





CÓMO CONTRATAR SERVICIOS IT APLICADOS AL FM

GUÍA DE CONTRATACIÓN

COMISIÓN DE TECNOLOGÍA
Sponsor: Ángela García Juste

IFMA® España Chapter
International Facility Management Association

ÍNDICE

INTRODUCCIÓN 03
Por Alfonso Díaz del Río

PREÁMBULO 04
Por Ángela García Juste

LA INFRAESTRUCTURA DE 'HARDWARE':
EL ECOSISTEMA CIBERFÍSICO (FM + IT) 06
Por Carmen Velasco

EL 'SOFTWARE' REDEFINE EL NUEVO 'FACILITY MANAGEMENT' 12
Por Juan Ignacio Herrero

GESTIÓN DEL CAMBIO: LAS PERSONAS EN EL CENTRO 16
Por Glòria Ausió

LA IMPORTANCIA DE LA CIBERSEGURIDAD:
ASPECTOS A TENER EN CUENTA 20
Por George Darlington

INTELIGENCIA ARTIFICIAL Y FM. ¿EN QUÉ PUNTO ESTAMOS? 28
Por George Darlington

AUTORES PARTICIPANTES 38

IFMA ESPAÑA 39



INTRODUCCIÓN

El *facility management* vive un momento decisivo. Durante años, nuestra disciplina ha sido percibida como una función de soporte: necesaria, sí, pero situada en un segundo plano frente a otras áreas consideradas más estratégicas. Sin embargo, la realidad de los últimos años ha demostrado con claridad que esa visión ha quedado superada. Hoy, el *facility management* es una palanca esencial para la continuidad de la actividad, la eficiencia de los recursos, la sostenibilidad de los activos y, sobre todo, la calidad de vida de las personas que trabajan, visitan, producen, aprenden o reciben servicios en nuestros edificios e infraestructuras.

Desde IFMA España venimos defendiendo que el *facility management* integra personas, espacios, procesos y tecnología con un propósito muy concreto: mejorar el rendimiento de las organizaciones y contribuir a entornos más seguros, eficientes, sostenibles y humanos. Esta definición, que puede parecer sencilla, encierra una enorme complejidad.

Porque gestionar hoy un edificio, un campus, una red de oficinas, un hospital, una infraestructura crítica, una industria o un centro logístico ya no consiste únicamente en asegurar que "todo funcione". Consiste en anticiparse, interpretar datos, coordinar servicios, gestionar riesgos, acompañar el cambio cultural y tomar decisiones que tienen impacto directo en la productividad, en la experiencia de usuario, en la resiliencia operativa y en la competitividad de las organizaciones.

Este documento nace precisamente en ese contexto. La transformación digital, la convergencia entre *software* y *hardware*, la inteligencia artificial, la ciberseguridad, la automatización, la eficiencia energética, la sostenibilidad, la gestión del cambio y los nuevos modelos de *workplace* están redefiniendo de forma acelerada el papel del *facility manager*. Nos encontramos ante una profesión cada vez más transversal, que debe dialogar con tecnología, recursos humanos, finanzas, real estate, compras, sostenibilidad, seguridad, operaciones y dirección general. Y esa transversalidad exige una mirada amplia, rigurosa y práctica.

Pero sobre todo nace alineado con nuestra responsabilidad como IFMA de generar conocimiento útil, compartir experiencias reales, abrirnos a nuevos sectores y geografías, y conectar a todos los actores de la cadena de valor: profesionales, empresas proveedoras, organizaciones usuarias, instituciones, universidades y administraciones públicas.

Estas páginas abordan algunas de las grandes dimensiones de esta transformación. Lo hacen desde una mirada técnica, pero también desde una perspectiva de gestión. Porque la tecnología por sí sola no transforma nada si no está al servicio de un propósito claro; y porque los datos, los sensores, el *software* o la inteligencia artificial solo generan valor cuando ayudan a tomar mejores decisiones y a mejorar nuestra vida.

Nuestro reto como sector es enorme, pero también lo es la oportunidad. Si somos capaces de combinar conocimiento técnico, visión estratégica, sostenibilidad, innovación y liderazgo humano, el *facility management* ocupará el lugar que le corresponde: no en la periferia de las organizaciones, sino en el centro de su capacidad para adaptarse, competir y prosperar en un mundo cada vez más complejo.

Alfonso Díaz del Río
Presidente de IFMA España



PREÁMBULO

Toda organización que decide adquirir tecnología (*hardware* o *software*) para la gestión de cualquier ámbito del *facility management* (FM), tarde o temprano, ha de enfrentarse a la misma pregunta: ¿cómo elegir bien? El mercado ofrece soluciones distintas con promesas parecidas, y no siempre es fácil distinguir cuál es la más adecuada en cada caso. Esta guía nace precisamente para acompañar a quienes se encuentran ante ese reto –el de contratar servicios de IT aplicados al *facility management*– y ofrecerles criterios claros para decidir con conocimiento y con visión de futuro.

Desde la Comisión de Tecnología de IFMA España quisimos que no fuera un documento teórico, sino una herramienta nacida de la experiencia real de quienes viven el sector desde dentro.

Por eso, el mayor valor de estas páginas está en las voces que las han hecho posibles. Y a ellas quiero dar las gracias.

A Carmen Velasco (Growth & Marketing Leader de Columat), que nos sitúa en la capa física y nos ayuda a entender el edificio como un ecosistema ciberfísico, donde la convergencia entre tecnología operativa y de información marca la diferencia. A Juan Ignacio Herrero (ingeniero de Telecomunicaciones en Ricoh España y Portugal), que explica cómo el *software* se ha convertido en el eje del nuevo *workplace* y por qué la interoperabilidad, que conecta espacios, dispositivos y personas, es hoy imprescindible. A Glòria Ausió (directora de Recursos Humanos de Ricoh España y Portugal), que pone el foco donde de verdad se juega todo: en las personas y en la gestión del cambio, recordándonos que la transformación no se mide por la tecnología implantada, sino por su capacidad de mejorar la experiencia de quienes la usan. Y a George Darlington (Senior Facilities & Business Improvement Manager en UBS), que aborda dos frentes decisivos –la ciberseguridad, que ha dejado de ser un asunto exclusivo de IT, y la inteligencia artificial– con la mirada de quien conoce tanto sus riesgos como su potencial.

Todos ellos son profesionales tan diversos como complementarios: tecnología, recursos humanos, ciberseguridad, negocio… Y esa diversidad no es casual: refleja lo que significa contratar servicios de IT, algo que trasciende lo técnico.

Aquí quiero detenerme, porque es la reflexión de fondo de esta guía. Cuando una organización afronta la contratación de tecnología para FM, los perfiles de compras tienden, con toda lógica, a fijarse en el precio. Es su función.

Pero un proyecto digital de *facility management* es mucho más que la simple adquisición de IT: es una decisión estratégica que afecta a procesos, a personas y, en el fondo, a la cultura de la organización. Implica cambiar la forma de trabajar. Por eso, más que un proveedor, lo que conviene buscar es un *partner*.

Esta guía nace precisamente para acompañar a quienes se encuentran ante ese reto –el de contratar servicios de IT aplicados al *facility management*– y ofrecerles criterios claros para decidir con conocimiento y con visión de futuro.



La reflexión de fondo de esta guía: cuando una organización afronta la contratación de tecnología para FM, los perfiles de compras tienden, con toda lógica, a fijarse en el precio. Es su función. Pero un proyecto digital de *facility management* es mucho más que la simple adquisición de IT: es una decisión estratégica que afecta a procesos, a personas y, en el fondo, a la cultura de la organización.

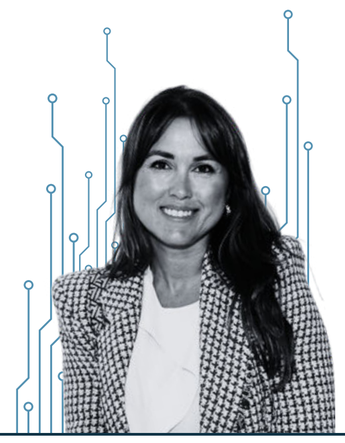
¿Y qué distingue a un *partner* estratégico? Que se le elige mirando más allá de la funcionalidad y del coste. Se valora su experiencia comprobada, muy especialmente en proyectos de gran complejidad, que es donde se demuestra de verdad quién te acompaña. Su solvencia y su estabilidad, porque reducen el riesgo operativo a largo plazo. La seguridad certificada de sus sistemas, hoy innegociable –como bien recuerda esta guía–. La cercanía y el acompañamiento, decisivos cuando lo que está en juego es un cambio cultural y operativo que las personas tienen que hacer suyo. Y la flexibilidad, para que sea la tecnología la que se adapte a las personas y a la idiosincrasia de cada organización y no al revés.

Esa es, en el fondo, la intención de esta guía: que ninguna organización tenga que recorrer sola ese camino, y que cuando lo recorra, lo haga bien acompañada. Espero que os resulte útil.

Por último, quiero dar las gracias también a Alfonso Díaz del Río, presidente de IFMA España, y a Rubén Hernández, gerente de IFMA España, por todo su apoyo en el desarrollo de esta guía, y a Óliver Mayorga por la estupenda maquetación de este documento.

Para mí es un auténtico privilegio seguir aportando valor al ámbito del FM a través de iniciativas como esta, que nacen con el propósito de acompañar y facilitar el trabajo de los profesionales que, día a día, impulsan y transforman nuestro sector.

Ángela García Juste
Líder de la Comisión de Tecnología
IFMA España



La infraestructura de ‘hardware’: el ecosistema ciberfísico (FM + IT)



Carmen Velasco
Growth & Marketing Leader
Columat

«Poseer la mejor infraestructura física del mercado es solo la mitad del camino; es, en esencia, dotar al edificio de sentidos, pero no de consciencia».

En el horizonte del *facility management* de 2026, el *hardware* ha dejado de ser un conjunto de dispositivos aislados para transformarse en un sistema ciberfísico (CPS). Esta capa representa los “sentidos” y los “músculos” del activo. Un edificio moderno es, en esencia, un nodo de computación distribuida que genera un flujo constante de información. La excelencia radica en la Convergencia IT/OT, donde los activos físicos (Operational Technology) se integran bajo arquitecturas de red seguras (Information Technology).



Clasificación del *hardware* y servicios relacionados

A continuación, se desglosan las ocho dimensiones que componen la infraestructura física, explicando su contexto y su aplicación práctica:

Capa sensórica e IoT (percepción y salud del edificio)

Esta capa es la fuente primaria de datos. No se trata solo de medir, sino de obtener metrología digital confiable.

- **Monitorización de calidad de aire interior (IAQ):** sensores que miden CO_2, partículas PM2.5/PM10 o Compuestos Orgánicos Volátiles (VOCs). Es vital para la productividad y salud de los ocupantes (estándares WELL/ASHRAE).

- **Gestión de ocupación y flujos:** uso de sensores de imagen térmica o de “Tiempo de Vuelo” (ToF). Estos dispositivos detectan la presencia humana sin capturar imágenes reales, garantizando el anonimato total (Privacy-by-Design).

- **Conectividad de bajo consumo:** se debe priorizar el hardware con protocolos LoRaWAN o NB-IoT. Estos permiten que los sensores funcionen con baterías durante años y atraviesen muros de hormigón sin colapsar el ancho de banda del Wi-Fi corporativo.

Automatización y control (BMS/BEMS – El sistema nervioso)

El *hardware* que regula el "pulso" del edificio (clima, iluminación, agua).

- **Controladores DDC (Direct Digital Control):** deben tener capacidad de *edge computing*. Esto significa que el *hardware* puede tomar decisiones locales (por ejemplo, cerrar una válvula ante una inundación) aunque se pierda la conexión a internet.

- **Interoperabilidad obligatoria:** el *hardware* debe hablar protocolos estándar como BACnet/SC (Secure Connect), Modbus TCP o KNX. Esto evita el *vendor lock-in* (quedar atrapado con un solo fabricante para siempre).

Logística interna y custodia: 'smart lockers' (el nodo logístico)

Hardware diseñado para automatizar la gestión de objetos y documentos.

- **Gestión de valija interna:** permite el envío y recepción de documentación sensible entre departamentos de forma automatizada. El *hardware* registra quién deposita, cuándo y quién recoge, eliminando el error humano y la necesidad de conserjería física 24/7.

- **Paquetería externa, compras e IT Asset Management:** taquillas inteligentes para la entrega, recogida, devolución o intercambios. Un empleado puede dejar un portátil averiado y recoger uno de sustitución de forma desasistida, integrándose con el *software* de tickets de IT y el departamento puede recibir sus compras corporativas en un *smart locker* sin necesidad de interrumpir al personal de recepción o mantenimiento, avisándole de la disponibilidad una vez se efectúa la entrega.

Energía y movilidad (Smart Energy & EV)

El FM ahora gestiona el edificio como una microrred eléctrica.

- **Cargadores de vehículo eléctrico (EV):** *hardware* con gestión dinámica de carga para no sobrepasar la potencia contratada.

- **Sistemas BESS (almacenamiento en baterías):** permite almacenar energía en horas valle o de fuentes fotovoltaicas para usarla en horas punta *(peak shaving).*

- **Vehicle-to-Grid (V2G):** *hardware* que permite que las baterías de los coches conectados devuelvan energía al edificio si es necesario.





Iluminación inteligente y robótica de servicio

- **Sistemas PoE (Power over Ethernet):** la iluminación se alimenta y comunica por cable de datos (RJ45). Cada luminaria se convierte en un nodo de red que además incluye sensores de temperatura y ocupación.

- **Cobots (robótica colaborativa):** robots autónomos de limpieza o desinfección con mapeo LiDAR. Requieren una infraestructura de carga y "muelles" de servicio específicos que el FM debe contratar.

'Workplace' y 'hospitality' (experiencia del usuario)

El *hardware* diseñado para eliminar la fricción operativa del empleado.

- **Interfaces de sala:** paneles de tinta electrónica *(e-Ink)* de bajísimo consumo que muestran la disponibilidad de salas sincronizados con M365/Google.

- **Kioscos de visitantes:** *hardware* con biometría ética e integración en el Active Directory (SSO) para que las visitas reciban sus credenciales automáticamente.

- **Wayfinding digital:** pantallas interactivas que guían a usuarios y proveedores por el edificio.

Conectividad y redes (infraestructura IT pasiva – El esqueleto)

Es el *hardware* que "no se ve" pero soporta todo lo anterior.

- **Cableado y fibra:** categoría 7A/8 y anillos de fibra óptica para garantizar que no haya cuellos de botella.

- **Cobertura interior (DAS):** antenas para asegurar que hay señal 5G/6G en zonas críticas como sótanos o búnkeres técnicos.

- **Edge Data Centers:** *racks* monitorizados y climatizados situados en el propio edificio para procesar datos de seguridad y control en milisegundos.

Seguridad electrónica y protección crítica (CCTV e incendios)

- **Visión artificial (Edge AI):** cámaras que no solo graban, sino que analizan. Pueden detectar humo o llamas antes que un sensor óptico tradicional, o detectar una caída de una persona mayor o trabajador solo.
- **Sistemas IP-PCI:** detección de incendios con direccionamiento IP para localizar el foco exacto del evento desde el *software* central.



Valor estratégico: el binomio rentabilidad vs. productividad

La implementación de este *hardware* no es un gasto, sino una palanca financiera. El éxito se mide mediante el impacto en dos ejes críticos:

Rentabilidad operativa y financiera (eficiencia del activo)

- **Optimización del espacio (Real Estate Rationalization):** la sensórica de ocupación identifica infrautilización, permitiendo reducir la huella de alquiler o subarrendar espacios, con un impacto directo en el P&L.
- **Mantenimiento Centrado en Fiabilidad (RCM):** detectar anomalías mediante *hardware* predictivo reduce costes de reparación urgente en un 50% y alarga la vida útil de los activos.
- **Eficiencia energética y ESG:** la monitorización precisa facilita el cumplimiento de la ISO 50001 y mejora el acceso a financiación verde *(sustainability-linked loans).*
- **Valoración del activo (The Smart Premium):** edificios certificados con SmartScore o WiredScore tienen una mayor liquidez y una valoración entre un 5% y un 10% superior al mercado analógico.

Productividad y capital humano (la regla del 3-30-300)

Bajo la premisa de que el mayor coste de una empresa son las personas (300 por metro cuadrado vs. 3 en energía), el *hardware* impacta donde más valor se genera:

- **Rendimiento cognitivo:** niveles óptimos de CO_2 aseguran que el aire nunca esté viciado, manteniendo el rendimiento de la plantilla hasta un 10% superior.
- **Eliminación de fricción:** los *smart lockers* y sistemas de reserva ahorran "micro-minutos" diarios. Multiplicado por la plantilla, supone la recuperación de miles de horas de productividad anuales.
- **Salud y absentismo:** la monitorización proactiva previene el "Síndrome del Edificio Enfermo", reduciendo las bajas laborales por enfermedades respiratorias.
- **Atracción de talento:** un entorno tecnológico de vanguardia es una herramienta de RRHH crítica para la retención del talento joven.

Marco normativo, legislativo y de certificación

La contratación de *hardware* debe estar blindada legalmente. Un dispositivo que no cumpla estas normas es una responsabilidad legal para la empresa:

Estándar / Ley	Ámbito	Relevancia estratégica
ISO 41001	Facility management	Garantiza que la tecnología sirve al modelo de negocio.
IEC 62443	Ciberseguridad OT	Blindaje del *hardware* industrial contra hackeos.
SRI (EU EPBD)	Smart Readiness	Indicador oficial (2026) de la inteligencia del edificio.
EN 301 549	Accesibilidad TIC	El *hardware* (Lockers/Kioscos) debe ser usable por todos.
ISO 50001	Gestión energética	Precisión obligatoria en sensores de medición *(submetering)*.
WiredScore / SmartScore	Certificación	Mide la calidad de la conectividad y la inteligencia del activo.
Project Haystack	Semántica	Estándar de etiquetado para que el *software* entienda el *hardware*.
EU AI Act	Inteligencia artificial	Regula el uso de cámaras y sensores con análisis inteligente.

Criterios de aplicación y excelencia en la contratación

Para que el *hardware* aporte valor real a largo plazo, el pliego técnico debe incluir estos criterios:

01 Análisis de coste de ciclo de vida (LCC)

No se debe contratar por el precio de compra, sino por el coste total en 7-10 años (Precio de Compra + Costos de Operación Futuros).

02 Identidad digital (Digital Birth Certificate)

Cada dispositivo debe tener un identificador único (QR/NFC) vinculado a su manual y garantía en el software de FM.

03 Commissioning técnico (Cx)

Protocolo obligatorio de pruebas. El *hardware* no se da por aceptado hasta que su dato es validado y etiquetado (bajo modelo Haystack) en la plataforma central.

04 Ciberseguridad Zero Trust

El *hardware* debe soportar seguridad moderna (802.1X) y el proveedor debe garantizar parches de seguridad en menos de 72 horas ante vulnerabilidades críticas.

05 Estrategia API-First

El *hardware* debe tener APIs abiertas y documentadas. Los datos generados son propiedad exclusiva del cliente, nunca del fabricante del *hardware*.

La orquestación del dato

Llegados a este punto, hemos definido el "cuerpo digital" del edificio y asegurado que los sensores sean precisos, que la red sea cibersegura y que cada componente de *hardware* esté alineado con una rentabilidad financiera y una productividad humana medibles. Sin embargo, poseer la mejor infraestructura física del mercado es solo la mitad del camino; es, en esencia, dotar al edificio de sentidos, pero no de consciencia.

Para que este ecosistema ciberfísico deje de ser una lista de activos y pase a ser una ventaja competitiva, necesitamos la capa que orqueste, procese y dote de sentido a cada bit de información. Es el momento de elevar la mirada desde el "hierro" hacia la Capa de Gobernanza Lógica: ese cerebro operativo capaz de transformar millones de señales aisladas en una sola interfaz de decisiones estratégicas, permitiéndonos, por fin, dejar de reaccionar al presente para empezar a gobernar el futuro: el *software*.

El *hardware* es el origen de la verdad, pero los datos, por sí solos, son solo ruido eléctrico atrapado en cables de cobre y ondas de radio. El verdadero desafío del *facility manager* moderno no es acumular dispositivos, sino evitar que el edificio se convierta en un conjunto de islas tecnológicas inconexas.

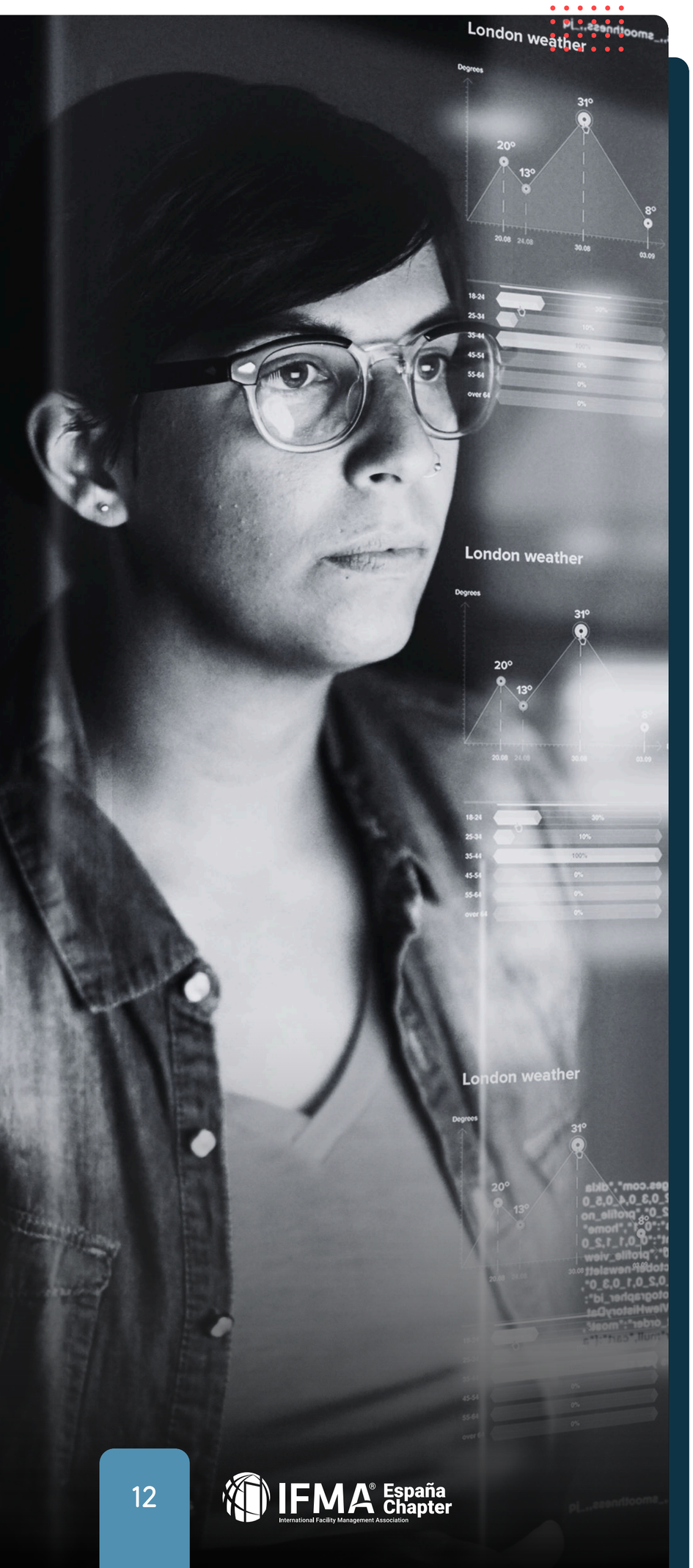
El ‘software’ redefine el nuevo ‘facility management’



Juan Ignacio Herrero
Ingeniero de Telecomunicaciones
Ricoh España y Portugal

«Ya no se trata solo de digitalizar procesos, sino de conectar espacios, dispositivos y personas».

Durante años, el *facility management* se centró en garantizar el correcto funcionamiento de los edificios: mantenimiento, eficiencia operativa, seguridad y control de costes. Sin embargo, la consolidación del trabajo híbrido y la evolución de las expectativas de los empleados han transformado el papel del *workplace* dentro de las organizaciones. Hoy, las oficinas son entornos estratégicos diseñados para favorecer la colaboración, la flexibilidad y la experiencia de las personas.



Este cambio plantea nuevos retos para los responsables de FM. La ocupación de los espacios fluctúa constantemente, conviven múltiples tecnologías y crece la necesidad de tomar decisiones basadas en datos, mientras las organizaciones buscan optimizar recursos y avanzar en sostenibilidad.

Sin embargo, muchas compañías siguen operando con herramientas desconectadas entre sí: plataformas de reserva, sensores IoT, controles de acceso, climatización o sistemas audiovisuales que generan información aislada y dificultan una gestión eficiente.

En este contexto, el *software* se ha convertido en el eje del *workplace* moderno. Ya no se trata solo de digitalizar procesos, sino de conectar espacios, dispositivos y personas en una única plataforma que permita gestionar los entornos laborales de forma inteligente, flexible y predictiva.

El *workplace* inteligente: de la gestión a la orquestación

La evolución del *facility management* está estrechamente ligada al desarrollo de plataformas capaces de integrar toda la operativa del entorno laboral. Su objetivo es simplificar la gestión y convertir los datos en información útil para la toma de decisiones.

Las soluciones IWMS (Integrated Workplace Management System) han evolucionado desde herramientas centradas en la reserva de espacios hacia plataformas SaaS que unifican la gestión de puestos de trabajo, salas, visitantes, aparcamientos, recursos compartidos y ocupación en un único entorno digital accesible desde cualquier dispositivo.

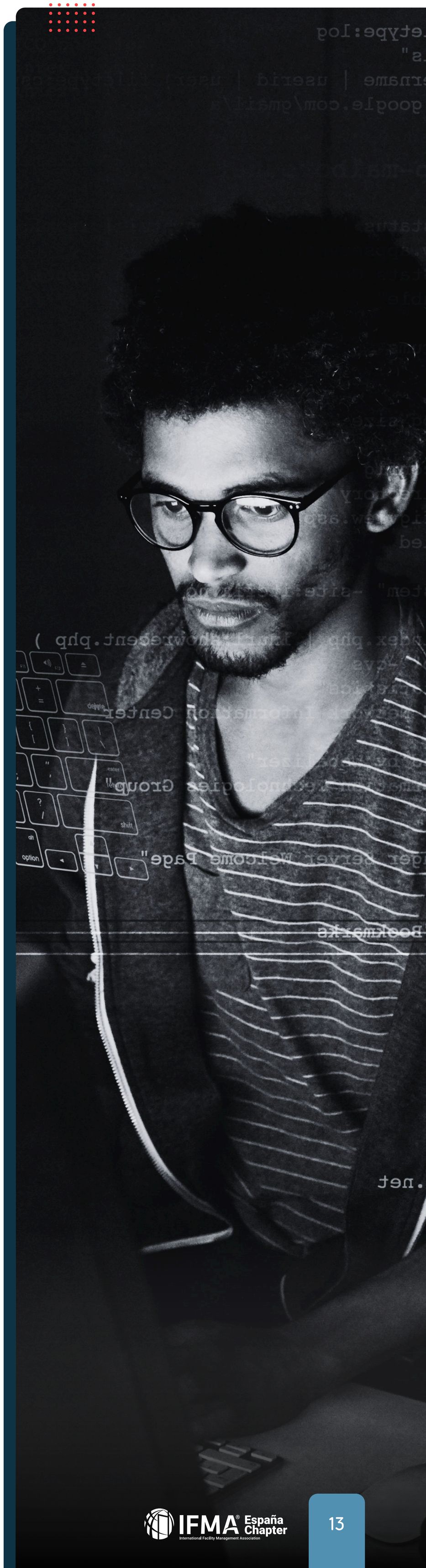
A nivel técnico, una de sus principales capacidades de estas plataformas reside en su arquitectura abierta e interoperable. La integración mediante APIs y *webhooks* permite conectar calendarios corporativos, plataformas de colaboración, sistemas de control de acceso, sensores IoT, soluciones audiovisuales o Building Management Systems (BMS), creando un ecosistema en el que la información fluye de forma bidireccional entre edificios, usuarios y servicios.

La captura continua de datos de ocupación permite optimizar el uso del espacio mediante cuadros de mando y motores analíticos que ofrecen información en tiempo real sobre utilización, disponibilidad de recursos o patrones de movilidad.

En entornos híbridos, esta capacidad es especialmente valiosa para adaptar la capacidad de las oficinas, redistribuir recursos y reducir espacios infrautilizados a partir de datos objetivos.

Otro elemento diferencial es la automatización de procesos. La integración entre plataformas de *workplace* y sistemas del edificio permite activar automáticamente la climatización o los sistemas audiovisuales antes de una reunión, liberar salas no utilizadas, ajustar la iluminación en función de la ocupación o generar incidencias técnicas de forma preventiva.

Esta automatización también alcanza la gestión de activos y servicios internos. El auge del trabajo flexible ha impulsado soluciones de almacenamiento inteligente para la entrega y devolución de dispositivos, material corporativo o paquetería, mejorando la trazabilidad y reduciendo tareas manuales.





Inteligencia unificada para el *workplace* conectado

El siguiente nivel de madurez tecnológica pasa por plataformas capaces de centralizar y contextualizar información procedente de múltiples sistemas.

Estas soluciones integran datos de sensores IoT, plataformas de reserva, climatización, sistemas audiovisuales, activos tecnológicos, control de accesos, consumo energético o incidencias operativas para construir una visión única del *workplace*.

Este enfoque permite evolucionar desde modelos reactivos hacia operaciones predictivas apoyadas en inteligencia artificial y *machine learning*. Los motores analíticos detectan anomalías, anticipan incidencias técnicas y optimizan automáticamente parámetros operativos a partir de patrones históricos y datos en tiempo real.

Entre sus aplicaciones destacan la gestión dinámica de la climatización según la ocupación real, la optimización automática del consumo energético, la preparación inteligente de espacios antes de eventos o la detección temprana de fallos en equipamiento crítico.

Para ello, es necesario contar con un agente de IA proactiva capaz de integrar y contextualizar información procedente de múltiples fuentes, como los inventarios de activos (BMS), las bases de conocimiento para la resolución de incidencias y peticiones (ITSM) o los procedimientos de aprobación y autorización. A partir de esa información, el agente debe ser capaz de proponer soluciones al Gestor del Servicio, respetando los flujos de aprobación según el nivel de criticidad técnica y económica, así como gestionar la notificación de alertas e incidencias y activar el nivel de escalado más adecuado a través de distintos canales, como mensajería instantánea, SMS, correo electrónico o llamada telefónica. La interoperabilidad se convierte aquí en un elemento crítico. Las nuevas plataformas están diseñadas sobre arquitecturas cloud nativas y modelos API-first que facilitan la integración con infraestructuras heterogéneas y dispositivos de distintos fabricantes, permitiendo evolucionar el ecosistema tecnológico sin sustituir sistemas existentes.

Para obtener este nivel de visualización es imprescindible disponer de una herramienta de observabilidad flexible que permita conocer en tiempo real el estado de cada activo, reaccionar rápidamente ante eventos críticos y analizar su evolución histórica para justificar, con datos, la sustitución, incorporación o retirada de activos ante el área financiera de la compañía.



Del Internet of Things al Workplace of Things

La evolución tecnológica de los edificios inteligentes está desplazando el foco desde el Internet of Things (IoT) hacia un concepto más amplio: el Workplace of Things, donde el objetivo ya no es únicamente conectar dispositivos, sino coordinar experiencias completas dentro del entorno laboral.

En este modelo, salas, puestos de trabajo, sensores, sistemas audiovisuales, controles ambientales y plataformas digitales funcionan como un ecosistema único capaz de adaptarse dinámicamente al comportamiento de los usuarios.

La clave reside en la capacidad de orquestación automática. Los espacios responden en tiempo real a la ocupación, las preferencias de los usuarios o las necesidades operativas sin requerir intervención manual, reduciendo fricciones y simplificando la experiencia del empleado.

Para ello, es fundamental incluir en todo proyecto de *facility management* una plataforma tecnológica que permita desarrollar automatizaciones e integraciones mediante herramientas visuales *low-code* e, incluso, incorporar un agente de IA capaz de desarrollar nuevas funcionalidades bajo petición del Gestor del Servicio utilizando lenguaje natural. Esto permitirá reducir la dependencia de equipos de desarrollo y responder con rapidez a nuevos retos tecnológicos.

En definitiva, el futuro del *facility management* está marcado por plataformas capaces de integrar tecnología, espacios y personas en un único ecosistema conectado, que permita que todas las herramientas trabajen de forma coordinada para convertir los datos en inteligencia operativa, simplificar la gestión y crear entornos de trabajo más eficientes, sostenibles y centrados en las personas.

Para los responsables de *facility management*, esta transformación supone evolucionar desde la gestión de infraestructuras hacia la administración inteligente de datos, operaciones y experiencia de usuario.

Gestión del cambio: las personas en el centro



Glòria Ausió

Directora de Recursos Humanos
Ricoh España y Portugal

«La evolución hacia modelos híbridos ha cambiado radicalmente la relación entre los empleados y el espacio de trabajo».

La transformación del entorno laboral no depende únicamente de la incorporación de nuevas tecnologías. El verdadero desafío para las organizaciones pasa por gestionar el cambio cultural que acompaña a los nuevos modelos de trabajo. La consolidación del trabajo híbrido, la flexibilidad y las nuevas expectativas de los empleados están obligando a replantear cómo diseñan los espacios, cómo impulsan la colaboración y cómo utilizan la tecnología para mejorar la experiencia diaria de las personas.



En este escenario, el *workplace* representa un ecosistema en constante evolución en el que convergen espacios físicos, herramientas digitales y dinámicas de trabajo cada vez más flexibles. La gestión del cambio, por tanto, requiere situar a las personas en el centro de toda la estrategia y ya no puede abordarse únicamente desde la tecnología o desde las operaciones.

Esto es porque la adopción tecnológica no depende solo de las herramientas disponibles, sino de cómo las viven los empleados. Un entorno de trabajo moderno debe ser intuitivo, accesible y capaz de adaptarse a diferentes necesidades y formas de trabajar. De lo contrario, incluso las mejores soluciones pueden generar fricción, rechazo o una pérdida de eficiencia.

Una nueva cultura organizativa

La evolución hacia modelos híbridos ha cambiado radicalmente la relación entre los empleados y el espacio de trabajo. Durante años, la oficina fue concebida como un lugar fijo y homogéneo.

Hoy, en cambio, se necesitan entornos mucho más dinámicos, flexibles y preparados para combinar trabajo presencial y remoto de forma fluida.

Este cambio ha hecho aflorar nuevas necesidades. Los empleados demandan herramientas que simplifiquen su día a día, espacios preparados para colaborar y tecnologías que funcionen de manera transparente, independientemente de dónde trabajen. Al mismo tiempo, esperan experiencias laborales más cómodas, ágiles y conectadas.

Por eso, la experiencia del empleado se ha convertido en un factor estratégico. No solo influye en la productividad o en la eficiencia operativa, sino también en aspectos como la atracción y retención del talento, el compromiso de los equipos y el bienestar laboral.

Por ello, cada vez más organizaciones entienden que la gestión del cambio no consiste únicamente en implantar tecnología, sino en facilitar la adaptación de las personas a nuevas formas de trabajar. Y eso implica escuchar, simplificar procesos y diseñar experiencias coherentes con las expectativas actuales del empleado.

Espacios y tecnología al servicio de las personas

El diseño de los espacios de trabajo también está evolucionando hacia modelos más humanos y colaborativos.

La oficina deja de ser un lugar pensado exclusivamente para tareas individuales y pasa a concebirse como un entorno de interacción, creatividad y conexión entre equipos.

En paralelo, la tecnología se convierte en un facilitador invisible de esa experiencia. Sistemas de reserva de espacios, plataformas colaborativas, soluciones audiovisuales o herramientas de gestión del *workplace* ayudan a eliminar barreras y permiten que las personas se centren en su trabajo sin preocuparse por la complejidad tecnológica.

El objetivo es crear entornos inteligentes capaces de adaptarse a las necesidades reales de los usuarios y donde todo debe funcionar de forma sencilla, integrada y natural. Por ello, una de las grandes prioridades actuales pasa por unificar experiencias y simplificar la interacción entre personas, espacios y tecnología.





La colaboración, clave en la transformación

La colaboración se ha convertido en uno de los pilares del *workplace* moderno. Pero para que sea realmente efectiva, las organizaciones necesitan eliminar barreras físicas y digitales que dificultan la interacción entre equipos.

Los nuevos entornos laborales requieren espacios versátiles, preparados para diferentes dinámicas de trabajo: reuniones híbridas, sesiones creativas, trabajo individual o colaboración espontánea. La flexibilidad deja de ser un elemento complementario para convertirse en una condición esencial del diseño de las oficinas.

En este sentido, la tecnología audiovisual y las plataformas de colaboración permiten conectar equipos distribuidos, facilitar la participación remota y garantizar experiencias homogéneas independientemente de la ubicación de cada empleado.

Gestión del cambio como ventaja competitiva

En muchas organizaciones, la transformación del *workplace* ya no responde solo a una necesidad operativa, sino a una decisión estratégica. La capacidad de adaptarse rápidamente a nuevas dinámicas laborales se ha convertido en un factor diferencial para mantener
la competitividad y responder a las expectativas de empleados y clientes.

Esto obliga a abordar la gestión del cambio desde una perspectiva mucho más transversal, para lo cual Facility Management, IT, Recursos Humanos y dirección deben trabajar de forma coordinada para diseñar experiencias laborales coherentes, sostenibles y alineadas con los objetivos del negocio.

Además, la evolución del *workplace* también está estrechamente vinculada a criterios de sostenibilidad y eficiencia. La optimización de espacios, el uso inteligente de recursos y la digitalización de procesos permiten reducir el impacto ambiental y avanzar hacia modelos de trabajo más responsables.

Para Ricoh, el futuro del *workplace* pasa precisamente por esa combinación entre tecnología, espacios y personas, porque la verdadera transformación digital no se mide solo por el nivel de tecnología implantada, sino por la capacidad de las organizaciones para mejorar la experiencia humana dentro del entorno laboral. Y en ese proceso, la gestión del cambio seguirá siendo el elemento decisivo para convertir la innovación en una ventaja competitiva sostenible.



La importancia de la ciberseguridad: aspectos a tener en cuenta

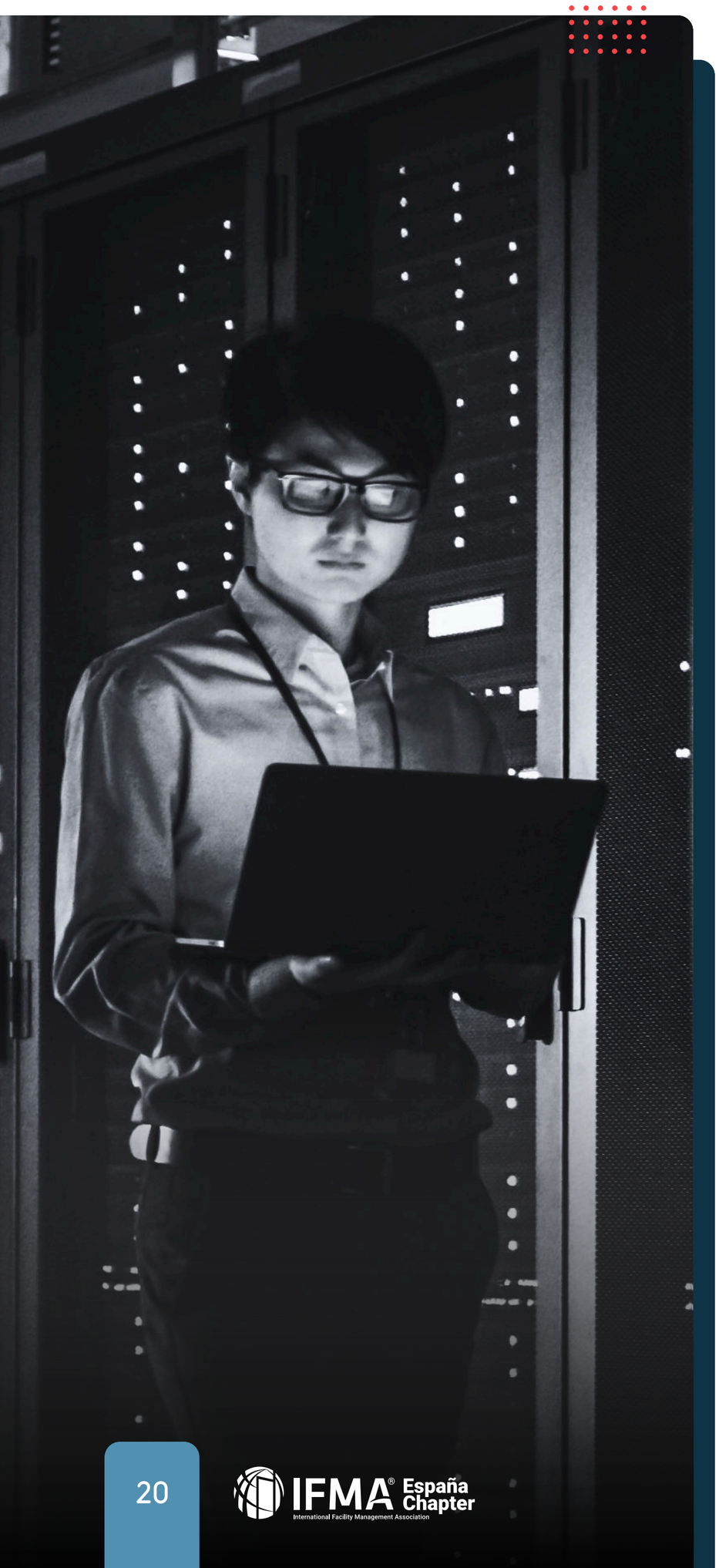


George Darlington

Senior Facilities & Business Improvement Manager
UBS

«La ciberseguridad ya no es un "extra" ni responsabilidad exclusiva del departamento de IT».

En los actuales edificios inteligentes, casi todos los sistemas que gestionamos como *facility managers* están conectados a redes TCP/IP: climatización (BMS), control de accesos, CCTV, detección y extinción de incendios, ascensores, iluminación, gestión energética, redes Wi-Fi para usuarios y hasta los sistemas de *ticketing* de mantenimiento. Un ciberataque ya no es «un problema de IT», puede parar literalmente el edificio.



Conviene detenerse un momento en lo que eso significa de verdad. Existe una dimensión, la digital, que la inmensa mayoría de nosotros apenas atisba por el ojo de la cerradura: vemos iconos, pantallas e informes, pero no vemos el tráfico, los protocolos ni a quienes se mueven por ellos. Y a esa dimensión que casi no vemos le hemos dado, y le seguimos dando cada día, más dominio sobre la nuestra: la física, la de las puertas que se abren, los ascensores que suben, el gas que se descarga y las bombas que impulsan el agua. Cada sistema que conectamos es un músculo más de ese mundo invisible actuando sobre el nuestro. Sus peligros no se ven venir por la calle, se materializan de repente, ya dentro del edificio, cuando el daño es físico. Y pocas disciplinas concentran tantos de esos músculos por metro cuadrado como el *facility management*. Un edificio inteligente es, en la práctica, una granja de colosos dormidos con fuerza física real, que obedecen órdenes llegadas desde un mundo que no vemos. Somos, sin haberlo pretendido, los guardeses de esa frontera entre dimensiones.

El gran apagón ibérico del 28 de abril de 2025 es una referencia obligada, aunque con una precisión importante. Todas las investigaciones oficiales (el comité del Consejo de Seguridad Nacional, el CNI y el panel europeo de expertos de ENTSO-E) descartaron que su origen fuera un ciberataque, atribuyéndolo a una cadena de fallos técnicos del propio sistema eléctrico.

Y precisamente por eso el suministro se restableció en menos de 24 horas. La infraestructura física estaba intacta y los operadores conservaban el control de sus sistemas para el rearranque, con el apoyo de las interconexiones con Francia y Marruecos.

Ahora hagamos el ejercicio que todo *facility manager* debe hacer, porque en ciberseguridad nada es imposible. ¿Y si lo hubiera sido?... Un atacante no provoca la avería y se marcha; permanece dentro de los sistemas de control, corrompe las herramientas de reposición y vuelve a tumbar cada intento de rearranque, como ocurrió en los ataques a la red eléctrica ucraniana de 2015, que obligaron a operar en manual durante meses. El guion, entonces, es otro.

La primera noche: ciudades a oscuras, sin semáforos ni alumbrado, y las baterías de las antenas de telefonía agotándose en cuestión de horas; con ellas caen el 112, los avisos a la población y nuestra capacidad de coordinar equipos.

Día 1: sin bombeo no hay agua en pisos altos ni presión en la red; las gasolineras no despachan (sus surtidores son eléctricos) y solo circula el dinero en efectivo, con los cajeros y datáfonos apagados.

Días 2 y 3: los grupos electrógenos de hospitales y centros de datos agotan un gasóleo cuyas autonomías típicas son de 24 a 72 horas, y no llega reabastecimiento porque la logística que lo transporta también está parada; se pierden las cadenas de frío alimentaria y farmacéutica

A partir de la primera semana: fallo del saneamiento, tensiones de orden público y éxodo urbano. La diferencia entre menos de 24 horas de apagón y varias semanas de colapso no la marca la magnitud de la avería; la marca si el adversario sigue dentro del sistema. Esa es la escala de lo que custodiamos. Ejemplos reales, estos sí de origen malicioso, que ilustran el riesgo:



2017 · Romantik Seehotel Jägerwirt (Austria): un *ransomware* (*software* malicioso que cifra sistemas y datos y exige un pago, normalmente en criptomonedas, para devolver el acceso) bloqueó el sistema de tarjetas-llave de un hotel alpino de cuatro estrellas. La dirección no podía emitir ni reprogramar llaves de habitación en plena temporada alta y acabó pagando el rescate para recuperar el sistema. Es el ejemplo perfecto de cómo un sistema «menor» del edificio (el control de accesos) puede secuestrar la operación completa del negocio.



2021 · Colonial Pipeline (EEUU): un *ransomware* del grupo DarkSide comprometió los sistemas informáticos de facturación de la compañía. Aunque el ataque no alcanzó directamente el control industrial, la empresa detuvo preventivamente el mayor oleoducto del país durante seis días al no poder facturar el suministro, provocando desabastecimiento de combustible en buena parte de la costa este. Se pagó un rescate de 4,4 millones de dólares, del que el FBI logró recuperar después unos 2,3 millones rastreando la transacción. El caso deja dos moralejas: una brecha en la parte «ofimática» puede parar la parte física, y las criptomonedas no eran tan irrastreables como se cree; pero ahora muchas sí lo son.

2023 · Hospital Clínic de Barcelona: el grupo RansomHouse comprometió los sistemas del hospital y exigió 4,5 millones de dólares de rescate. Se cancelaron unas 150 intervenciones quirúrgicas, se suspendieron más de 2000 consultas y sesiones de radioterapia y se aplazaron más de 11 000 visitas externas, con semanas de recuperación y vuelta temporal al papel.

Y hasta aquí lo documentado. Ahora bien; ¿quién nos dice que mañana el objetivo no serán los ascensores de una torre de oficinas o de un hospital, gestionados por mantenimiento remoto a través de la nube del fabricante, con pasajeros dentro y las cabinas inmovilizadas hasta que alguien pague? ¿O el sistema de extinción por gas de nuestro CPD, disparado deliberadamente en la sala equivocada o con los técnicos dentro trabajando y dejándolos encerrados? Técnicamente, nada lo impide si esos sistemas están mal segmentados y expuestos. Que aún no haya ocurrido a gran escala no es un argumento de seguridad, es una cuenta atrás.

¿Qué servicios del edificio pueden verse afectados?

Un listado no exhaustivo de los sistemas de tecnología operativa (OT) que hoy son superficie de ataque en un edificio terciario:

Sistemas de gestión del edificio (BMS/BEMS y protocolos SCADA, BACnet, Modbus, KNX, DALI)

Controlan HVAC, iluminación y consumos. Un atacante que tome el control puede disparar consumos, apagar la climatización o generar averías ficticias.

Control de accesos y presencia

Tarjetas, biometría, tornos y cerraduras inteligentes. Su compromiso permite desde una entrada no autorizada hasta el bloqueo total del edificio, como demuestra el caso del hotel austriaco.

Videovigilancia (CCTV-IP)

Cámaras conectadas a grabadores en red. Pueden usarse como puerta de entrada al resto de la red o simplemente apagarse para facilitar intrusiones físicas.



Detección y extinción de incendios

Muchos paneles modernos son IP. Un ataque puede inhibir alarmas o activar descargas de gas en zonas críticas. Provocar una evacuación con una falsa alarma es, además, una técnica conocida de intrusión física; se aprovecha el caos.

Ascensores y escaleras mecánicas

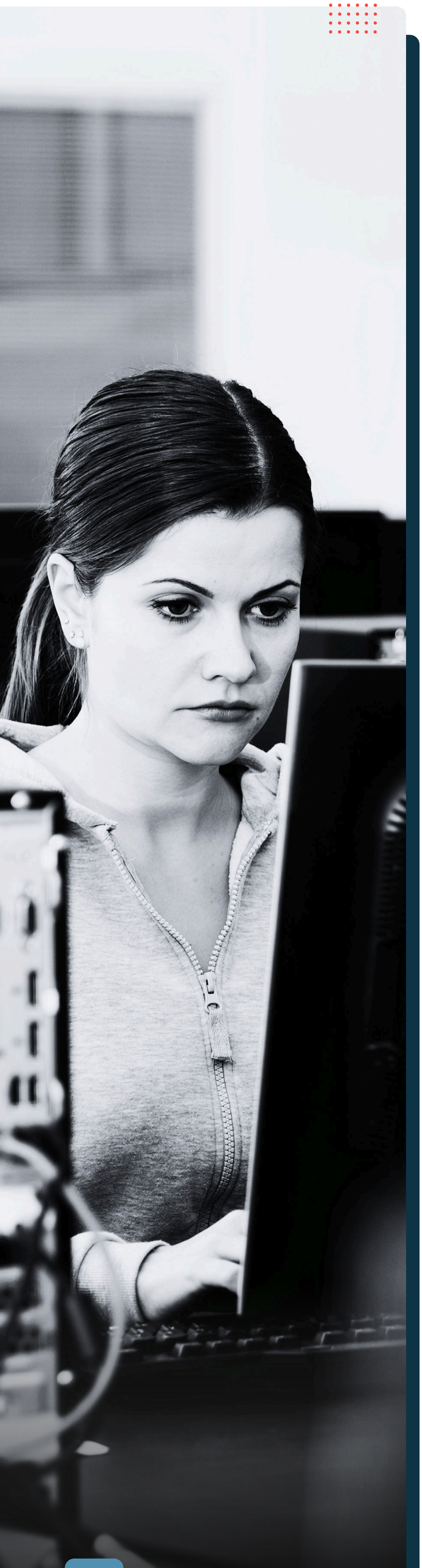
Los sistemas de monitorización y mantenimiento remoto de los grandes fabricantes están conectados a la nube. Cada conexión de fabricante es un acceso de terceros que hay que gobernar contractualmente.

Redes Wi-Fi corporativa y de invitados

El punto de entrada más habitual. Una subred mal configurada puede dar acceso a toda la VLAN, tanto a la red corporativa como a la de operaciones.

Gestión energética y contadores inteligentes

La manipulación de datos o el apagado remoto afectaría a contratos de suministro y certificaciones LEED/BREEAM. Desde ese momento, todos los SLA/KPI medidos perderían su trazabilidad y robustez ante un litigio o disputa.



Sistemas de respaldo y SAI (UPS)

Muchos se monitorizan vía SNMP, un protocolo veterano cuyas versiones 1 y 2c se autentican con simples cadenas de comunidad que, de fábrica, suelen ser «public» y «private». Un atacante dentro de la red las detecta en segundos y puede modificar el estado o apagar el SAI en el peor momento. La medida correcta es exigir SNMP v3 con autenticación y cifrado, o aislar por completo esa gestión.

Aspectos clave que todo *facility manager* debe exigir y supervisar

Segmentación de red obligatoria

Los sistemas del edificio (tecnología operativa, también denominada OT) nunca deben estar en la misma VLAN que la red corporativa o la Wi-Fi de invitados. Se deben usar cortafuegos dedicados y VLAN aisladas, con la segmentación acreditada documentalmente por el integrador.

Inventario actualizado

Saber exactamente qué dispositivos IP hay, quién los mantiene y qué *firmware* llevan, monitorizando quién tiene las claves de acceso y cómo las custodia.

Política de actualizaciones y parches

Muchos fabricantes de BMS o CCTV tardan en publicar parches. Conviene exigir compromisos contractuales escalonados, con penalización por incumplimiento: ante una vulnerabilidad crítica, mitigación o solución provisional en menos de 72 horas y parche definitivo en menos de 30 días. Este criterio debe leerse junto al capítulo de infraestructura de esta misma guía, que fija las 72 horas como referencia para la respuesta inicial.

Acceso remoto seguro

Eliminar o restringir al máximo los accesos VPN directos de fabricantes. Usar *bastion hosts* (servidores blindados a los que solo se accede con doble autenticación) o arquitecturas “Zero Trust”. Un modelo en el que ningún usuario, dispositivo o conexión se considera confiable por defecto, esté dentro o fuera de la red, y cada acceso se verifica continuamente en función de identidad, contexto, dispositivo y comportamiento.

Certificación y cumplimiento

Exigir en los contratos que los integradores de sistemas trabajen conforme a la familia IEC 62443, la norma internacional de referencia para la ciberseguridad de sistemas industriales y de edificio. No es de aplicación obligatoria, pero es el estándar de facto que auditores y aseguradoras toman como estado del arte, y define cuatro niveles de seguridad (SL 1 a SL 4) sobre siete requisitos fundamentales. Como mínimo alternativo, ISO 27001 (sistema de gestión de seguridad de la información). En el plano normativo europeo, la Directiva NIS2 está en vigor desde enero de 2023 y su plazo de transposición venció en octubre de 2024; en España la transposición es aún parcial (Real Decreto-ley 7/2025) y la Ley de Coordinación y Gobernanza de la Ciberseguridad que la completará sigue, al cierre de este texto, en tramitación parlamentaria. Conviene verificar su estado en el momento de redactar cada pliego, porque sus obligaciones de fondo (gestión de riesgos, responsabilidad de los órganos de dirección, notificación de incidentes) emanan de la propia directiva y no del BOE. A ello se suma la Directiva CER para la resiliencia de entidades críticas.

Plan de respuesta a incidentes específico para OT

Los planes de IT clásicos no bastan, porque se ceñían a intrusiones en servidores. Un incidente OT exige coordinar la recuperación física con múltiples actores: INCIBE-CERT (empresas) o CCN-CERT (sector público y organizaciones bajo el ENS), la AEPD si hay datos personales comprometidos, Fuerzas y Cuerpos de Seguridad, bomberos, compañía eléctrica, ascensoristas, cerrajería, operadores de SAI y grupo electrógeno, y las aseguradoras. Y hay que incorporar ya la disciplina de notificación que consagra NIS2: alerta temprana en 24 horas, notificación en 72 horas e informe final en un mes.

Seguro cibernético con cobertura OT

La mayoría de las pólizas excluyen los sistemas de edificio si no se declaran expresamente. Además, exigen certificados de cumplimiento, personal cualificado, simulacros periódicos, registro de incidentes y auditorías independientes. El riesgo de gestionar mal este apartado va desde el encarecimiento de primas hasta la denegación de indemnizaciones. Muchas compañías descubren esto ex post, tras el incidente, que la aseguradora rechaza el pago por la falta de uno solo de esos requisitos formales.





La cadena de seguridad es tan fuerte como su eslabón más débil. En un entorno donde prácticamente todos los sistemas operativos (OT) y de información (IT) están conectados a través del protocolo TCP/IP, cualquier punto débil puede comprometer el conjunto. Y esta vulnerabilidad se ha agravado con la irrupción de la inteligencia artificial. En foros clandestinos ya se ofrecen modelos maliciosos de IA, entrenados para generar código dañino o ejecutar campañas avanzadas de ingeniería social por encargo, lo que reduce drásticamente la barrera de entrada para atacantes sin grandes conocimientos técnicos.

Para el pliego: cláusulas mínimas de ciberseguridad OT

- Segmentación de red acreditada (VLAN OT dedicadas y cortafuegos), con diagrama entregable y verificable en el *commissioning*.
- SLA de parcheo con penalización. Mitigación de vulnerabilidades críticas $\leqslant$ 72 h; parche definitivo $\leqslant$ 30 días.
- Acceso remoto de fabricantes exclusivamente a través de bastón o solución Zero Trust, con doble factor y registro de sesiones.
- Protocolos de gestión seguros. SNMP v3 o equivalente; prohibición de credenciales por defecto; inventario de dispositivos y firmware como entregable vivo.
- Certificaciones exigibles al integrador: conformidad IEC 62443 o, como mínimo, ISO 27001; compromiso de adaptación a NIS2 y normativa española de transposición.
- Obligación contractual de notificación de incidentes al cliente en $\leqslant$ 24 h, alineada con NIS2.
- Derecho de auditoría de seguridad (propia o de tercero independiente) al menos anual y tras cada incidente.
- Declaración expresa de los sistemas OT en la póliza ciber, con evidencias de cumplimiento anexas al contrato.

Conclusión

La ciberseguridad ya no es un «extra» ni responsabilidad exclusiva del departamento de IT. Un *facility manager* que no incluya la dimensión cibernética en sus pliegos y revisiones está exponiendo al edificio, a sus ocupantes y a la propiedad a riesgos muy reales de interrupción grave del servicio y de responsabilidad civil. Incorporar estos criterios desde la fase de diseño o renovación, y mantener una supervisión activa, forma parte de la due diligence moderna en la gestión de instalaciones.

Conviene además ser realistas. Prácticamente ninguna organización, ni siquiera las mejor dotadas, logra cubrir de forma plena y continua todo el cumplimiento normativo en materia de ciberseguridad OT. Las exigencias de RGPD, NIS2, la Directiva CER, ISO 27001 o IEC 62443 superan la capacidad real de la mayoría de las estructuras, y lo más costoso es descubrirlo después de la brecha, cuando a los daños directos se suman las sanciones del regulador y, con frecuencia, la constatación de que el seguro no cubre por la falta de un requisito formal. Nadie puede permitirse hoy sentirse en «pleno cumplimiento»; lo máximo realista es un estado de mejora continua y riesgo controlado.

Las organizaciones que dedican recursos humanos especializados y con formación continua a la protección de los sistemas de edificio (o alianzas estratégicas que los proporcionen) logran tiempos de detección y respuesta significativamente menores, menor exposición a multas y mayor resiliencia operativa. Proteger la red del edificio es proteger el propio edificio; es vigilar el ojo de la cerradura por el que, la otra dimensión, toca la nuestra. Y eso, en última instancia, es nuestra responsabilidad principal.



Inteligencia artificial y FM. ¿En qué punto estamos?



George Darlington

Senior Facilities & Business Improvement Manager
UBS

«La inteligencia artificial (IA) se posiciona como el mayor catalizador para la transformación de esta disciplina».

La misión del *facility management* (FM); coordinar espacios físicos, infraestructuras y servicios para optimizar el rendimiento organizacional, se complica día a día en un entorno cada vez más digitalizado y con masividad de datos. La inteligencia artificial (IA), tecnología que simula procesos cognitivos humanos mediante algoritmos y datos, se posiciona como un catalizador clave para la transformación de esta disciplina. Desde la automatización de procesos hasta la predicción de necesidades, la IA facilita decisiones informadas y en tiempo real, con reducciones de costes y mejoras en la sostenibilidad.



En 2026, la integración de la IA en el FM ha experimentado un crecimiento significativo, impulsado por los avances en el procesamiento de datos y por su convergencia con tecnologías ya cruciales para la profesión, como el Internet de las Cosas (IoT). La red de dispositivos conectados que recolectan y comparten datos en tiempo real para monitorizar activos. Pero antes de entrar en materia conviene situar este capítulo en su verdadera dimensión, que enlaza con el anterior. Si al conectar los sistemas del edificio le dimos al mundo digital, ese que apenas vemos por el ojo de la cerradura, manos sobre el nuestro, con la IA damos un paso más: le damos también criterio e iniciativa. Ya no solo ejecuta órdenes que alguien teclea; observa, decide y actúa. La pregunta que da título a esta guía, cómo contratar, es en el fondo la pregunta de cómo criar y adiestrar a estas criaturas: con qué vallas (segmentación y permisos), con qué correa (supervisión humana) y con qué registro de conducta (trazabilidad). Bien gobernados, estos colosos trabajan para nosotros; sueltos y sin adiestrar, son el riesgo del capítulo anterior elevado al cuadrado.

En este capítulo examinaremos qué tipos de IA existen realmente hoy y cuáles son promesa de futuro; sus aplicaciones prácticas en la gestión de instalaciones; su potencial en la revisión automatizada de Acuerdos de Nivel de Servicio (SLA) e indicadores clave de rendimiento (KPI), enriquecida por la integración con *blockchain*, *smart contracts*, contratos ricardianos y el marco regulatorio que cualquier contratación de IA debe respetar en Europa.

Qué IA existe hoy (y cuál, aún, no está disponible). Un mapa honesto para el *facility manager*

El primer servicio que esta guía puede prestar es de vocabulario, porque el mercado mezcla deliberadamente conceptos de madurez muy distinta. A efectos prácticos, el *facility manager* va a encontrarse tres familias de IA disponibles hoy, y un cuarto concepto que todavía no está disponible para el mercado:

IA predictiva y analítica ('machine learning')

Modelos que aprenden de datos históricos y de sensores para identificar patrones y anticipar eventos: la avería de una enfriadora, el pico de ocupación de una planta, la deriva de consumo de una instalación. Es la familia más madura y la que sostiene el mantenimiento predictivo y la optimización energética.

IA generativa (LLM)

Subtipo especializado en crear contenido nuevo (texto, imágenes, código, síntesis de documentos) a partir de patrones extraídos de datos existentes, apoyado en los grandes modelos de lenguaje (LLM). Opera de forma reactiva a peticiones concretas y su valor en FM está en la redacción de informes, la preparación de pliegos, la síntesis de documentación técnica o la atención a usuarios. Conviene conocer su limitación característica: por sí solo, un LLM no es fiable haciendo cálculos (aunque sí tremendamente rápido), ni citando datos que no se le han proporcionado anteriormente o tiene acceso a ellos, por lo que debe integrarse con fuentes de datos verificadas y supervisión humana.

Sistemas agénticos y multiagente

La frontera actual; combinaciones de modelos de IA con capacidad de planificar, encadenar acciones y coordinarse entre sí para ejecutar flujos de trabajo completos con autonomía acotada y bajo supervisión humana. Es la tecnología que hoy permite, por ejemplo, orquestar una flota de robots de limpieza o encadenar la detección de una anomalía con la apertura de una orden de trabajo, la reserva del técnico y la verificación posterior. Buena parte de lo que el mercado vende como «IA autónoma» pertenece, en realidad, a esta categoría. Permite que IA's supervisen a otras IA's.





Inteligencia artificial general (AGI)

Un sistema no disponible comercialmente, capaz de realizar cualquier tarea intelectual humana con adaptabilidad total entre dominios, sin entrenamiento específico para cada uno. Hoy existe en ámbitos de investigación y de muy escasas corporaciones con recursos para su pago a medida y, confinamiento. La gran diferencia es su capacidad de interacción, orden y reprogramación de otros sistemas. Aun no es un producto contratable. Cuando un proveedor atribuya a su solución capacidades «de AGI», la respuesta correcta del *facility manager* es pedir la especificación concreta de qué hace el sistema, con qué datos, con qué grado de autonomía y con qué supervisión.

Comprender estas diferencias permite seleccionar herramientas adecuadas, dimensionar expectativas y, sobre todo, redactar pliegos que compren capacidades reales y no promesas.

Usos actuales de la inteligencia artificial en la gestión de instalaciones

La IA ha permeado diversas áreas del FM, evolucionando de enfoques reactivos a estrategias proactivas y basadas en datos.

Mantenimiento predictivo

Algoritmos de aprendizaje automático analizan datos de sensores IoT en equipos como sistemas HVAC (climatización) o ascensores, pronosticando averías antes de que ocurran. Esto reduce interrupciones y prolonga la vida útil de los activos. Las estimaciones clásicas del sector (Departamento de Energía de EE. UU. y grandes consultoras) sitúan el ahorro del mantenimiento predictivo entre el 30 y el 40% frente al correctivo, y entre el 8 y el 12% frente al preventivo programado, además de reducir drásticamente las paradas no planificadas.

Optimización energética

La IA evalúa patrones de consumo en tiempo real, ajustando iluminación y climatización según la ocupación y las variables externas. En los modelos de trabajo híbrido, donde la demanda de espacios varía por días y por horas, la integración con los sistemas de gestión de edificios (BMS) permite una asignación eficiente de recursos, alineada con los objetivos de sostenibilidad y con una regulación ambiental cada vez más exigente.

Actualmente incluso, combinada con plantas solares de cualquier tamaño, permite ir más allá de los ahorros, entrando en la soberanía energética, traspasando la frontera del PayBack hacia el ROI real durante bastantes años, con el arbitraje.

Cargar almacenamiento en periodo barato y poner los excedentes operativos a disposición del operador en el periodo caro.

Gestión de espacios y seguridad (con una cautela legal imprescindible).

Los datos de sensores de ocupación y el análisis de vídeo permiten monitorizar la utilización de áreas, optimizar distribuciones y facilitar reservas dinámicas en oficinas flexibles. En seguridad, el reconocimiento de patrones identifica anomalías (intrusiones, accesos fuera de horario, congestiones en vías de evacuación) y mejora los protocolos de emergencia.

Ahora bien: en España, cualquier tratamiento de datos de presencia, vídeo o biometría de trabajadores entra de lleno en el RGPD, en la LOPDGDD y en la doctrina de la AEPD, que ya ha demostrado que sanciona con dureza los tratamientos biométricos sin base legal adecuada (la mayor multa de su historia, de diez millones de euros, fue precisamente por reconocimiento facial).

Además, el Reglamento europeo de IA prohíbe expresamente el reconocimiento de emociones en el lugar de trabajo. La regla práctica para el *facility manager*: priorizar datos agregados y anonimizados, realizar evaluación de impacto (EIPD) antes de desplegar, informar a la representación legal de los trabajadores y descartar cualquier caso de uso orientado a la vigilancia individualizada del empleado.





Robótica orquestada

Tanto los robots no humanoides (aspiradoras autónomas, vehículos de limpieza guiados, drones de inspección) como los humanoides emergentes, están cambiando las operaciones. Cuando estas unidades se conectan y coordinan mediante sistemas agénticos, se logra una orquestación autónoma. Planificación dinámica de rutas a partir de los patrones de uso y de las cámaras del edificio, colaboración en tiempo real entre unidades, respuesta inmediata a incidencias y ejecución continua. Esta integración eleva la productividad, reduce riesgos laborales y permite reasignar personal a actividades de mayor valor estratégico.

Realidad aumentada y virtual como extensión de la IA

La realidad aumentada (AR) y la realidad virtual (VR) complementan de forma natural estas capacidades. Un ejemplo concreto: un técnico de mantenimiento con gafas AR frente a una climatizadora recibe superpuestos el modelo BIM del equipo, su historial de órdenes de trabajo y la guía paso a paso de la intervención, mientras un experto remoto ve lo mismo que él y puede asistirle o supervisarle en directo.

En VR, los equipos se forman en maniobras de alto riesgo (trabajos en tensión, espacios confinados, descargas de extinción) sin exponerse a ellas. Combinadas con IA e IoT, estas tecnologías reducen errores en las intervenciones, aceleran la transferencia de conocimiento y recortan tiempos de inactividad.

Automatización administrativa y de cumplimiento

La IA automatiza funciones administrativas como la programación de servicios de limpieza o el control de inventarios, y los cuadros de mando impulsados por IA simulan escenarios de inversión, evaluando impactos en infraestructuras y proveedores.

Destaca especialmente su eficiencia en el reemplazo de tareas masivas y burocráticas que, aunque necesarias, aportan escaso valor añadido final. En el compliance interno y externo (auditorías repetitivas de normas, certificaciones y reportes reglamentarios) consume recursos humanos significativos sin contribuir directamente al negocio. Su automatización mediante IA, combinada con blockchain para la trazabilidad, libera personal cualificado, reduce errores y permite enfocarse en decisiones estratégicas.

Los dos frenos reales: competencias laborales y alianzas empresariales

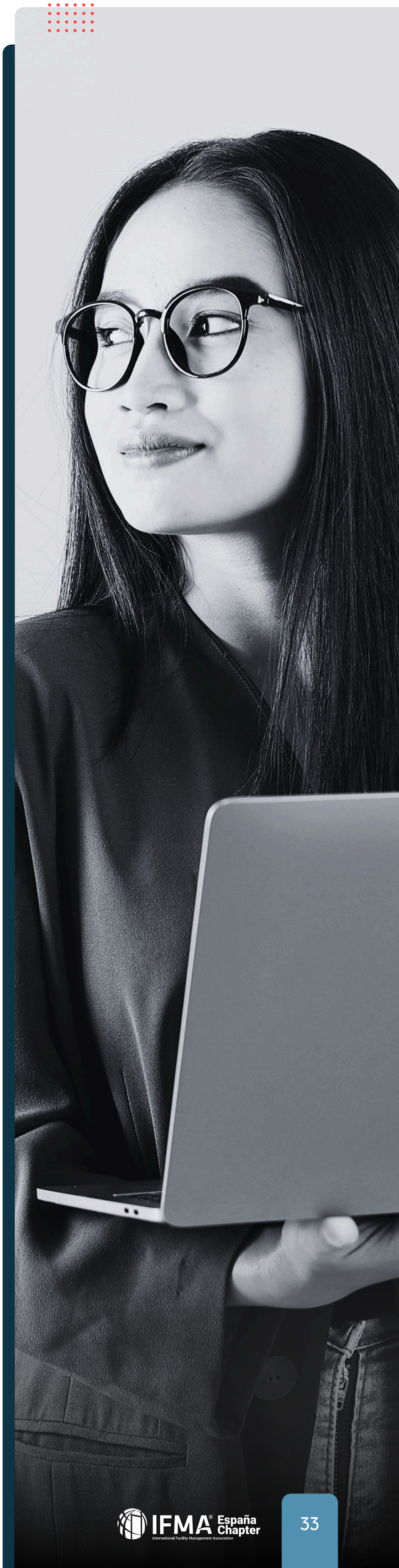
A pesar de ventajas económicas claras, muchas organizaciones de FM permanecen rezagadas en la adopción de estas tecnologías, y quienes invierten temprano capturan eficiencias estructurales mientras, el resto, acumula gasto reactivo y menor agilidad. Dos frenos explican buena parte del retraso.

El primero es de competencias. La formación en evaluación tecnológica no ha acompañado a la velocidad de adopción, y eso afecta a toda la cadena de decisión, desde la operación hasta los comités que aprueban las inversiones.

Entender las tecnologías emergentes, identificar sus puntos de aplicación real en cada instalación, justificar económica y técnicamente su implantación y evaluar con objetividad a las empresas oferentes son habilidades que, aún, no forman parte del bagaje habitual de la profesión; lo que frena la adopción y genera una dependencia excesiva de consultores externos extremadamente caros. Cerrar esa brecha con formación específica es, probablemente, la inversión con mejor retorno de todas las que describe este capítulo.

El segundo es de ecosistema. La escasez de alianzas estratégicas entre corporaciones consolidadas y *startups* especializadas en IA, robótica o AR/VR. Las empresas establecidas no abren fácilmente sus puertas a pilotos a escala, mientras las *startups* no logran madurar sin acceso a entornos reales de gran volumen.

Es un círculo vicioso frecuente en nuestro entorno («no encuentro trabajo porque no tengo experiencia, y no adquiero experiencia porque nadie me da trabajo»), en contraste con otros mercados donde la colaboración temprana y el riesgo compartido han acelerado la innovación. Romper este patrón mediante alianzas estructuradas es esencial para escalar soluciones en FM.





La potencia de la IA en revisiones de cumplimiento (SLA/KPI), integrada con *blockchain* y *smart contracts*

Una de las contribuciones más impactantes de la IA en FM es su capacidad para realizar revisiones automatizadas del cumplimiento de SLA y KPI. Históricamente, estas evaluaciones dependían de revisiones manuales, susceptibles a inexactitudes, retrasos y discrepancias de interpretación entre las partes. La IA procesa datos multifuente (sensores, registros y métricas operativas) para monitorizar el cumplimiento en tiempo real. En un edificio inteligente, puede rastrear indicadores como el tiempo medio de resolución de fallos, generar alertas ante desviaciones y producir informes predictivos, acelerando auditorías que pasan, de días a minutos.

La integración con *blockchain* (un registro distribuido y compartido de transacciones que no puede alterarse una vez consolidado) eleva estas capacidades. Conviene precisar qué aporta exactamente: *blockchain*. No cifra la información, sino que garantiza su integridad e inalterabilidad; una vez registrado un dato de cumplimiento, ninguna de las partes puede modificarlo retroactivamente, lo que previene manipulaciones y da a cada asiento valor probatorio en caso de disputa.

Sobre esa base, los *smart contracts* (códigos autoejecutables que activan acciones automáticas cuando se cumplen condiciones predefinidas) juegan un papel primordial. Aplicar penalizaciones por incumplimiento de SLA, liberar bonificaciones por superar KPI o desencadenar pagos automáticos a proveedores una vez que la IA verifica las métricas, reduciendo disputas y agilizando los flujos financieros. Complementariamente, los contratos ricardianos, vinculan los términos legales redactados en prosa natural con el código del *smart contract*, de modo que las intenciones contractuales resulten claras y vinculantes tanto para las partes humanas como para los sistemas automatizados. El documento detalla los SLA en términos accesibles mientras, su componente codificado, interactúa con la IA para validar los KPI sobre la *blockchain*.

Dos cautelas separan aquí el entusiasmo de la buena contratación. La primera es el llamado “problema del oráculo”. La cadena garantiza que el dato no se altera, pero no que el dato fuera cierto al entrar. Si el sensor está descalibrado o la fuente es errónea, la *blockchain* conservará ese error para siempre con apariencia de verdad. Por eso el pliego debe exigir calibración certificada y periódica de los sensores que alimentan el sistema, redundancia de fuentes para las métricas que activan pagos o penalizaciones y, un procedimiento pactado de impugnación del dato con arbitraje de tercero.

La segunda es jurídica. El contrato ricardiano carece hoy de reconocimiento específico en el Derecho español (no así en el anglosajón), por lo que el contrato tradicional firmado por las partes debe prevalecer expresamente sobre el código, y debe mantenerse una cláusula humana de resolución de disputas (mediación, arbitraje o jurisdicción) por encima de cualquier ejecución automática, con la posibilidad de revertir o compensar una penalización ejecutada por error.

Con esas salvaguardas, las ventajas de la sinergia son sustanciales: integridad y trazabilidad de los datos de cumplimiento en contratos de mantenimiento, auditorías (internas y legales) más rápidas y baratas sobre registros inalterables, y, en escenarios multiparte como instalaciones compartidas, una confianza colaborativa que elimina intermediarios y automatiza ejecuciones. No solo se robustece la supervisión de SLA y KPI: se construye un marco de trabajo transparente que evita una cantidad ingente de posibles disputas entre las partes.

El marco regulatorio: contratar IA en Europa

Ninguna contratación de IA en FM puede diseñarse hoy de espaldas al Reglamento europeo de Inteligencia Artificial (Reglamento (UE) 2024/1689), de aplicación directa en España sin necesidad de transposición y con un calendario escalonado: las prácticas prohibidas (entre ellas, el reconocimiento de emociones en el trabajo) son exigibles desde febrero de 2025, las obligaciones para los modelos de IA de propósito general desde agosto de 2025, y el grueso de las obligaciones para los sistemas de alto riesgo se aplica a partir de agosto de 2026.



Para el *facility manager*, la consecuencia práctica es doble: primero, clasificar cada caso de uso (la mayoría de las aplicaciones de FM serán de riesgo limitado o mínimo, pero las que afectan a trabajadores, como el control de accesos biométrico, pueden escalar de categoría). Segundo, trasladar al proveedor, vía pliego, la obligación de acreditar esa clasificación, la documentación técnica y los mecanismos de supervisión humana.

Dado que el despliegue normativo sigue en marcha, conviene verificar el estado de aplicación en el momento de redactar cada contrato.

Para el pliego: qué exigir al contratar servicios de IA en FM

- Propiedad del dato: los datos generados por la instalación son propiedad exclusiva del cliente; prohibición de usarlos para entrenar modelos del proveedor sin autorización expresa.
- Portabilidad y salida: formato abierto de exportación de datos y modelos de configuración; plan de reversión a origen al término del contrato.
- Trazabilidad y explicabilidad: capacidad de justificar cada alerta, predicción o penalización con los datos que la originaron.
- Clasificación acreditada del sistema bajo el Reglamento de IA, con documentación técnica y declaración de conformidad cuando proceda.
- Supervisión humana obligatoria en toda decisión con efecto económico (penalizaciones, pagos) o sobre personas.
- Cumplimiento RGPD demostrable en cualquier tratamiento de ocupación, vídeo o biometría: EIPD previa, minimización y agregación de datos, información a la representación de los trabajadores.
- Calidad del dato de origen: calibración certificada de sensores, redundancia de fuentes para métricas contractuales y procedimiento de impugnación del dato.
- SLA del propio sistema de IA: precisión mínima acordada, tratamiento de falsos positivos/negativos y responsabilidad por decisiones erróneas del modelo.
- Prevalencia del contrato firmado sobre el código *(smart contracts)* y cláusula de resolución de disputas con reversibilidad de ejecuciones automáticas periódicas.

Una reflexión final: Europa y el coste de esperar

El avance, sin embargo, no es uniforme. La hiper-burocratización que caracteriza a gran parte del tejido empresarial y administrativo europeo (procesos lentos, múltiples capas de aprobación, regulaciones superpuestas y una acusada aversión cultural al riesgo) está situando al continente en posición rezagada en la carrera tecnológica global. Mientras regiones con enfoques más ágiles aceleran la adopción masiva de IA, robótica coordinada, AR/VR y modelos de colaboración *startup*-corporación, Europa acumula demoras que erosionan su competitividad estructural.

Este retraso no es meramente coyuntural. El día en que la inercia se revierta, muchas organizaciones podrían descubrir que ya no lideran sus propias operaciones, sino que operan bajo la coordinación efectiva de los actores (proveedores globales, plataformas tecnológicas, socios que sí invirtieron temprano) que alcanzaron mayor excelencia operativa. En FM, esto se traduciría en dependencia creciente de ecosistemas externos para la gestión de activos críticos, la optimización energética, el cumplimiento normativo y la seguridad, con pérdida de soberanía operativa y márgenes cada vez más estrechos.

Quien hoy construye las capacidades (tecnológicas, competenciales y de colaboración) será quien dicte las reglas del juego mañana. Para los *facility managers* y las organizaciones europeas el mensaje es claro: la adopción decidida, la formación intensiva, la eliminación selectiva de burocracia autoimpuesta y la creación de alianzas estratégicas han dejado de ser opciones deseables para convertirse en requisitos de competitividad.



Conclusión

La inteligencia artificial transforma la gestión de instalaciones a través de tres familias tecnológicas ya operativas y disponibles para todos, independientemente de su tamaño: (predictiva, generativa y agéntica) que, optimizan las operaciones diarias. Su integración con blockchain, potenciada por *smart contracts* y contratos ricardianos, eleva el cumplimiento de SLA y KPI a niveles de eficiencia y transparencia inéditos, siempre que la contratación incorpore las salvaguardas de calidad del dato, supervisión humana y prevalencia jurídica del contrato.

A una dimensión que apenas vemos por el ojo de la cerradura le hemos dado primero las llaves y ahora el criterio sobre nuestro mundo. La respuesta no es cerrar esa puerta, que ya no tiene vuelta atrás, sino agrandar la cerradura.

Formación para ver más, gobernanza para medir mejor y contratos que hagan visible, auditable y reversible lo invisible. Los *facility managers* que adopten estas tecnologías con ese criterio (comprando capacidades reales, exigiendo cumplimiento regulatorio racional y formando a sus equipos) no solo cumplirán con estándares rigurosos; posicionarán al FM donde le corresponde: como pilar estratégico del éxito organizacional y como el oído más atento en la frontera entre dos dimensiones (digital vs. físico).

AUTORES PARTICIPANTES



Carmen Velasco

Columat

Growth & Marketing Leader con trayectoria en escalado de ecosistemas SaaS y Phygital. Estratega con experiencia liderando el crecimiento acelerado de compañías tecnológicas con un enfoque transversal en el sector de *facility management*. Experta en la integración de soluciones de Hardware & Software aplicadas a la optimización de activos y eficiencia operativa. Especialista en liderar equipos multidisciplinares y diseñar hojas de ruta de crecimiento para entornos de PropTech e Industria 4.0, transformando la complejidad técnica en valor de negocio y posicionamiento de mercado dominante.



Juan Ignacio Herrero

Ricoh España y Portugal

Ingeniero de Telecomunicaciones y Máster en Liderazgo Digital en ESADE, cuenta con más de 15 años de experiencia en el sector TI. A lo largo de su trayectoria ha desempeñado funciones en I+D, desarrollo de negocio, gestión de servicios y preventa. Actualmente lidera la estrategia de innovación en soluciones Workplace de Ricoh España y Portugal, impulsando la transformación digital de las organizaciones mediante tecnologías que mejoran la colaboración, la productividad y la experiencia del empleado.



Glòria Ausió

Ricoh España y Portugal

Directora de Recursos Humanos de Ricoh España y Portugal, y miembro del Comité Ejecutivo de Iberia, así como del Comité de Gestión de Riesgos y del equipo ejecutivo de Recursos Humanos para EMEA. Es responsable del Strategic Business Partnering, la estrategia de Personas y Cultura y la gestión del cambio de la compañía. Ha impulsado la transformación del negocio hacia una compañía global de servicios digitales mediante una estrategia de talento, el desarrollo organizativo y el cambio cultural, alineados con los objetivos ESG (Environmental, Social and Governance).

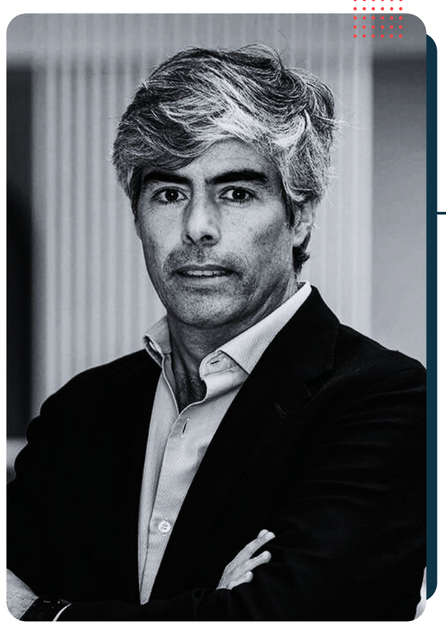


George Darlington

UBS

Ingeniero industrial y Executive MBA, con 25 años dirigiendo instalaciones y sedes corporativas de alta exigencia en Reino Unido y España (UBS, American Express, Penguin Random House, DHL). Especializado en la digitalización de la operación –IoT, inteligencia artificial y gobierno del dato aplicados al mantenimiento, la energía y el control de contratos por SLA/KPI– y en eficiencia energética y autoconsumo fotovoltaico. En la sede de UBS en Londres implantó una plataforma de IoT, IA y validación de datos sobre 65 000 m² de operación, con una reducción del 85% en el tiempo de gestión del cumplimiento contractual. Asesor de tecnología aplicada y *contract management* en IFMA España e IWFM (Reino Unido).

IFMA ESPAÑA



Alfonso Díaz del Río

Presidente de IFMA España

Ingeniero de Caminos Canales y Puertos por la Universidad Politécnica de Madrid y Executive MBA por ESADE Business School. A lo largo de más de 18 años de experiencia en el sector de las infraestructuras y servicios, ha ocupado diferentes puestos y geografías (España, EEUU y Australia) en Ferrovial y Serveo. Miembro de la Junta Directiva de IFMA España desde 2023, donde además ha sido sponsor de la Comisión de FM del Sector Público y la Comisión de Tecnología. Actualmente es Director de Estrategia y Mercados en Serveo, desde donde se impulsa la estrategia, el M&A y el desarrollo de negocio de la compañía en los sectores de Corporate, Industria, Salud, Infraestructuras y Government.



Ángela García Juste

Líder de la Comisión de Tecnología de IFMA España

Licenciada en Ciencias Ambientales por la Universidad Autónoma de Madrid, Máster en Gestión y Planificación por la Universidad de Liverpool y PSDV por ESIC Business School. Más de 10 años de experiencia en el sector del *facility management*, ayudando a las organizaciones a optimizar todos los procesos relacionados con activos, infraestructuras, tecnologías existentes, personas y procesos. En la actualidad, dirige la compañía FAMA, aliado tecnológico para la gestión integral de activos e infraestructuras de las organizaciones.

IFMA® España Chapter
International Facility Management Association

Somos la Asociación Española de Facility Management

IFMA España es una asociación sin ánimo de lucro que tiene como objetivo desarrollar y promocionar la disciplina del *facility management* en nuestro país, así como reconocer y posicionar la figura profesional del *facility manager* en todas las organizaciones. Impulsamos nuestro conocimiento, valor y crecimiento colectivos para que los profesionales se desempeñen al más alto nivel.

Más información

ifma-spain.org

IFMA® España Chapter
International Facility Management Association

Únete a nuestra comunidad

facility management





eventos

conocimiento





Más información en la web

ifma-spain.org/unete

Título

Cómo contratar servicios IT aplicados al FM

Edición

Octubre de 2026

Diseño y maquetación

Óliver Mayorga López
IFMA España

Elaborado con ❤ por IFMA España

Quedan reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida ni incorporada a un sistema informático, ni está permitida su transmisión en cualquier forma o cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros medios, sin el permiso previo y por escrito de IFMA España.

IFMA® España Chapter

International Facility Management Association

www.ifma-spain.org