuirá al desarrollo de ciberincidentes de alto impacto en los próximos meses.

Por ello su adopción debe estar sujeta a reflexión e incorporada al plan de ciberriesgos de las organizaciones. Actualmente, tan solo el 19% (24% en España) de los directivos manifiesta no sentirse cómodo desplegando herramientas IA antes de contar con las regulaciones y políticas internas correspondientes al respecto.

Figura 7.- Estimación de uso y retorno de valor de GenAI.

Figura 8.- (Respuesta múltiple) Principales tipos de regulación con impacto en crecimiento futuro del negocio.

4. Simplificación a la hora de proteger. El **reto** para las organizaciones no es tanto la falta de herramientas o inversión en ciberseguridad, sino cómo obtener valor y beneficio real de la ciberseguridad y su aprovechamiento. En ocasiones la complejidad de la arquitectura tecnológica y el conjunto de herramientas utilizadas hace demasiado complicada la protección de las organizaciones, por lo que la inversión en ciberseguridad puede no resultar efectiva en todos los casos.

De hecho, el 49% de los líderes encuestados (42% en España) seleccionaron la modernización tecnológica, incluida la infraestructura ciber, y el 45% (44% en España) la optimización de tecnologías e inversiones existentes, como las mayores prioridades de inversión en ciberseguridad para 2024.

En los últimos años, los directivos encuestados han trasladado su preocupación respecto a que sus organizaciones se hubieran vuelto demasiado complejas como para contar con una protección eficaz. Este año, el 44% de los participantes en la encuesta afirma utilizar ya un conjunto integrado de soluciones ciber, y el 39% planea migrar a uno en los próximos dos años. El exceso de soluciones específicas puede ser una de las razones por las que sólo la mitad de los encuestados afirma estar "muy satisfecho" con las capacidades tecnológicas de sus soluciones de ciberseguridad, ya que las herramientas que no proporcionan soluciones integrales pueden obstaculizar el rendimiento, requerir más tiempo de gestión e impedir la visión global, esencial para gestionar el ciberriesgo.

5. Cumplimiento normativo: nuevos retos. Aproximadamente un tercio de los encuestados de este año coincide en que cumplir con los requisitos normativos puede convertirse en una ventaja competitiva y señalan los siguientes tipos de regulación como los que pueden tener mayor impacto en el crecimiento futuro de su organización: la regulación de la IA (37%), la armonización de las leyes de ciberseguridad y protección de datos (36%), el reporting obligatorio en torno a la gestión, estrategia y gobierno del ciberriesgo (35%) y los requerimientos sobre la obligatoriedad de establecer planes de respuesta ante incidentes o resiliencia operativa (32%).

El incremento de las sanciones, las penalizaciones y cargas penales a la Alta Dirección y transparencia, son algunos de los factores comunes presentes y futuros en el ámbito regulatorio. En este sentido, las nuevas normas de la SEC, por ejemplo, exigen la divulgación pública de los ciberincidentes que puedan tener un efecto material en los inversores y en el horizonte se vislumbran normativas que regularán la inteligencia artificial, como la Ley de Inteligencia Artificial de la UE. ■

De un vistazo

- Aunque las **expectativas e inversiones en ciberseguridad aumentan** a mayor ritmo que años anteriores, los ciberriesgos y riesgos tecnológicos continúan siendo los que más preocupan a las organizaciones, siendo **oportuno adoptar medidas innovadoras** más allá del *cyber as usual*.
- Tanto el **número de ciberincidentes como su impacto económico han vuelto a crecer** un año más, mientras que la adopción de planes de respuesta a incidentes y resiliencia por parte de las organizaciones evolucionan de forma más contenida.
- La **seguridad en la nube es la principal preocupación en materia de ciberriesgos**. Sin embargo, la gran mayoría de las organizaciones reconoce gestionar estos riesgos de forma insuficiente.
- La revolución de la **IA generativa aporta expectativas en las mejoras de ciberseguridad para la mayoría de los encuestados**, pero también requiere un análisis de uso ético y responsable, así como de control de los riesgos subyacentes.
- Las organizaciones continúan **preocupadas por tener que proteger entornos demasiado complejos**, por lo que tienden a **simplificar sus herramientas ciber** de forma que proporcionan soluciones integrales de ciberseguridad.
- Los **nuevos retos normativos** pasan por la regulación de la IA, la armonización de las leyes de ciberseguridad y protección de datos, el reporting de la gestión del ciberriesgo, el establecimiento de planes de resiliencia y la transparencia, todo ello con el incremento de las sanciones, penalizaciones y cargas penales a la **Alta Dirección.**

** El informe PwC Global Digital Trust Insights 2024 se encuentra disponible en* https://www.pwc.es/bss

JULIO CASTILLA
Director
Business Security Solutions
PwC España