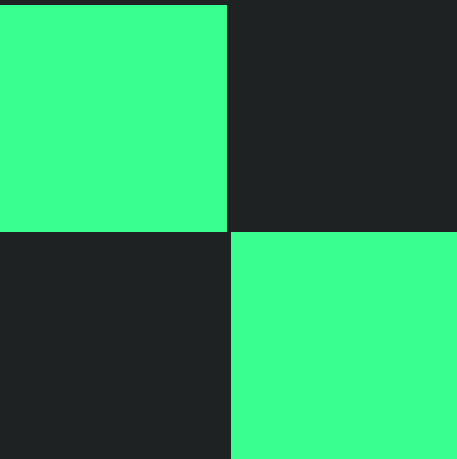


# [LA\_TECNOLOGÍA QUE\_MÁS VALOR:APORTA]

Las 5 tendencias tecnológicas  
que marcarán el rumbo de  
tu negocio en 2024



La inteligencia artificial generativa, la estrategia de ciberseguridad que integra detección y respuesta, herramientas para domar el caos multicloud, la identidad digital y la gestión de datos inteligente son las tecnologías clave que permitirán a tu organización ganar eficiencia y competitividad.



# ÍNDICE

<b>[1] Inteligencia artificial: fuerza impulsora de la innovación y la eficiencia</b>	<b>5</b>
<b>[2] Ciberseguridad integral y proactiva: detección y respuesta</b>	<b>11</b>
<b>[3] Herramientas para domar el caos multicloud</b>	<b>16</b>
<b>[4] Gestión de la identidad: imperativo tecnológico para ofrecer confianza</b>	<b>19</b>
<b>[5] Gestión inteligente de datos para maximizar la eficiencia y sostenibilidad</b>	<b>26</b>



Un contexto geopolítico y económico incierto y cambiante, marcado por la creciente inflación, los conflictos bélicos en Ucrania y Gaza o la crisis de los semiconductores, condicionarán las inversiones de las organizaciones en servicios tecnológicos y software. A pesar de este escenario, las previsiones auguran un crecimiento mundial del gasto en IT. La consultora de referencia Gartner apunta a un **aumento de la inversión del 8% durante el 2024**, impulsado especialmente por la subida de precios de la nube y la imparable y exponencial demanda de servicios de ciberseguridad que apunta a liderar la inversión IT en los próximos meses.

	2022 Spending	2022 Growth (%)	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)
Data Center Systems	227,021	19,7	237,703	4,7	260,221	9,5
Devices	766,279	-6,3	689,288	-10,0	722,472	4,8
Software	811,314	10,7	916,240	12,9	1,042,386	13,8
IT Services	1,305,699	7,5	1,401,038	7,3	1,547,349	10,4
Communications Services	1,423,128	-1,9	1,449,286	1,8	1,497,345	3,3
<b>Overall IT</b>	<b>4,533,441</b>	<b>2,9</b>	<b>4,693,556</b>	<b>3,5</b>	<b>5,069,773</b>	<b>8,0</b>

Pronóstico mundial de gasto en IT (millones de dólares estadounidenses). Fuente Gartner

Las previsiones de IDC van más allá del próximo año y apuntan a una evolución constante hasta 2027 con una **tasa de crecimiento anual compuesto (TCAC) del 5,7%**. En España, por ejemplo, se prevé que el gasto en TI siga por encima del PIB, por sexto año consecutivo. Y en Latinoamérica se espera un crecimiento de la inversión en tecnologías centradas en los negocios del 15,5% en los próximos dos años. Con este contexto, las personas con responsabilidad empresarial quieren centrar sus inversiones en conseguir resultados claros y medibles. Por ello pondrán el foco en plataformas digitales y escalables, en la transformación inteligente del puesto de trabajo y en seguridad y sostenibilidad. Todo con el objetivo de buscar la **mayor eficiencia del negocio en la inversión digital**.

## ¿Cuáles serán las tecnologías protagonistas del 2024?

Optimizar las inversiones, fortalecer la ciberseguridad o impulsar la innovación. Son tres de los principales desafíos a los que deberán hacer frente las compañías en los próximos meses. Y para abordar estos retos, la tecnología es un elemento habilitador que permite mejorar la competitividad, el rendimiento y la capacidad de adaptación a un entorno en continua transformación. En este informe te ayudamos a entender cómo la tecnología puede ayudar a definir la estrategia de futuro de tu negocio.

# [1] INTELIGENCIA ARTIFICIAL: FUERZA IMPULSORA DE LA INNOVACIÓN Y LA EFICIENCIA

Seguro que en los últimos meses le has pedido ayuda a ChatGPT, Bing, Copilot o Bard para que te oriente o te ayude a completar alguna de tus tareas. Sin entrar a valorar el grado de precisión de la respuesta que ofrecen, es una muestra de la popularización de los sistemas de inteligencia artificial generativa (AIGen) gracias, precisamente, a su accesibilidad.

Aunque cada vez son más las organizaciones que están explorando sus usos y aplicaciones, expertos y consultoras coinciden en que, al

menos en el próximo año, esta tecnología no tendrá aún un impacto notable en la inversión IT. Lo que sí está provocando ya es un cambio de mentalidad y planificación que hará que, a medio y largo plazo, sí tenga una repercusión en la asignación del presupuesto tecnológico. Por ahora, solo entre el 4 y el 10% de los empleados utilizan de forma regular herramientas de IA generativa en sus trabajos, según una encuesta de McKinsey. Todo apunta que ese porcentaje irá escalando y, progresivamente, irán cubriendo una parte de los procesos de las compañías.

La IA generativa está preparada para aumentar la productividad de las TI. Algunas herramientas suponen el ahorro de 30 minutos diarios para poder dedicarlos a tareas de mayor concentración o mejoras de hasta el 40% en las tareas de desarrollo de software.

## ¿En qué está ayudando la IA generativa?



Crear contenido escrito  
o gráfico



Escribir código  
de programación



Automatizar tareas y  
procesos repetitivos



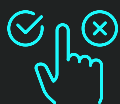
Mejorar y personalizar  
los servicios de atención  
al cliente



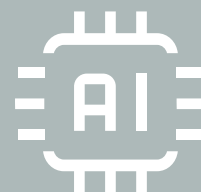
Identificar y pronosticar  
tendencias de necesidades

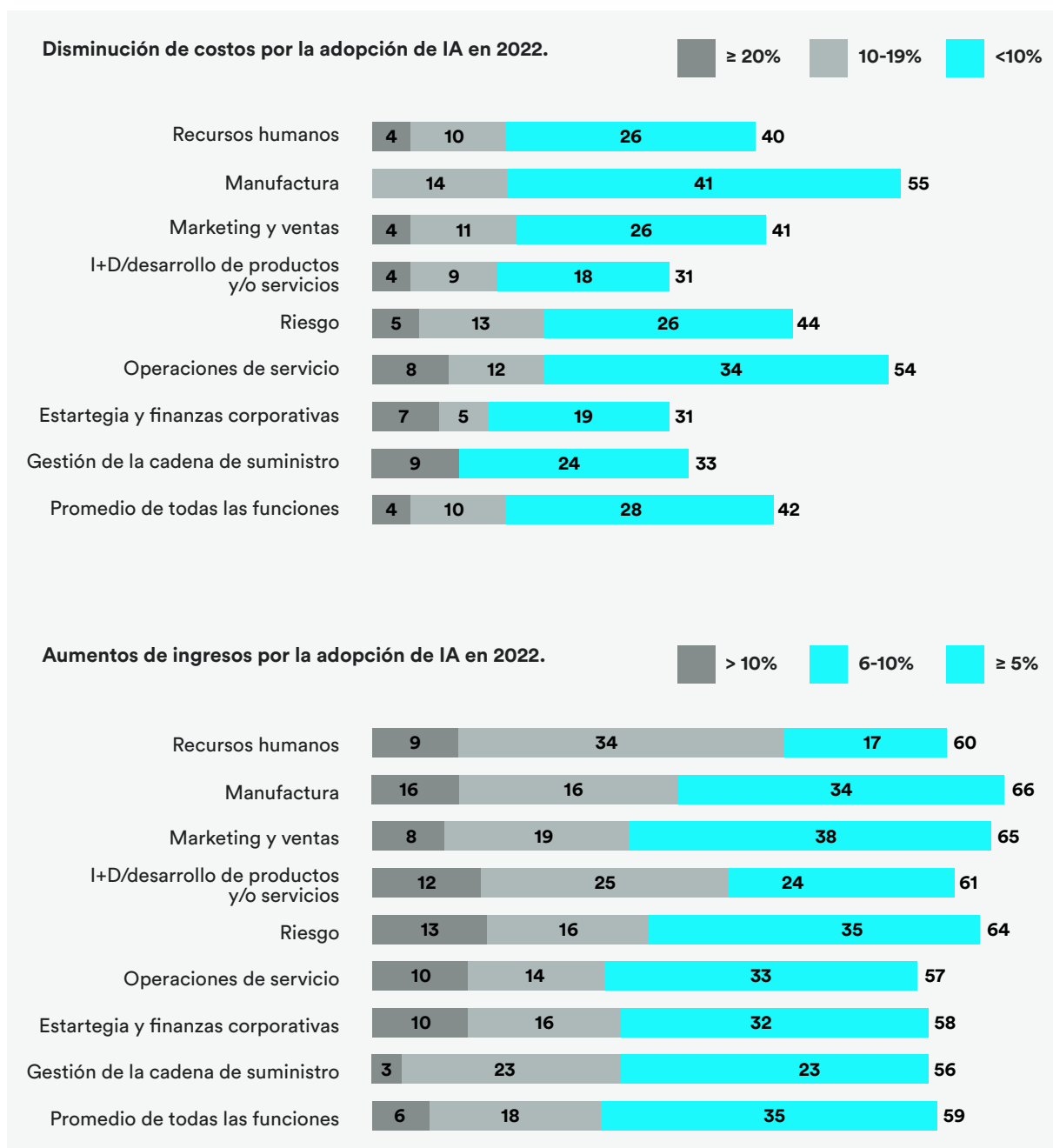


Analizar e interpretar datos



Mejorar la toma  
de decisiones





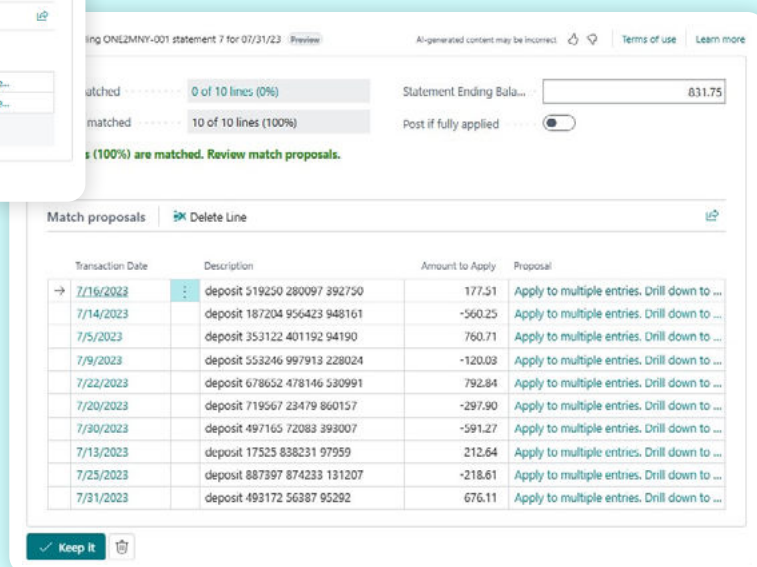
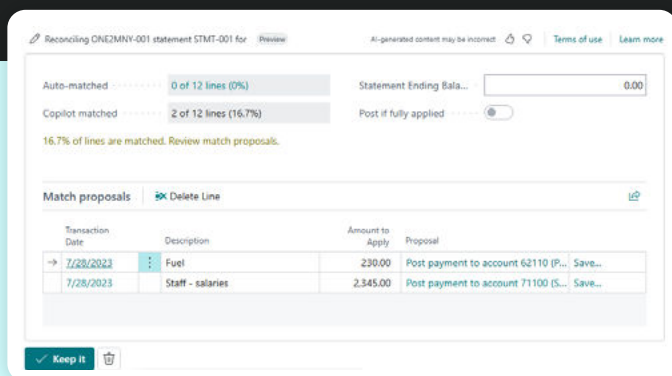
El estado de la IA en 2023: El año clave de la IA generativa Fuente: [McKinsey](#)

Aunque parece haber todavía un abismo entre las expectativas y la realidad, cada vez conocemos más casos de uso que van desde los motores de búsqueda y los paquetes de diseño, comunicación y marketing a los recursos humanos o el software de gestión empresarial. Es el caso, por ejemplo, de **Copilot** que permite, a través de la suite de productos de Microsoft, transcribir las reuniones para organizar ideas, sugerir texto en un documento, resumir una conversación o un hilo de correos para ponerse al día de forma rápida o crear el borrador de una presentación proporcionándole simplemente un tema.

Este asistente, que combina las capacidades de los **modelos masivos de lenguaje (LLM)** con el **análisis de datos**, también se ha integrado en su ERP Dymanics 365 Business Central, del que en Cuatroochenta somos partners. Ofrece funcionalidades más avanzadas para agilizar algunos procesos financieros y de operaciones. De hecho, según una encuesta publicada por Microsoft, el 70% de los usuarios de Copilot afirman que son **más productivos** con esta herramienta y un 68% considera que **mejora la calidad de su trabajo**.

“Es Copilot y no Autopilot, porque el piloto seguimos siendo nosotros. Es un asistente muy útil para que haga tareas tediosas, que nos ocupan mucho tiempo y una de ellas es la conciliación bancaria”.

Rubén Quesada,  
Functional Consultant Software  
de Gestión Empresarial



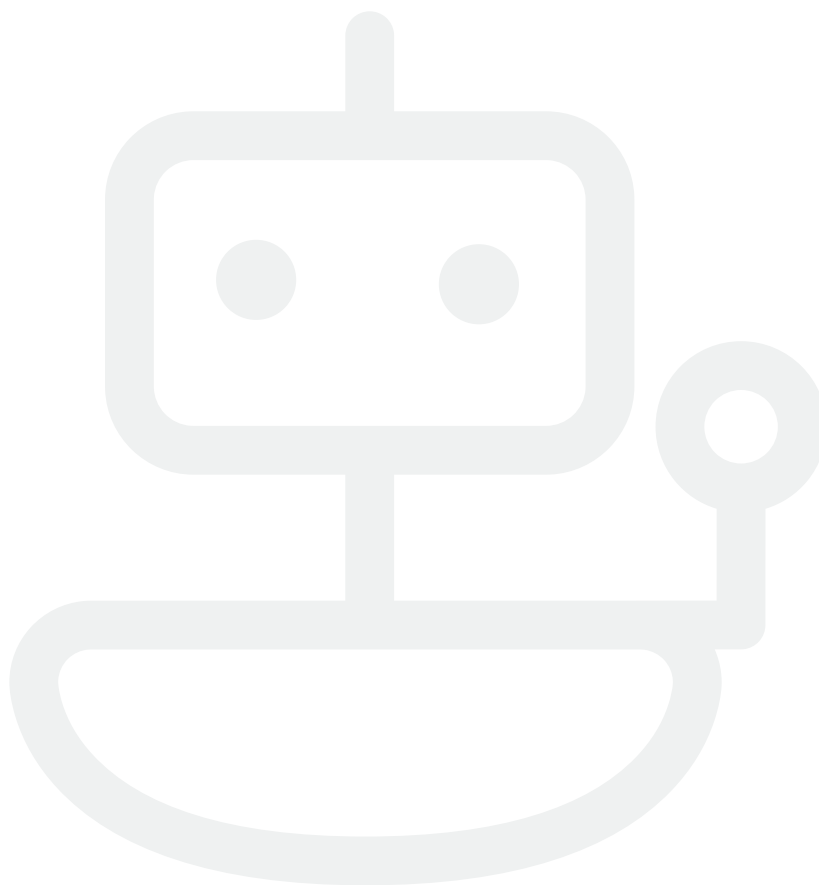
¿Quieres conocer las últimas novedades que incorpora Business Central?

[Consulta](#)



Lo que sí parece claro es que la IA generativa está **impulsando la innovación** en las empresas. Las compañías están integrando progresivamente este tipo de herramientas en sus procesos diarios y, recelosos del uso y la privacidad de algunos de estos modelos, están incluso desarrollando sus propias soluciones basadas en procesamiento del lenguaje natural (PNL). La compañía textil Mango, por ejemplo, ha creado su propio sistema conversacional para utilizarlo en sus procesos internos de diseño de colección y gestión de la postventa. Ferrovial cuenta con un asistente interno para facilitar las tareas diarias a sus empleados.

Otro ejemplo es Charlotte AI, un chatbot avanzado de análisis de seguridad de CrowdStrike, capaz de proporcionar información en tiempo real sobre vulnerabilidades o riesgos de una organización. Con esta misma filosofía, en Cuatroochenta hemos implementado un chabot que responde dudas sobre FAMA, la plataforma de *Facility Management* de la compañía. Aunque, por ahora, se limita a un uso interno, se prevé que se convierta en un asistente abierto para clientes.



## Próximo horizonte y retos

A estas iniciativas se suma el reciente anuncio del lanzamiento de la propia GPT Store de Open AI para ofrecer versiones personalizadas de ChatGPT, como un bot que ayude a solucionar problemas informáticos o una aplicación que permite leer un documento y transformarlo en una presentación. Hay quien va más allá y ya habla de **IA interactiva**. El cofundador de DeepMind (Google), Mustafa Suleyman, cree que pronto los robots serán capaces de realizar tareas recurriendo a otros softwares y a otras personas. De una opinión similar es el fundador y consejero delegado de Cuatroochenta, Sergio Aguado, quien apuesta por **la aparición a medio y largo plazo de agentes autónomos**. Se trataría, por ejemplo, de un sistema que estuviera instruido para manejar el perfil de LinkedIn de una empresa, generando una serie de posts dirigidos a unos clientes concretos y en unos momentos determinados del día.

Ante este futuro que se dibuja de software cada vez más autónomo, gobiernos y autoridades intentan acelerar el paso para regularizar el uso y la privacidad de los datos con los que se alimentan este tipo de sistemas. El objetivo es que ofrezcan **mayores garantías de seguridad y confianza**. Y es que la ciberseguridad, la infracción de la propiedad intelectual y el cumplimiento normativo son, junto a la imprecisión, los riesgos más revelantes que identifican las empresas relacionados con la adopción de esta tecnología. Dejando al lado la regulación, otra cosa que podría ralentizar o frenar las ambiciones y aspiraciones de muchas de las grandes tecnológicas, según algunos expertos, es la limitada disponibilidad mundial de unidades de procesamiento gráfico (GPU) y de producción de chips.



“En un medio y largo plazo, veremos aparecer agentes autónomos. Es un paso más allá. En lugar de dar órdenes concretas, podremos definir objetivos y ese agente irá iterando, de forma autónoma, para conseguirlos”.

Sergio Aguado,  
Cofundador y consejero  
delegado de Cuatroochenta

## [2] CIBERSEGURIDAD INTEGRAL Y PROACTIVA: DETECCIÓN Y RESPUESTA

Tener y ofrecer confianza forma parte del eje central de cualquier organización. Y esa confianza, si ponemos el foco en la parte digital, está siendo especialmente amenazada por esos sistemas de IA generativa que mencionábamos. Con esta tecnología, los grupos de ciberdelincuentes son capaces de lanzar y automatizar sofisticados ataques de *phishing* o *vishing* o de generar contenido falso como deepfakes, promoviendo la desinformación. Este nuevo desafío se suma a la lista de **principales amenazas de ciberseguridad** a los que se enfrentan las compañías y administraciones:



### Ransomware

Es la amenaza más preocupante. Los ciberdelincuentes utilizan técnicas de extorsión para la filtración de información, secuestro de información y extorsión.



### Malware

Se trata de software malicioso como los troyanos, gusanos o programas espías.



### Ingeniería social

Se recurre al engaño y el error humano para obtener información.



### Ataques DDoS

Sobrecargan una red, sistema, aplicación, web o incluso un dispositivo IoT a través de botnets para inhabilitar su servicio.



### Cadena de suministro

Ante el mayor grado de madurez de la grandes corporaciones, los atacantes lanzan amenazas contra proveedores o librerías desarrolladas por terceros.



### Entornos cloud

Buscan errores en la configuración, que es la principal causa de las brechas de seguridad.

En vista del creciente riesgo de vulnerabilidades, la proliferación de ciberamenazas y un entorno en constante evolución, resulta vital que las organizaciones fortalezcan y perfeccionen sus estrategias de ciberseguridad.

## 8%

Es el aumento de ciberataques semanales globales que se ha producido en la primera mitad de 2023, el más significativo en 2 años (Check Point Reserach).

## 227 días

Es lo que tardan, de media, las organizaciones en detectar y contener una brecha de seguridad (IBM).

## 4,45M\$

Máximo histórico del coste medio de una brecha, un 16% más que hace 5 años (IBM).

Las infraestructuras críticas, especialmente el sector sanitario y las entidades financieras, siguen siendo los ámbitos más amenazados. Ante este escenario global, se espera que **el gasto mundial en seguridad y gestión de riesgos siga aumentando y crezca un 14% para el 2024 (Gartner)**, liderando en muchas organizaciones la inversión IT. La continua adopción y demanda de servicios cloud, el trabajo híbrido y el emergente y rápido uso de la IA generativa están impulsando la inversión en seguridad.

Además de la gestión de la seguridad en la nube, las compañías se enfrentan a la complejidad de los entornos que combinan **equipos IT y OT** (maquinaria industrial o tecnología operativa) en sectores como la agricultura, la logística, el transporte, la energía o incluso el sanitario. Parte del hardware o de los dispositivos no están preparados para estar conectados fuera de una red local o con sistemas operativos antiguos, lo que dificulta la protección de este tipo de entornos.

Este horizonte que se dibuja para los próximos meses se complica todavía más con la proliferación de los dispositivos IoT, las amenazas a través de terceros o los ataques **Zero Day** que aprovechan vulnerabilidades desconocidas por fabricantes y desarrolladores. Los ciberdelincuentes siguen utilizando estas brechas como vector de entrada, según destacaba el director de Estrategia de Exabeam, Gorka Sadowski, en la charla #EnModoAvión 'Próximo vuelo: IA y Zero Trust. Ciberseguridad 360° en el sector aéreo', que Sofistic y Cuatroochenta organizaron en septiembre de 2023 en el Hotel La Compañía del Casco Viejo de Panamá. Los sistemas de **análisis de patrón del comportamiento**, sustentados en *machine learning*, son la única vía para poder identificar y responder a este tipo de amenazas.



## Objetivo: mejorar la detección y respuesta

La tardanza en identificar y dar respuesta a incidentes de seguridad, que de media llega a los 9 meses desde que los atacantes logran entrar en la red o sistema, hace que tengan mucho mayor impacto. Para mejorar esta identificación, minimizar el tiempo de respuesta y reducir el impacto de los ataques son prioritarios los **servicios *Managed Detection & Response* (MDR)**. Existen plataformas de MDR que analizan e integran datos de diversas fuentes, de manera que aceleran y unifican la detección de amenazas encubiertas.

Este tipo de herramientas, se combinan con la securización 24/7 que ofrecen los Security Operations Center (SOC). Con esta integración, no solo se identifican e investigan de manera efectiva las amenazas, sino que también se toman medidas para bloquear y contener el impacto del ataque. Antes, únicamente se lanzaba la alerta y se reportaba al cliente la brecha de seguridad. Con estos servicios, además de generar los avisos, paralelamente se ejecutan las medidas adecuadas y acordadas con la organización atacada, con el objetivo de neutralizar la amenaza en cuestión de segundos.

### ¿Por qué un servicio MDR?

- Monitoreo de alertas
- Investigación de ataques
- Visibilidad más amplia sobre superficie de ataque
- Búsqueda proactiva de amenazas
- Evitar falsos positivos
- Respuesta coordinada e inmediata

“La principal ventaja que aportan los servicios MDR es que la gestión y la contención de los incidentes es mucho más rápida. No tenemos que avisar a la organización del incidente para que actúe, sino que tenemos capacidad de respuesta para tomar las medidas oportunas y bloquear la amenaza”.

Juan Carlos García,  
Sofistic COO & SOC Director





La monitorización continua de un servicio MDR se complementa con las **auditorías de seguridad** periódicas que permiten hacer una evaluación exhaustiva de la situación actual de un entorno o red para aflorar vulnerabilidades y ofrecer recomendaciones de mejora. Otra de las acciones que garantiza la protección de las organizaciones son los **servicios de seguridad activa** que permiten tener una capa adicional de seguridad para mantener las configuraciones óptimas de los servicios IT en cada momento. Suponen un ciclo de mejora continua sobre todo el perímetro de seguridad de una organización, desde las apps, la infraestructura y las redes a la identidad y los dispositivos y los *endpoints*.

### Definición del perímetro en los servicios de seguridad activa



La **ciberseguridad** es una inversión estratégica que **fortalece la resiliencia de la empresa** en un entorno digital en continua transformación.

¿Está tu organización preparada para afrontar los desafíos emergentes y proteger los activos digitales de manera efectiva?

[Contacta](#)

## [3] HERRAMIENTAS PARA DOMAR EL CAOS MULTICLOUD

Tras diversos años de impulso de la inversión en **cloud**, por la acelerada transformación digital que provocó la pandemia, la nube continúa siendo uno de los mayores habilitadores de valor en las organizaciones. Las grandes empresas aspiran a tener aproximadamente el 60% de su entorno en la nube para 2025, según [Mckinsey](#). La **inversión en cloud pública crecerá un 20,4%** durante el 2024, según [las estimaciones de Gartner](#), para responder a las necesidades empresariales y las tecnologías emergentes como la GenAI.

Las **soluciones SaaS** (*software as a service*) siguen siendo las más demandadas, concentrando el 36% del gasto. El sanitario, las telecomunicaciones, la banca, el retail, el transporte y el energético son los sectores que más están apostando por este tipo de tecnología. Si hace un año apuntábamos al **multicloud como una tendencia creciente** para diversificar servicios entre varios proveedores en la nube, ahora tenemos que hablar de las plataformas o soluciones que intentan poner orden y facilitar el desarrollo de soluciones en este tipo de entornos.

**El 85% de las empresas están utilizando dos o más plataformas cloud y el 25% está utilizando como mínimo 5 ([Deloitte](#))**

### ¿Cuáles son los retos del multicloud?

- **Complejidad**
- **Costes**
- **Rendimiento**
- **Interoperabilidad**
- **Seguridad**
- **Privacidad**
- **Sostenibilidad**





## Unificar la gestión de entornos multicloud

Para abordar estos desafíos las empresas de software están utilizando cada vez más plataformas que permiten una gestión unificada del entorno IT para agilizar el desarrollo de aplicaciones y permitir que escalen de forma flexible y segura. Las conocidas como **infraestructuras como código (IaC)** permiten **automatizar la construcción de arquitecturas en la nube** con código, legible por las máquinas, lo que permite optimizar el desarrollo de soluciones y el control de versiones.

En un entorno multicloud, se debe configurar cada solución y servicio en función de las características y herramientas que ofrece cada proveedor. En cambio, este tipo de herramientas IaC lo que hacen es unificar la configuración y la infraestructura como si fuera un centro de datos, independientemente de la nube en la que se trabaje. Y además, como se utiliza código, es mucho más fácil escalar y hacer versiones. Terraform, Ansible, Chef o Pulumi son algunas de las plataformas de estas características más utilizadas.

### Ventajas

- **Automatización**
- **Mayor velocidad**
- **Control de versiones**
- **Escalabilidad y flexibilidad**
- **Simplificar la gestión**
- **Mayor control de costes**

## Automatizar el flujo de trabajo de desarrollo

Para simplificar y acelerar el proceso de desarrollo, testeo e implementación de soluciones, también se están popularizando las plataformas de alojamiento web y despliegue de aplicaciones sin servidor. Es el caso de Vercel o Netlify que permiten a los equipos de desarrollo alojar sus soluciones web y desplegarlas en la nube de una manera sencilla y productiva. Este tipo de herramientas están dando respuesta a la alta demanda de entornos de desarrollo ágiles y eficientes.

### Ventajas

- **Facilidad de uso**
- **Soporte para tecnologías modernas**
- **Alojamiento escalable y seguro**
- **Automatización del flujo de trabajo**

## Ingeniería de plataformas

Hay un concepto emergente del que cada vez hablan más informes y expertos que es el de la **ingeniería de plataformas** (Platform Engineering). No es una herramienta ni un rol determinado, sino una disciplina que persigue crear plataformas internas que aglutinen y compartan las herramientas, sistemas y servicios que pueden necesitar los diferentes equipos de desarrollo de una misma organización. Se trata de ofrecer soluciones para gestionar, automatizar y optimizar el ciclo de desarrollo de **aplicaciones nativas en la nube**.

Son como portales de autoservicio para desarrolladores que buscan optimizar los recursos, automatizar procesos, estandarizar herramientas y promover buenas prácticas. Uno de los ejemplos más conocidos es Backstage, de código abierto y desarrollado por Spotify, que alberga los recursos que pueden necesitar los desarrolladores como repositorios Git, procesos de creación o APIs. Forrester prevé que, durante el 2024, la adopción de este tipo de portales se extienda entre los equipos de infraestructura y operaciones. Empresas como American Airlines, Ericsson, Lowe's o Mercedes-Benz ya están implementando este tipo de portales.

### Ventajas

- **Eficiencia**
- **Mayor velocidad de entrega**
- **Flexibilidad**
- **Estandarización**
- **Automatización y optimización**
- **Reducción de costes**

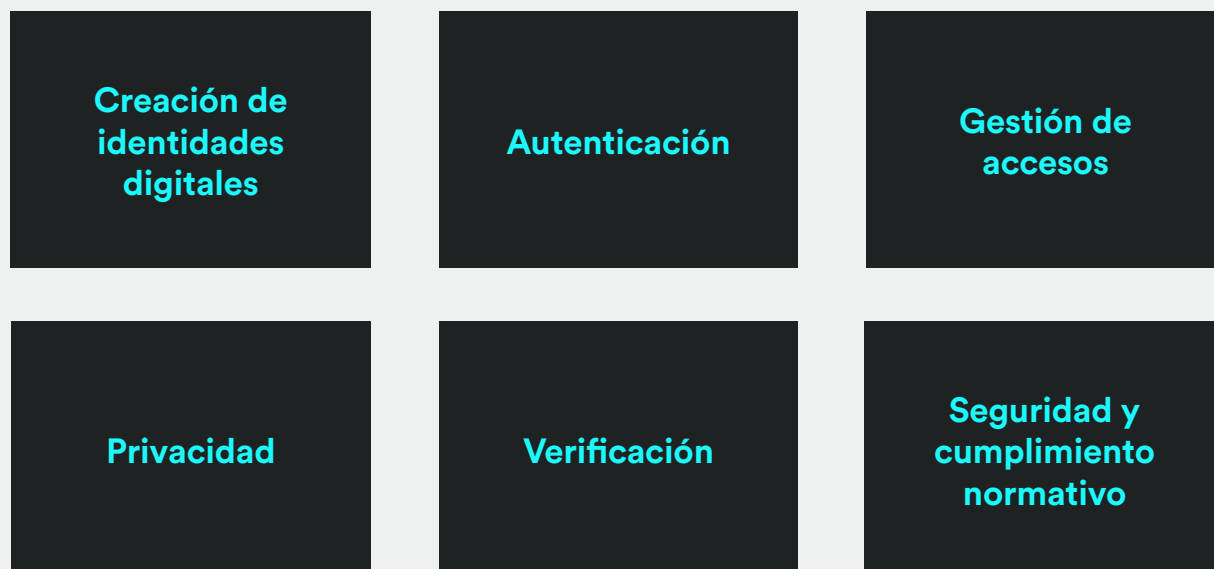
## [4] GESTIÓN DE LA IDENTIDAD: IMPERATIVO TECNOLÓGICO PARA OFRECER CONFIANZA

Un mundo cada vez más digitalizado y con un complejo entorno multicloud ha generado un nuevo desafío para las organizaciones que es el de la **gestión de la identidad digital** (IDM). Para las empresas privadas y las administraciones, la verificación y autenticación de la identidad de los usuarios y las usuarias, tanto internos como externos, se ha convertido en una prioridad para garantizar la seguridad, la privacidad y la eficiencia de los procesos y transacciones en línea, así como para proteger los activos. La gestión de la identidad abarca el conjunto de procesos, políticas y tecnologías que se encargan de administrar y certificar la identidad de personas, usuarios, entidades, sistemas o dispositivos en los entornos digitales y que van muy ligadas a la confianza que aportan las compañías.

### Administrar y asegurar la identidad

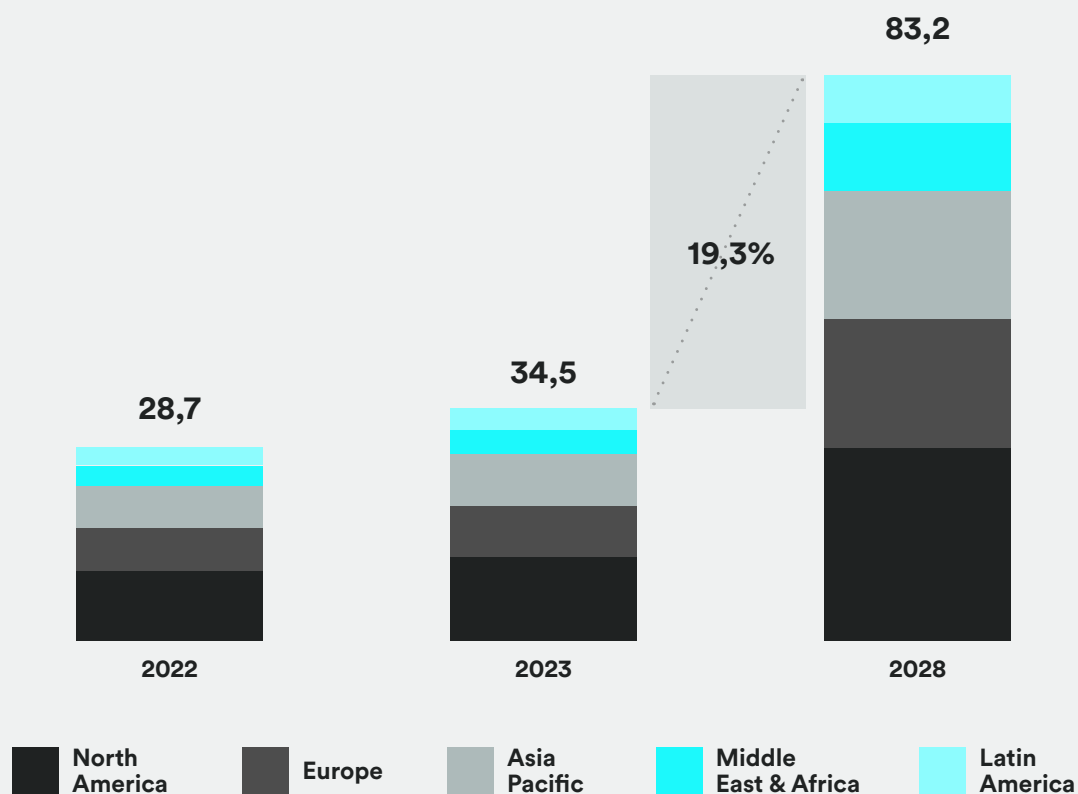


## ¿Qué ámbitos abarca?



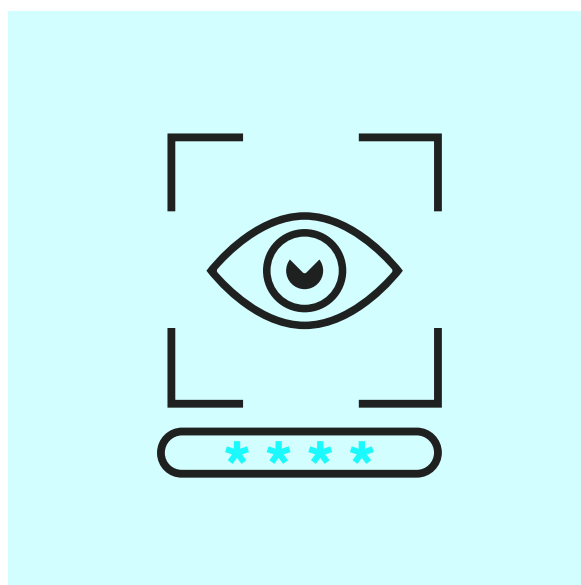
La identidad digital es un elemento clave que asegura la operativa diaria de muchas organizaciones, la gestión de la información y la interacción entre personas, máquinas y activos. Es necesaria, por ejemplo, para acceder a servicios esenciales como el correo electrónico o aplicaciones de gestión, pero también para hacer el registro de jornada, utilizar dispositivos o hardware, firmar documentos o interactuar con clientes a través de plataformas digitales. Todo ello ha provocado una intensificación de los riesgos asociados que van desde el fraude o robo de datos al desafío de verificar quién está detrás de una identidad. Y más teniendo en cuenta que tendemos, como apuntamos hace un año, hacia un modelo de superapps, en el que una única plataforma concentra prestaciones o características de diferentes herramientas.

Toda esta multiplicidad de retos y amenazas se ha traducido en un incremento de la inversión en soluciones de identidad digital para intentar atajarlos. Según un informe de MarketsandMarkets, el mercado global de este tipo de herramientas experimentará **una tasa de crecimiento CAGR del 19,3% hasta 2028**. Un aumento que también se explica por la integración, en estas soluciones, de otras tecnologías como la inteligencia artificial, el *machine learning* o la blockchain.



Mercado de soluciones de identidad digital mundial hasta 2028. Fuente: [Marketsandmarkets](#)

La banca, los servicios financieros, los seguros, el retail y los servicios sanitarios son los sectores que están apostando firmemente por estas tecnologías. Las soluciones de biometría son las que se prevé que tengan un mayor peso en los próximos años, a pesar de las polémicas que ha suscitado en relación a la intrusión en la privacidad. Además de contar con una capa adicional de protección para garantizar la seguridad y la privacidad, estas organizaciones buscan ofrecer una mejor experiencia a usuarios y clientes.



## ¿Cuáles son las principales tecnologías de gestión de identidad y acceso?

**Sistemas de Gestión de Identidad (IDM)**

**Single Sign-On (SSO)**

**Autenticación Multifactor (MFA)**

**Control de acceso basado en roles**

**Gestión de Acceso Privilegiado**

**Identidad autosoberana o descentralizada (SSI)**

**Biometría**

**Autenticación sin contraseña (comportamiento o contexto)**

Los métodos más tradicionales como las contraseñas o el control de accesos son ahora insuficientes ante la proliferación de riesgos y el avance de la AIGen. Las organizaciones se han visto obligadas a optar por nuevas tecnologías y enfoques, como la biometría, la identidad descentralizada o soberana basada en tecnología blockchain o la gestión de identidades sin contraseña. En este último caso, por ejemplo, se utilizan técnicas de **autenticación por comportamiento** en las que se analiza la forma en que una persona escribe en un teclado o dispositivo móvil, teniendo en cuenta la velocidad, el patrón de pulsación de teclas o el estilo de escritura. También existen métodos de **verificación de identidad por contexto** en los que se utiliza la ubicación física de la persona

usuaria y la red utilizada para acceder, por ejemplo, a una app de gestión corporativa.

Mientras soñamos con la llegada de una sesión única verificada para acceder a todos nuestros servicios digitales, las tecnologías de autenticación seguirán madurando en los próximos años. Existen iniciativas privadas y públicas que impulsan desde hace años la estandarización de la verificación y autenticación de la identidad. Pero a la espera de que se materialicen esos proyectos, las diferentes organizaciones buscan soluciones que les permitan construir, escalar y mantener la confianza de trabajadores, clientes y usuarios en el uso de datos, productos y servicios digitales como, por ejemplo:

La Comisión Europea trabaja en diversos casos de uso para crear las bases del futuro **wallet de identidad digital**, para que ciudadanos y empresas de toda Europa puedan acceder a servicios en línea públicos y privados.



CheckingPlan, la plataforma inteligente de Cuatroochenta para la gestión de tareas, registro horario y control de accesos, ofrece la posibilidad de identificación a través del reconocimiento facial biométrico sin contacto. Este sistema es extremadamente útil en hospitales, fábricas, escuelas, instalaciones comerciales o estaciones.

Los aeropuertos son una de las infraestructuras que han implementado la tecnología biométrica para comprobar documentación e identidad de los pasajeros.



## ¿Por qué es importante gestionar la identidad digital?

Además de garantizar la operativa de una compañía con eficiencia, la identidad digital protege de intrusiones e incidentes. Hace dos años la perito judicial, experta en ciberinvestigación y CEO de Obranding, Selva Orejón, ya alertaba en el podcast *Cuidado con las macros ocultas* del aumento de casos de robo y **suplantación de identidad** y de la necesidad de contar con **sistemas de alerta temprana** sobre la compra de dominios, generación de usuarios, uso ilícito de logotipos o filtración de claves.

# 82%

De las brechas involucran compromiso de identidad (Verizon). Es el principal instrumento que utilizan los ciberdelincuentes para quebrantar el acceso al sistema o red de una organización.

# 79'

Es el tiempo que, de media, tardan los ciberdelincuentes desde que acceden a una organización hasta que realizan movimientos laterales (Crowstrike).

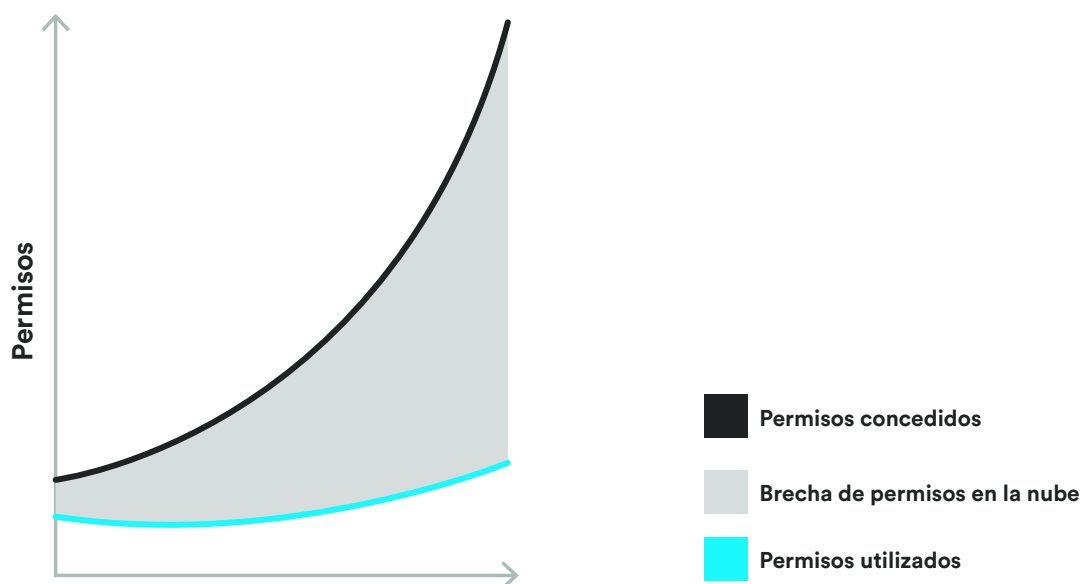
# 160%

De aumento de intentos de obtener claves secretas y otros credenciales a través de APIs de metadatos en la nube (Crowstrike).

Para detener las amenazas de identidad los expertos recomiendan servicios de monitoreo proactivo y continuo de usuarios, roles y servidores para detectar y prevenir ataques. Y complementarlo con un modelo de seguridad Zero Trust. A pesar de la complejidad de su implantación, se trata de establecer una política de mínimos privilegios y de controlar y verificar cada autenticación, transacción y acceso a la información en una organización.



### Brecha de permisos



“Para minimizar riesgos es importante pensar en soluciones que detecten actividades en países infrecuentes, cuando un trabajador está intentado usar una red de Thor o una VPN anónima o, simplemente, alerten que está sentado en un café de mala reputación donde le han robado las credenciales a otras personas”.

Juan David Díaz,  
Active Security Director Sofistic

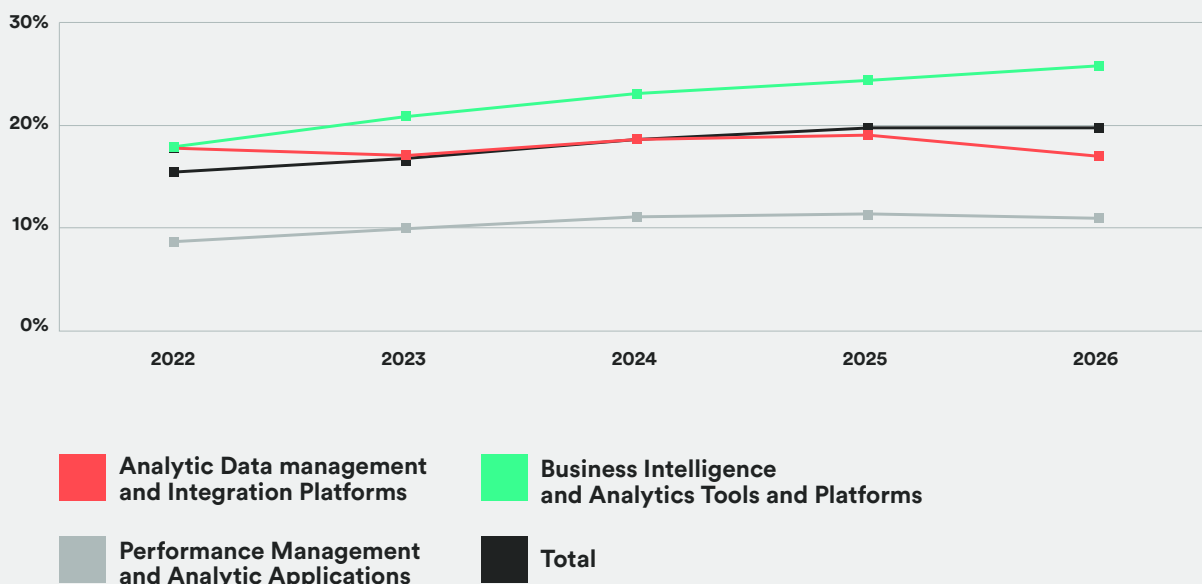


## [5] GESTIÓN INTELIGENTE DE DATOS PARA MAXIMIZAR LA EFICIENCIA Y SOSTENIBILIDAD

Es indudable que, en el actual panorama digital, los datos se han convertido en uno de los activos más estratégicos y preciados de las organizaciones. Diariamente recopilan miles de datos que van desde las métricas de ventas y facturación al consumo energético, el inventario y logística o el estado y rendimiento de maquinaria, por citar algunos ejemplos. Ante ese gran océano de información, hace tiempo que empresas y administraciones entendieron que el **big data** era el gran aliado para mejorar la toma de decisiones y, en definitiva, ser más eficientes.

La creciente importancia de los datos en la empresa moderna, la mayor adopción de la nube pública y el aumento del uso de sistemas de inteligencia artificial y aprendizaje automático en las aplicaciones empresariales explican la escalada que ha tenido el big data en los últimos años. El pronóstico, además, sigue siendo positivo. IDC vaticina un **crecimiento del mercado de gestión y analítica de datos del 23,6% hasta 2026**.

Previsión mundial de software BDA - 2022-2026



Fuente: IDC

## Tecnologías que marcan la diferencia

La tecnología ayuda a transformar la gran cantidad de datos que generan las compañías en conocimiento y acciones concretas. No se trata simplemente de que las soluciones analicen los datos, sino que los conviertan en información estratégica y propongan ideas para que los negocios sean verdaderamente eficientes y sostenibles en un mercado altamente competitivo.

### IA y machine learning:

Automatización de procesos, análisis predictivo y gestión inteligente.

### IoT:

Monitoreo y gestión de recursos en tiempo real y mantenimiento predictivo.

### Computación en la nube:

Escalabilidad y flexibilidad.

**La eficiencia y la responsabilidad ambiental no son objetivos opuestos, sino complementarios en el mundo empresarial actual.**

La optimización de rutas en el transporte y logística, la planificación de servicios de limpieza y mantenimiento, el análisis del comportamiento de los clientes en el sector del retail o el mantenimiento predictivo de maquinaria industrial son algunos ejemplos en los que la **gestión inteligente de datos** está teniendo mayor impacto. Gracias al software conectado a dispositivos IoT, las organizaciones pueden monitorizar servicios, equipos y personal en tiempo real.

En el sector alimentario, por ejemplo, existen soluciones que permiten visualizar información sobre el estado y rendimiento de los equipos para optimizar su producción y funcionamiento. En este caso, Cuatroochenta trabaja en diversos proyectos en los que el **software, conectado a terminales IoT** integrados en las máquinas, ofrece datos sobre su uso para poder adaptar su configuración a los hábitos de consumo de los usuarios. De esta manera, según explica el desarrollador de software de la compañía, Carlos Cabezas, se pueden hacer actualizaciones de forma remota para cambiar la iluminación en un proceso, la fuerza de un pistón o la velocidad del motor, por ejemplo. En definitiva, este mantenimiento predictivo “mejora el tiempo de respuesta y optimiza costes”.

## Analítica de datos en la gestión de servicios e instalaciones

Otro ejemplo lo encontramos en los hospitales, donde el IoMT permite automatizar la gestión de incidencias, tareas y personal, para mejorar la asistencia a pacientes. A esa lista de procesos que generan información de valor para mejorar la toma de decisiones, podríamos añadir también la factura electrónica que próximamente será obligatoria en España para todas las relaciones comerciales B2B.

En la gestión de inmuebles, patrimonio y servicios, lo que se conoce como *Facility Management* y *Facility Services*, también cobra mucha importancia esa gestión inteligente. En este sentido, el software para el registro de tareas y fichajes CheckingPlan, que utilizan más de 50 hospitales y centros sanitarios o empresas como Serveo, Alstom o Alvic, permite automatizar la gestión de tareas e incidencias, a partir de los datos que recibe de múltiples fuentes como el registro horario o sensores.

Además genera informes de actividad que pueden ser muy útiles para el departamento de Recursos Humanos.

También es de gran valor la información que puede ofrecer una plataforma de gestión integral de activos e infraestructuras. Para las organizaciones que buscan la máxima eficiencia es vital, por ejemplo, disponer de información sobre la desviación en el consumo energético de un mes respecto a otro, sobre las instalaciones que han requerido mayor inversión para su mantenimiento o sobre el proveedor más o menos eficiente a partir de los tiempos de resolución de incidencias y los costes derivados. Son ejemplos de cómo una solución, interoperable y con una homogeneización y estructuración de datos, como es FAMA permite ayudar a tomar mejores decisiones y optimizar los recursos en una compañía.



“La propuesta de valor para buscar la eficiencia y la optimización de procesos está en que la tecnología analice de manera desatendida datos asociados a cualquier entidad y nos sugiera y aporte ideas para solucionar situaciones que a las personas se nos pueden pasar por alto”.

Ángela García,  
FAMA General Manager

## Software para avanzar en la responsabilidad ESG

Ya lo apuntábamos el año pasado, pero las compañías cada vez están más preocupadas por cumplir con sus estándares ESG. Las empresas se encuentran en un punto crucial en que la eficiencia no significa solo lograr los objetivos financieros, sino también abrazar la responsabilidad corporativa y la sostenibilidad. En este sentido, la tecnología es estratégica para gestionarla. Existen soluciones que monitorizan la cadena de suministro, el rastreo de la huella de carbono o la gestión de residuos.

“No se contempla hablar de **un proyecto de gestión de infraestructuras y activos sin hablar de sostenibilidad**” apuntaba el socio director de Cuatroochenta, Santi Gimeno, el pasado mes de octubre en la Feria FACMAN de México, el mayor evento de *Facility Management* en la región. Gimeno añadía que “la gestión eficiente de infraestructuras ayuda a las organizaciones a ser más competitivas. Es un elemento tractor y disparador para tomar decisiones”. Este tipo de software permite identificar áreas de mejora. Es, por ejemplo, un instrumento básico para digitalizar el proceso de reporting de consumos energéticos e indicadores clave como el cálculo de la huella de carbono en sectores como el transporte o la alimentación.

En Cuatroochenta disponemos de la herramienta FAMA SOSTenible, una solución tecnológica para la automatización y gestión centralizada e integrada de los diferentes aspectos relativos al ámbito de la sostenibilidad que ayuda a cumplir con las regulaciones e integrar la sostenibilidad en la estrategia de las compañías.



## FAMA SOSTENIBLE

¿Quieres saber más sobre esta herramienta?

[Ver más](#)



## ¿Quieres aplicar estas tecnologías en tu negocio para que sea más eficiente?

En Cuatroochenta te ayudamos a afrontar los retos de tu organización con software cloud y ciberseguridad.

Cuéntanos lo que necesitas.

[Contacta](#)

480



[cuatroochenta.com](http://cuatroochenta.com)