

TENDENCIAS TECNOLÓGICAS PARA EL AÑO 2024

Introducción

2024 se presenta como un año lleno de oportunidades donde tecnologías que han ido cobrando protagonismo durante los últimos meses van a ocupar un mayor espacio en las operaciones diarias de las organizaciones. El impacto que van a experimentar quienes decidan apostar por estas tecnologías les permitirá situarse como los auténticos líderes en sus sectores.

Desde Grupo Oesía hemos querido dividir estas tendencias tecnológicas en **cuatro grandes áreas, de acuerdo con nuestros centros de competencias: Simulación, Cloud, Ciberseguridad e Inteligencia Artificial**. Lógicamente, estas tecnologías no funcionan como silos independientes, sino que poseen vasos comunicantes a través de los cuales se nutren unas de las otras, ampliando capacidades y ventajas.

Desde Grupo Oesía esperamos que estas reflexiones contribuyan a que **todas las empresas puedan alcanzar los objetivos que se han marcado para 2024**, a la vez que contribuimos, en términos generales a completar nuestra misión: crear un mundo mejor, más eficiente, seguro y sostenible.

Simulación

Simulación inmersiva: el uso de la Realidad Virtual

La simulación inmersiva permite a sus usuarios adentrarse en espacios digitales gracias al uso de la Realidad Virtual. Gracias a este tipo de simulación **las fronteras entre el mundo físico y virtual se difuminan**, creando experiencias 360 a través del uso de dispositivos que traen un mayor realismo a las interacciones que se producen en este ámbito.

Un factor determinante que permitirá la aplicación de la simulación inmersiva dentro de las empresas es **potenciar el grado de realismo a través de elementos gráficos de alta calidad**. El uso de la realidad virtual inmersiva está ya presente en industrias como la de los videojuegos, en la que sus usuarios están acostumbrados a “entrar” en otros espacios para hacer su experiencia más auténtica. Sin embargo, su potencial va más allá del mundo del entretenimiento, gracias a su capacidad para **crear contextos que suponen retos potenciales que debemos afrontar, pero sin llevar a ningún riesgo físico a sus usuarios**.



Integración de la simulación con la IA

A la hora de crear estos escenarios complejos a los que debemos hacer frente, la simulación cuenta con una gran aliada: la Inteligencia Artificial. Las simulaciones generadas en base a la IA permiten a las empresas **proyectar escenarios donde la rápida toma de decisiones es un factor clave para poder solventar situaciones complejas**, así como **adelantar** cuáles son las **consecuencias** de cada una de estas medidas.

En el ámbito de la fabricación los **gemelos digitales** son un claro ejemplo de cómo usar esta integración. La **creación de maquinaria industrial compleja** es costosa y, por tanto, debemos ser capaces de anticipar al máximo posible su rendimiento bajo determinadas situaciones de estrés y ver así cuál sería el comportamiento que adopta en esas circunstancias especiales.

Simulación computacional

Otra de las maneras a través de las cuales las empresas pueden fomentar el crecimiento de sus negocios es a través de la simulación computacional. El modelado computacional tiene en las matemáticas, la informática o incluso la física unas herramientas de valor incalculable. La reducción de recursos y del tiempo necesario para llevar un producto final al mercado **agiliza de forma considerable los procesos**, impactando en todas las fases de los proyectos.

Pero no solo permite mejorar la producción o ejecución de servicios. La simulación computacional es un **importante factor de seguridad**, ya que permite identificar posibles fallos, anticipar cuál sería su impacto y tomar decisiones para evitar esas situaciones. Esta mayor capacidad de confiabilidad es **muy relevante cuando estamos analizando sistemas altamente complejos con muchos elementos interdependientes**. Contar con análisis previos de posibles situaciones extremas sin tener que esperar a que se produzcan en la vida real puede marcar la diferencia entre superar o no una crisis en nuestra operativa diaria.



Simulación aplicada en el día a día

Pudiera parecer que las empresas solo pueden beneficiarse de la aplicación en sus modelos productivos de diseño. Sin embargo, el potencial de la simulación también puede aplicarse en acciones concretas de nuestro día a día. Por ejemplo, la **educación y formación** de profesionales a través de simuladores tiene una gran importancia en la evolución de profesiones tan diversas como la sanitaria o los agentes de seguridad y defensa.

Otra aplicación práctica de la simulación es la **mejora de la experiencia de los clientes** de una compañía. Como veíamos previamente, al difuminarse las fronteras físicas y virtuales, podemos estar más cerca de nuestros usuarios, sin intrusismo, pero ofreciendo nuevas interacciones personalizadas en base a sus gustos y necesidades. Incluso podemos crear **salas de exposiciones virtuales** para poder mostrar nuestras capacidades sin tener que desplazarnos a una feria, eliminando costes de material, personal y tiempo. Además, las virtual showrooms no tienen limitaciones de fechas o espacios, tenemos más control de lo que podemos hacer y es más fácil de replicar y adaptar para nuestros diferentes públicos.

Cloud

Edge computing

Los usuarios llevan ya años adentrándose en la nube, tanto a nivel personal como profesional. Sin embargo, a veces no somos conscientes de dónde se están procesando los datos a los que estamos queriendo acceder con nuestras interacciones. El objetivo principal del edge computing es **acercar el procesamiento de los datos lo máximo posible al punto de donde se generan, es decir, al usuario.**

La ventaja principal del Edge computing es la **velocidad**. Permite a los usuarios acceder a la información de forma mucho más directa. Además, con el Edge computing conseguimos también **reducir los tiempos de latencia**, es decir, el tiempo de comunicación de ida y vuelta entre el usuario y el servidor. Esta reducción de latencia es clave en situaciones donde se exige una toma ágil y acertada de decisiones. Un escenario militar o un coche conectado necesitan acceso a la información de forma rápida y confiable para poder estar al tanto de cualquier imprevisto que se haya podido producir y ver qué medida es la que corresponde aplicar en un momento concreto.

Serverless computing

Relacionada con el punto anterior, otra de las tendencias que está cobrando un mayor protagonismo es la computación sin servidor. De esta forma **es el proveedor del servicio cloud quien asigna recursos específicos de forma automatizada y dinámica**. Este sistema de trabajo se ajusta al uso real de los recursos, encontrando las empresas un importante **ahorro** en sus operaciones diarias, ya que solo pagan por lo que usan.

La externalización de toda la gestión de la infraestructura cloud también **permite que los desarrolladores de una organización puedan dedicar su tiempo a generar un mayor impacto en el negocio**, ya que les evita tener que hacer frente a tareas rutinarias. Una forma de optimizar los recursos con los que cuentan las empresas, sin necesidad de tener que aumentar sus costes en formación o contratación de profesionales.



Green cloud

Nuestra sociedad es consciente de los retos medioambientales que tenemos enfrente. El acceso a bienes vitales para nuestra subsistencia, como el agua, supone un reto cada vez mayor. No sirve de nada contar con capacidades tecnológicas más avanzadas si acaban reduciendo nuestro acceso a recursos necesarios para nuestra subsistencia. Desde este punto de vista, el green cloud, más que una tendencia, es **una necesidad y una obligación**.

Con green cloud nos referimos a aquellas **medidas y servicios que la tecnología cloud puede ofrecer a las sociedades en términos medioambientales**. Si bien toda infraestructura cloud es beneficiosa, ya que nos ayuda a reducir hardware en nuestras operaciones o reducir los costes energéticos de nuestro día a día, adicionalmente, es conveniente contar con un buen plan de diseño para contar con energías renovables que sirvan de motor a los data center.

Entornos multicloud

En determinadas circunstancias, una empresa puede optar por contar con más de una plataforma de nube, ya sean públicas, privadas o una combinación de ambas. Poder sacar partido a las diferentes ventajas que ofrecen cada una de ellas, a la vez de reducir posibles riesgos a los que nos podemos enfrentar en un entorno cloud, es una **gran ventaja competitiva**. Este uso de dos o más plataformas es lo que se conoce como multicloud.

Con esta estrategia **las empresas evitan la dependencia que puede generar contar con un solo proveedor de aplicaciones en la nube**. Al ser menos vulnerables en términos de dependencia, las empresas también se encuentran en una situación de poder que le permita **negociar de igual a igual tarifas y servicios con sus proveedores cloud**. Además, podemos explotar las fortalezas de cada plataforma en base a las necesidades que nuestras diferentes áreas de negocio requieran en sus operaciones diarias. Toda estrategia que permita a los usuarios contar con una mayor flexibilidad será determinante para poder adaptar sus operaciones a las condiciones cambiantes del mercado.

Ciberseguridad

Seguridad cibernética: la criptografía postcuántica

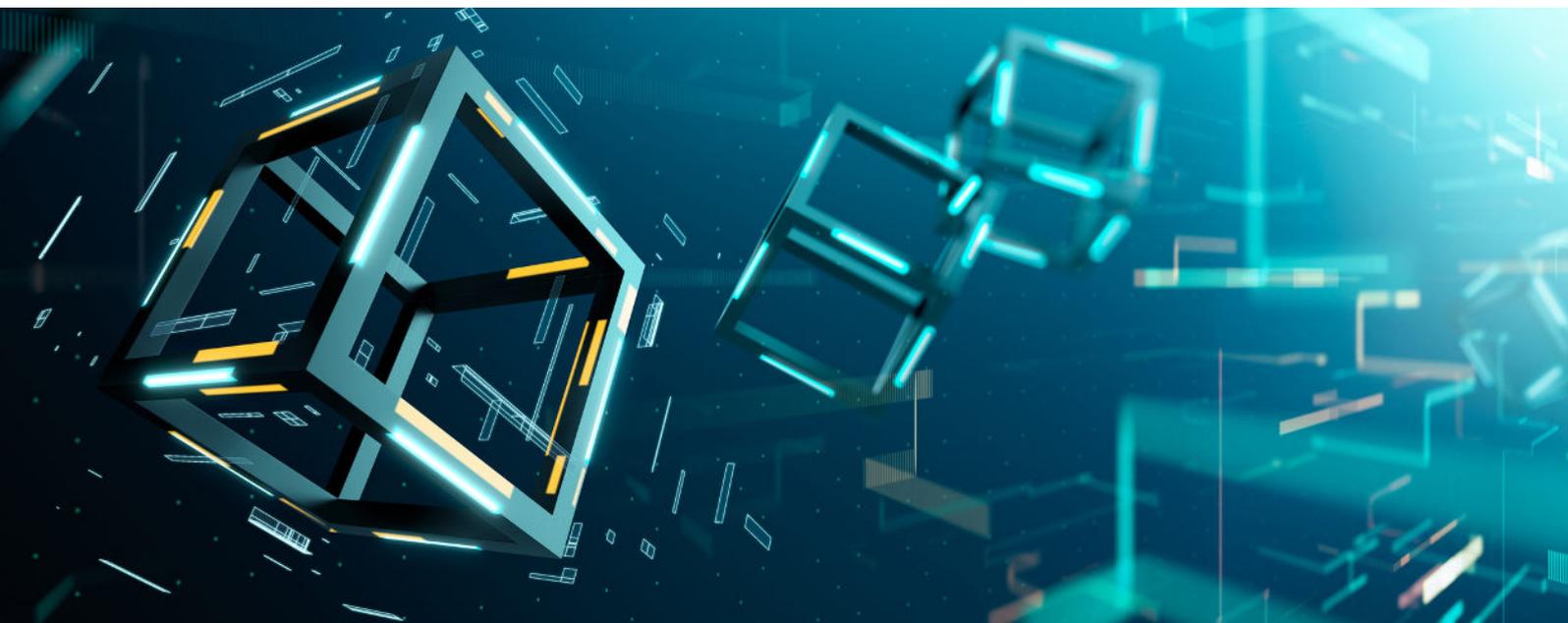
La llegada de los ordenadores cuánticos, basados en el uso de la mecánica cuántica para procesar los datos, ha aumentado nuestras capacidades de forma exponencial, de eso no cabe la menor duda. El reto al que debemos enfrentarnos ahora es **cómo establecer medidas de seguridad frente a unas máquinas capaces de descifrar algoritmos** convencionales que debe proteger nuestra privacidad y nuestra información más sensible.

La criptografía postcuántica se basa en los fundamentos de la física cuántica para garantizar la seguridad de la información. No solo nos permite proteger nuestros datos de una forma más segura. También sirve para garantizar la integridad de nuestra información. La implementación de la criptografía postcuántica **será un paso fundamental en las organizaciones de todo el mundo**. Deberán acometer planes de ejecución en el que van a convivir temporalmente sistemas cuánticos y no cuánticos, con las complejidades que eso implica. Contar con partners de confianza en estos procesos es un factor clave.

Blockchain y seguridad en la cadena de suministro

La digitalización ya está presente en todos los sectores económicos. Por eso las medidas de defensa deben estar presentes en todos sus aspectos para garantizar un correcto funcionamiento de las operaciones. **Uno de los eslabones más sensibles de las operaciones de producción son los relativos a las cadenas de suministro**, cuyo buen funcionamiento es vital para el negocio de cualquier empresa, más bajo el contexto político internacional que está poniendo a prueba el acceso a materias primas y componentes estratégicos.

En la cadena de suministro intervienen un gran número de actores e interacciones, lo cual genera una gran complejidad. La tecnología Blockchain, con su capacidad de registro de las diferentes transacciones que se producen, es una aliada muy importante. **Su capacidad de procesamiento permite identificar si una información se ve alterada ya que deja un registro claro**. Esta transparencia permitirá también una mayor confianza por parte de nuestros clientes en los productos y servicios que ofrecemos.



Seguridad de los puntos finales

El diseño de grandes estrategias de ciberseguridad no debe solo centrarse en cómo poner a salvo toda la infraestructura de una organización. Hay que tomar una clara concepción de que el riesgo tiene una entrada mucho más simple de lo que anticipamos y muchas veces les basta con atacar **las puertas de acceso más débiles: los Endpoints o puntos finales**.

Con puntos finales nos referimos a **cualquier dispositivo de la organización, como un portátil o un teléfono móvil corporativo**. Las empresas deben evaluar los riesgos a los cuales estos terminales se ven expuestos y la sensibilidad de los datos que almacenan. Una vez realizado ese análisis tienen que tomar las medidas que se correspondan en cada caso, como son antivirus, cortafuegos, medidas que prevengan la intrusión y herramientas de detección. Es fundamental **asegurar que los dispositivos mantienen sus softwares actualizados en todo momento y que usan solo software legítimo**.

Estrategia de Zero Trust

Una estrategia importante de cara a poder establecer una estrategia de seguridad de puntos finales efectiva se basa en la **concienciación de los profesionales**. Un concepto clave en esta concienciación es el Zero Trust. Los ataques se han vuelto cada vez más sofisticados y lo que antes era distinguible de forma más evidente ahora ya no es tan obvio. Es decir, tenemos que asumir que **ningún usuario o dispositivo está libre de poder ser atacado o salir indemne ante una crisis de seguridad**.

Un ejemplo de acción de Zero Trust son los **procesos de autenticación exhaustivos** para garantizar que solo acceden a la información sensible las personas que deben hacerlo. No se conceden por tanto autorizaciones por defecto, sino que el contexto cobra importancia. **La inspección continua del tráfico** debe ser otro elemento importante para identificar comportamientos anómalos. Cuanto mayor sea el número de herramientas de monitorización de nuestra actividad en nuestras tareas diarias más fácil será poder descubrir comportamientos no legítimos. Porque solo hay una cosa peor que sufrir un ataque: no ser consciente de que estamos siendo atacados.

Inteligencia Artificial

Aprendizaje por refuerzo aplicado a gemelos digitales

En el apartado de simulación que hemos analizado previamente ya hemos hecho referencia al potencial del uso de la Inteligencia Artificial aplicada a los gemelos digitales. En este punto queremos mencionar un concepto que es clave y que podrá servir de una gran utilidad a una cantidad de organizaciones de diferentes sectores: el aprendizaje por refuerzo.

El aprendizaje por refuerzo **propicia una mejora en el rendimiento a través de una interacción continua**. Las situaciones simuladas de forma constante consiguen ajustar su adiestramiento recompensando o penalizando cada una de las decisiones en tiempo real. De esta forma se **produce un refinamiento en permanente evolución que genera soluciones más flexibles en un menor periodo de tiempo**, abriendo nuevas puertas a la innovación y la eficiencia para las empresas que deciden implantar este tipo de tecnología.

Explainable AI (XAI) / Inteligencia Artificial Explicable

Además de ser capaces de ofrecer respuestas rápidas y precisas, tenemos que poder entender cuál ha sido el proceso que ha llevado a tomar esas decisiones. Frente a las IA tradicionales, que se caracterizan por su opacidad, emerge **la Inteligencia Artificial Explicable (IAE) que pone el foco en los procesos que llevan a las tomas de decisiones.**

Este acercamiento tiene una **doble ventaja**. Por un lado, las empresas son más conscientes de cuáles han sido los mecanismos a través de los cuales se ha llegado a una decisión, generando una **mayor confianza en la tecnología**. Por otro lado, esta transparencia permite un **mayor compromiso ético** de las organizaciones. Su público menos especializado en estos procesos contará con un mayor conocimiento de sus procesos, y podrá corroborar que no se ha producido sesgo derivado de algún tipo de discriminación oculta.



IA aplicada al Reclutamiento

Uno de los grandes retos a los que se deben enfrentar las empresas es la captación de talento. La dificultad creciente para conseguir algunos perfiles tecnológicos puede lastrar las operaciones de una compañía, impactando de forma determinante en sus resultados financieros. Sin embargo, los departamentos de Recursos Humanos van a encontrar en la Inteligencia Artificial un nuevo aliado para **poder identificar, atraer y captar talento**. Y todo ello **de una forma mucho más eficiente**.

La IA puede involucrarse desde su fase más temprana como es el caso del **filtrado de CVs**, labor que en muchos casos supone una pérdida de tiempo muy valioso para los reclutadores. Más allá de estas labores más tediosas o administrativas, pueden implementarse otras técnicas más novedosas como la **realización de entrevistas virtuales** que permita analizar las respuestas de los candidatos e incluso realizar evaluaciones de competencias técnicas. El uso de IAs en una organización, en general, la hace más atractiva para sus trabajadores y contribuirá a disminuir el número de profesionales que la abandonan por otras organizaciones.

La IA como herramienta colaborativa

La Inteligencia Artificial ha pasado ya a la cotidianeidad de las operaciones de cualquier empresa. Poco a poco se ha ido integrando en los procesos de trabajo de las compañías, consiguiendo redefinir la relación con nuestro trabajo y la forma en la que llevamos a cabo nuestras tareas, también, con otros profesionales de nuestras organizaciones. Ya solo la posibilidad de **eliminar del trabajo en equipo las tareas más rutinarias permite eliminar un posible conflicto entre trabajadores.**

Otra forma de facilitar la colaboración es el **procesamiento del lenguaje natural con una evaluación constante de la comunicación entre los trabajadores** identificando patrones y dinámicas que permitan a los equipos ser más eficientes. Entre otras labores, puede **asignar los recursos más idóneos de una forma objetiva en base a los resultados que se quieren obtener**, eliminando decisiones arbitrarias que pudieran afectar al desarrollo de un proyecto. Este horizonte de expectativas más ajustado redundará en un **equipo mejor cohesionado y con un mejor ambiente laboral**. En definitiva, una gran herramienta para todas aquellas empresas que quieran fomentar una cultura de colaboración en sus equipos.



Por

Arnaud Marivain

Partner y

Global Digital Director

en Grupo Oesía



Crear un mundo mejor,
más eficiente, seguro y sostenible

grupooesia.com

