IFMA™ España Chapter
International Facility Management Association

FMM FACILITY MANAGEMENT MAGAZINE

Número 34 | Junio 2026

El FM ante las ciberamenazas en la continuidad operativa

ESPECIAL #FM_CIBERSEGURIDAD

Editorial

La ciberseguridad como pilar de la continuidad operativa

La digitalización ha transformado profundamente la manera en que concebimos, gestionamos y operamos los edificios. La incorporación de sistemas inteligentes, plataformas conectadas y tecnologías de automatización ha permitido alcanzar niveles sin precedentes de eficiencia, sostenibilidad y capacidad de gestión. Sin embargo, esta evolución también ha introducido un nuevo factor crítico para la continuidad operativa: la ciberseguridad.

Hoy resulta imposible hablar de resiliencia organizacional sin considerar la protección de los entornos digitales que sustentan la operación de los activos físicos. Los edificios modernos integran sistemas de climatización, control de accesos, gestión energética, sensores IoT y plataformas de supervisión que, además de optimizar el rendimiento, amplían la superficie de exposición frente a potenciales amenazas. La interrupción o vulneración de cualquiera de estos sistemas puede afectar directamente a la seguridad de las personas, la continuidad del negocio y la reputación de la organización.

En este contexto, la ciberseguridad ha dejado de ser una responsabilidad exclusiva de los departamentos de tecnología para convertirse en una cuestión estratégica que involucra de forma directa al Facility Management. La protección de los activos conectados exige una visión integral que combine tecnología, procesos y personas, así como una estrecha colaboración entre todas las áreas implicadas en la gestión y operación de los espacios.

La experiencia demuestra que la diferencia entre una organización vulnerable y una organización resiliente no suele radicar únicamente en las herramientas implementadas, sino en su capacidad para anticipar riesgos, definir responsabilidades, coordinar respuestas y desarrollar una cultura de seguridad compartida. A medida que los edificios se vuelven más inteligentes, también deben ser más seguros y mejor gobernados.

El Facility Management afronta así el reto de liderar entornos cada vez más conectados garantizando su fiabilidad, disponibilidad y protección. Conocer los activos críticos, gestionar adecuadamente los accesos y preparar a las organizaciones para responder ante incidentes ya no son elementos diferenciales, sino requisitos esenciales para una gestión responsable. Porque en la era de los edificios inteligentes, la resiliencia no es fruto de la improvisación, sino de una estrategia integrada desde el primer momento.

Marta Sevila Marinas
Sponsor de la Comisión de Comunicación de IFMA España

Continuidad operativa en entornos conectados: el valor de los datos en mantenimiento

Centralizar los datos de la operación es clave para evitar paradas inesperadas o garantizar la seguridad de la información

En entornos conectados, los riesgos que pueden detener una operación de mantenimiento ya no están asociados únicamente al fallo de un activo. La pérdida de acceso a órdenes de trabajo, históricos de mantenimiento o información crítica sobre los equipos puede tener un impacto similar en la continuidad operativa.

Fracttal

Durante años, la continuidad operativa estuvo asociada a la capacidad de prevenir averías en activos y reducir tiempos de inactividad. Sin embargo, la transformación digital de edificios e infraestructuras ha ampliado el alcance de este concepto.

Hoy, una incidencia puede detener una operación por el fallo de un activo, pero también puede hacerlo la falta de acceso a información crítica, la ausencia de un histórico de registros sobre el activo o la existencia de datos dispersos entre múltiples sistemas y departamentos.

De hecho, en muchos entornos de Facility Management todavía conviven herramientas desconectadas, documentación manual o procesos que dependen excesivamente de personas concretas. Y cuando la información no está centralizada, la capacidad de reacción se reduce precisamente en los momentos más críticos.

El reto de un mantenimiento conectado

La incorporación de **tecnologías como IoT o plataformas cloud impulsadas por IA** ha multiplicado la cantidad de información disponible dentro de los edificios y operaciones sobre el estado de los activos, las intervenciones realizadas, el rendimiento de los equipos y la planificación del mantenimiento. El reto ya no es únicamente capturar esa información, sino convertirla en una herramienta útil para la toma de decisiones operativas.

La gestión centralizada del mantenimiento adquiere un papel estratégico. Disponer de una única plataforma donde activos, incidencias, órdenes de trabajo e históricos estén conectados ha transformado su operativa, permitiéndoles actuar con mayor rapidez y minimizar el impacto de las interrupciones.

Pero cuanto más centralizada está la operación, **más crítica resulta su protección**. Un entorno donde toda la información de tu operación se almacena en una misma plataforma es también un entorno donde un acceso no autorizado o una interrupción del sistema puede paralizar varias capas de la operación.

Problemáticas como la falta de visibilidad, la seguridad de los datos o la dificultad para

anticipar incidencias siguen siendo habituales en entornos operativos conectados. Según el informe Diagnóstico del Downtime Industrial 2026 elaborado por Fracttal, **solo el 20% de las organizaciones conoce el coste real de una parada** cuando ocurre, mientras que el 65% reconoce sufrir incidencias sin previo aviso. Estos datos reflejan hasta qué punto la accesibilidad y trazabilidad son factores críticos para que estas empresas minimicen interrupciones y mejoren su capacidad de respuesta.

Proteger la operación para proteger los datos

En entornos de Facility Management, donde edificios e infraestructuras están cada vez más conectados a redes corporativas, plataformas cloud y dispositivos IoT, la superficie expuesta a incidentes de seguridad se ha ampliado. Un ataque que afecte a los sistemas de gestión operativa puede traducirse directamente en pérdida de control sobre activos críticos e incapacidad para ejecutar órdenes de trabajo, consultar planes de mantenimiento preventivo o acceder a registros históricos de los activos.

Pero proteger los datos operativos no consiste únicamente en evitar ataques externos. También implica garantizar que la organización pueda seguir funcionando con normalidad ante cualquier tipo de incidencia: desde un acceso no autorizado hasta la pérdida accidental de registros históricos.

En este sentido, elementos como los **modelos de acceso controlado por rol**, la trazabilidad completa de cada intervención o el almacenamiento seguro en **entornos cloud certificados** pasan a ser requisitos operativos. El FM manager necesita poder auditar quién hizo qué, cuándo y sobre qué activo, como mecanismo de control ante incidencias de seguridad.

La evolución del Facility Management está llevando al mantenimiento hacia un papel cada vez más estratégico dentro de las organizaciones. Más allá de corregir averías o ejecutar tareas preventivas, el **mantenimiento se ha convertido en una fuente crítica de información operativa**, ya que concentra buena parte del conocimiento sobre el estado de los activos, las intervenciones realizadas y los riesgos asociados a la operación.

Proteger esa información es también proteger la capacidad de las organizaciones para planificar, ejecutar y optimizar sus estrategias de mantenimiento.

FRACTTAL

Smart buildings y mantenimiento: el reto pendiente

Los edificios ya generan datos casi en tiempo real, pero muchas operaciones siguen reaccionando demasiado tarde

La digitalización de edificios e infraestructuras avanza rápidamente gracias a los sensores IoT, automatización, sistemas BMS y plataformas de monitorización capaces de recopilar información en tiempo real sobre prácticamente cualquier aspecto de la operación. Sin embargo, disponer de más información no siempre significa disponer de una operación más inteligente.

Abelardo Oropeza, Regional Sales Manager

Temperatura, calidad ambiental, consumo energético, rendimiento de activos o alarmas técnicas generan datos de forma constante. Ello hace que, en muchos entornos, los edificios ya sean capaces de detectar lo que ocurre en sus instalaciones. Pero **las decisiones de mantenimiento siguen dependiendo de dinámicas reactivas** y procesos manuales que ralentizan la capacidad de respuesta. Y ese retraso no solo tiene coste operativo: reaccionar tarde ante una anomalía también puede significar reaccionar tarde ante un incidente de seguridad.

La transformación digital del Facility Management ha avanzado con fuerza en la capa tecnológica de los edificios, pero **todavía existe una brecha importante entre monitorizar y actuar**. Y esa diferencia es precisamente la que determina si una infraestructura puede operar de forma realmente eficiente.

Del edificio monitorizado a la operación inteligente

La mayoría de edificios inteligentes ya dispone de información suficiente para detectar desviaciones, anomalías o comportamientos fuera de lo habitual en sus activos e instalaciones. El problema sigue siendo transformar esa información operativa en decisiones más ágiles y orientadas a una operación más predictiva, tal y como refleja el informe El Estado del Mantenimiento de Fracttal.

Lo cierto es que muchas organizaciones continúan gestionando incidencias una vez que el problema ya ha impactado en la operación, incluso aunque existieran señales previas en los sistemas de monitorización. Así, **buena parte de las operaciones de mantenimiento sigue funcionando bajo modelos reactivos**, donde las intervenciones se producen después del fallo y no antes de la incidencia.

El paso hacia una operación más inteligente requiere evolucionar desde la simple monitorización hacia modelos capaces de actuar sobre la operación prácticamente en tiempo real. Esto implica **integrar mantenimiento, operación y monitorización dentro de una misma estrategia operativa**, priorizar activos críticos según su comportamiento y utilizar realmente los datos para anticipar incidencias antes de que afecten al servicio.

> **“El reto ya no es recopilar datos, sino reaccionar a tiempo ante lo que ocurre en la operación.”**

Anticipación y capacidad de respuesta

Un edificio no es inteligente únicamente por la cantidad de tecnología que incorpora. Lo es cuando toda esa información contribuye a acortar la velocidad de reacción, un factor crítico para minimizar interrupciones en entornos complejos y conectados.

Integrar monitorización, mantenimiento y operación dentro de una misma estrategia permite aprovechar realmente el potencial de los sistemas desplegados en las instalaciones. Pero la evolución de los smart buildings apunta hacia un escenario todavía más avanzado, donde las operaciones no solo reaccionen más rápido, sino que sean capaces de **anticiparse automáticamente a muchas incidencias gracias al uso de inteligencia artificial** y analítica avanzada.

La combinación de sensores IoT, plataformas cloud y modelos basados en IA está permitiendo evolucionar desde edificios monitorizados hacia operaciones más inteligentes y preparadas para anticipar el fallo.

La inversión en edificios inteligentes solo alcanza su verdadero impacto cuando mantenimiento y operación evolucionan al mismo ritmo que la tecnología instalada. Y eso incluye tanto la capacidad de anticipar el fallo como la de garantizar que los sistemas que lo detectan sean seguros, trazables y estén siempre disponibles."

Fracttal One es el primer software de mantenimiento que conecta tu operación con el LLM que elijas. Trabaja con información real de tus activos y OTs desde Claude, ChatGPT o Gemini. Sin desarrollos ni migraciones adicionales, y con la garantía de seguridad de tus datos.

Más de 375 profesionales en el IFM Summit Madrid 2026

El sector del facility management se enfrenta a un cambio de paradigma impulsado por la inteligencia artificial, los datos y la automatización. Ese fue el eje del IFM Summit Madrid 2026, que reunió en la capital a más de 375 profesionales de operaciones, mantenimiento y gestión de edificios.

Bajo el lema "¿Vamos a romper el ciclo?", el encuentro puso sobre la mesa el debate sobre la **transición desde modelos reactivos hacia enfoques más predictivos y estratégicos**, donde la tecnología y la colaboración entre equipos se convierten en elementos centrales.

Durante el encuentro, directivos de compañías como **ALE-HOP, Elecnor, FNAC, Grupo EULEN, IKEA, The Adecco Group, OdiseIA, Verisure**, analizaron cómo están evolucionando sus modelos operativos hacia estructuras más eficientes y con mayor capacidad de decisión en entornos complejos.

La inteligencia artificial ocupó un papel protagonista, tanto en las sesiones estratégicas como en las ponencias especializadas, donde se abordó su impacto directo en la toma de decisiones y en la evolución de los equipos de operaciones.

El evento también dedicó un espacio a la innovación tecnológica, con la participación de **18 empresas del ecosistema FM que presentaron nuevas soluciones y servicios** para la gestión de activos, mantenimiento y edificios inteligentes.

Principales ganadores de los Infraspeak FM Awards 2026:

Champion del Año: Jose Luis Yubero Gil Dreamfit

Operación de FM Más Colaborativa: Elecnor

Operación de FM Más Inteligente: Unica Group

Operación de FM Más Integrada: Trébol

Líder en Innovación en FM: Sage

Operación de FM Más Eficiente (Oro): The Charming Concept, Club de los Menceyes Tenerife, ALE-HOP

Pre-lanzamiento durante el IFM Summit Madrid

Compartimos en exclusiva el primer capítulo del libro de Rui Santos Couto: la guía para salir del modo reactivo y liderar con propósito.

La mayoría de los FM siguen atrapados en el ciclo de "apagar fuegos". Este libro propone un camino claro —**en cuatro etapas, del reactivo al cognitivo**— para transformar el FM en un motor de valor: datos gobernados, contratos por resultados, automatización e IA al servicio de equipos que deciden mejor y antes.

Incluye el Iceberg del FM, un **roadmap trimestral** y **plantillas para construir business cases y liderar el cambio** con indicadores que importan al negocio.

Descarga el primer capítulo

INFRASPEAK

La ciberseguridad, aliado estratégico del Facility Management para garantizar la continuidad operativa

Durante décadas, la percepción general sobre el Facility Management ha estado centrada en una visión física y tradicional. Al pensar en este sector, pensábamos en el personal que asegura la limpieza de las oficinas, que revisa los sistemas de climatización o que controla los accesos a los edificios.

Sin embargo, en la era de los edificios inteligentes y los espacios de trabajo hiperconectados, el FM y la infraestructura digital se han fusionado hasta volverse inseparables. Actualmente, las **empresas de servicios integrados no solo manejamos herramientas tradicionales, también gestionamos un inmenso flujo de datos, redes de sensores (IoT) y sistemas automatizados.**

En este nuevo ecosistema, **la ciberseguridad ya no es problema exclusivo del departamento de IT**, sino que se ha convertido en una aliada estratégica del *Facility Management*, para garantizar la continuidad operativa de cualquier organización.

Si bien las nuevas tecnologías están ayudando a optimizar recursos y mejorar la eficiencia, esta conectividad también implica riesgos. Una simple vulnerabilidad puede paralizar por completo la actividad de una empresa. Y, cuando hablamos de vulnerabilidades en los sistemas de FM, el impacto de un ciberataque trasciende la pantalla del ordenador y puede tener consecuencias inmediatas en el mundo físico.

Estas amenazas, que no siempre llegan a través de ataques a los ordenadores centrales, pueden infiltrarse a través de puertas de entrada aparentemente inofensivas, como termostatos inteligentes o cámaras de seguridad. Y, en entornos críticos y sensibles, como un hospital, un centro de datos o una planta de producción industrial, una pérdida de control físico desencadena una crisis operativa total, generando no solo pérdidas económicas, sino también un daño reputacional incalculable.

Desde ISS Iberia, además del cuidado del entorno físico, también nos posicionamos como la primera línea de defensa entre lo físico y lo digital. **Contamos con una estructura de *Global Information and Cyber Security Services* (GICSS)**, cuyo propósito es proteger las operaciones, generar confianza absoluta en nuestros servicios y consolidarnos como el proveedor de *Facility Management* más seguro de la industria.

Cuando hablamos de vulnerabilidades en los sistemas de FM, el impacto de un ciberataque trasciende la pantalla del ordenador y puede tener consecuencias inmediatas en el mundo físico.

Para aportar valor tangible y proteger las operaciones de nuestros clientes, hemos incorporado la ciberseguridad en el núcleo de nuestro trabajo diario, aplicando el principio de seguridad desde el diseño en todas nuestras tecnologías e integraciones. Realizamos una gestión rigurosa del hardware y software que introducimos, apoyados por nuestro Centro de Operaciones de Seguridad y Redes (SOC), que monitoriza y protege constantemente la conectividad. Además, nuestra **resiliencia cibernética se refuerza mediante el enfoque proactivo** de un equipo interno especializado que adopta la perspectiva de un "hacker" para identificar, reportar y mitigar vulnerabilidades antes de que puedan ser explotadas.

Más allá de la infraestructura tecnológica, tenemos en cuenta la **importancia del factor humano en la ciberseguridad.** Por ello, impulsamos comportamientos seguros, contando con un estricto sistema de Gestión de Identidad y Accesos (IAM) que proporciona una identidad digital a cada persona, garantizando que solo las personas adecuadas tengan acceso a la información sensible. Paralelamente, consideramos que el personal de servicios es, a menudo, el que más se mueve por las instalaciones, y convertirlos en un "cortafuegos humano" es esencial para la seguridad global de cualquier edificio.

la resiliencia de una organización no solo se mide por cómo evita los ataques, sino por su capacidad de reacción cuando estos ocurren.

Asimismo, **la resiliencia de una organización no solo se mide por cómo evita los ataques, sino por su capacidad de reacción cuando estos ocurren.** Todos los equipos deben trabajar conjuntamente para establecer planes de contingencia que permitan mantener la operatividad frente a brechas de seguridad. Por ejemplo, pasando a operaciones manuales de forma rápida y segura, para garantizar que la actividad principal del cliente sufra las menores interrupciones posibles.

En definitiva, el ***Facility Management* moderno exige una visión holística donde la seguridad física y la digital son dos caras de la misma moneda.** Las organizaciones deben entender que cuidar integralmente de un edificio significa también blindarlo digitalmente. Para lograrlo, resulta necesario **contar con un entorno de trabajo digital seguro e integrar protocolos de ciberseguridad en las tareas más cotidianas,** asegurando que la innovación tecnológica siga siendo un motor de eficiencia y no una vulnerabilidad latente.

Las nuevas herramientas deben servir para reforzar el objetivo principal de las empresas que lideramos el sector del *Facility Management:* garantizar que nuestros clientes puedan enfocarse en su negocio y actividad, con la absoluta tranquilidad de que su entorno operativo no se detendrá.

Jordi Vizcaíno
Chief Information Officer (CIO) en ISS Facility Services España

Cuando un edificio inteligente deja de ser seguro

Por qué la ciberseguridad ya no es un asunto del equipo de Sistemas, sino un pilar del Facility Management

Durante años, el *Facility Management* consideró la ciberseguridad un asunto ajeno, limitado a Sistemas. Hoy, la convergencia entre Sistemas y toda la operación ha roto esa lógica: climatización, control de accesos, iluminación, ascensores o videovigilancia están conectados, monitorizados y gestionados digitalmente. Y eso cambia por completo las reglas del juego.

Si todavía existen dudas sobre la magnitud real de este riesgo, conviene recordar un caso que marcó un antes y un después. En 2020, un ataque de ransomware paralizó los sistemas del Hospital Universitario de Düsseldorf, obligó a cerrar urgencias y desviar pacientes a otros centros. Una mujer falleció durante el traslado al no poder ser atendida a tiempo.

Aquella noche, la ciberseguridad dejó de ser un concepto abstracto para convertirse en una cuestión de vida o muerte. La lección fue clara: en entornos críticos, un fallo digital puede tener consecuencias físicas irreversibles.

NIS2: el regulador entra en la ecuación

A este nuevo escenario se suma un marco normativo que ya no deja lugar a la ambigüedad. La Directiva europea NIS2 no es una recomendación ni una guía de buenas prácticas: es una obligación legal que eleva la ciberseguridad al máximo nivel de responsabilidad corporativa.

Por primera vez, la normativa establece una responsabilidad directa de la alta dirección ante los incidentes de seguridad y extiende estas obligaciones a toda la cadena de suministro: desde el fabricante de un sensor hasta la empresa que realiza el mantenimiento de una instalación. Externalizar el riesgo ya no es una opción.

La verdadera pregunta ya no es si esto afecta al Facility Management, sino: ¿estamos preparados para responder?

No es solo tecnología: es estrategia

Ante este contexto, la reacción habitual es pensar en nuevas herramientas. Sin embargo, la ciberseguridad en el *Facility Management* no se resuelve solo comprando tecnología, sino construyendo una estrategia sólida y transversal que se apoya en varios pilares fundamentales:

- **Gobernanza y cultura: romper los silos**
  Mantener la frontera tradicional entre TI y OT ya no solo es ineficiente, es peligroso. La ciberseguridad exige una gobernanza compartida, espacios de decisión comunes y un lenguaje alineado.

- **Confianza cero: verificar siempre**
  El paradigma debe cambiar radicalmente. La filosofía de "nunca confiar, siempre verificar" se convierte en la base de la nueva arquitectura. Estándares como ISA/IEC 62443 ofrecen marcos claros para proteger entornos OT, apoyados en medidas como la microsegmentación, que limita el movimiento lateral de un atacante, o el parcheo virtual, clave para proteger sistemas heredados que no pueden actualizarse.

- **La cadena de suministro como vector de riesgo**
  Somos tan fuertes como el eslabón más débil de nuestra cadena de suministro. Su riesgo es también el nuestro. La ciberseguridad debe incorporarse a contratos, auditorías y procesos de verificación.

- **Hablar el idioma de la dirección**
  La ciberseguridad no se defiende con acrónimos, sino con impacto en el negocio. Lograr el compromiso real de la alta dirección exige traducir el riesgo digital a términos económicos: interrupciones del servicio, impacto en ingresos, daño reputacional. Métricas como la Pérdida Anual Esperada (ALE) permiten demostrar que la ciberseguridad no es un coste, sino una inversión estratégica.

- **Impacto de la IA**
  La IA redefine el riesgo: es simultáneamente amenaza y aliado estratégico. Mientras potencia ciberataques, permite una defensa predictiva en IT y OT. Integrarla en la estrategia de seguridad es una obligación.

La ciberseguridad ya no es un complemento tecnológico: es un requisito crítico para la continuidad del negocio, la seguridad física de las personas y la resiliencia de las organizaciones.

Un edificio no es más seguro por tener más tecnología, sino porque las personas que lo gestionan saben reaccionar cuando algo no va como debería.

Gestionamos edificios cada vez más inteligentes, conectados y eficientes. Pero sin seguridad, esa inteligencia no solo deja de aportar valor: puede convertirse en un riesgo.

Una conclusión incómoda, pero necesaria

Gestionamos edificios cada vez más inteligentes, conectados y eficientes. Pero sin seguridad, esa inteligencia no solo deja de aportar valor: puede convertirse en un riesgo.

Invertir en ciberseguridad ya no va de cumplir normativas ni de proteger sistemas. Va de garantizar que los edificios y servicios que gestionamos sigan siendo fiables en un entorno cada vez más hostil.

Porque hoy, en *Facility Management*, **un edificio inteligente que no es seguro es, sencillamente, un riesgo.**

serveo

Óscar Sánchez
Head of IT Infrastructure & Cybersecurity

Innovar en FM exige cambiar el contrato

La tecnología existe, falta convertirla en resultados operativos medibles.

La tecnología para transformar el Facility Management ya existe: IA, robótica, analítica de ocupación, mantenimiento predictivo y plataformas IoT. Sin embargo, la Jornada de Innovación organizada por Optima evidenció que el verdadero cuello de botella no está en la solución técnica, sino en la capacidad de integrarla, financiarla, gobernarla y convertirla en resultados operativos medibles.

De la adopción a la integración

La pregunta que abrió la sesión fue directa: si la innovación existe, ¿por qué no acaba de cuajar en las corporates? La respuesta fue tomando forma desde el primer bloque. Miguel Mier -miembro de la junta de IFMA España- y Manuel Járrega -presidente de la ACFM- situaron tres factores que condicionan la transformación del sector: los proveedores de FM, la propia tecnología y, sobre todo, la integración real de esa tecnología en las organizaciones. No basta con adoptar herramientas. El reto es conectarlas con sistemas, procesos, cultura y contratos.

Los datos presentados refuerzan esta lectura. Según el estudio citado de Johnson Controls, el 86% de los responsables de negocio ya utiliza algún tipo de tecnología de workplace management, pero la principal dificultad sigue siendo la integración. En paralelo, el estudio de JLL comentado en la sesión señala que una parte relevante del coste tecnológico se pierde en fricciones, duplicidades, licencias infrautilizadas y baja adopción.

Del dato al resultado

Los pitchs de Brain Corp, Foot Analytics y Mindsett aterrizaron el debate en soluciones concretas. Anders Terkildsen -Vice President Business Development EMEA & APAC de Brain Corp- mostró cómo la robótica autónoma puede mejorar la calidad, la frecuencia de limpieza, la eficiencia laboral y la satisfacción del usuario. Miquel Gummà -CEO & Co-Founder de Foot Analytics- defendió que los edificios ya generan datos suficientes, pero que el valor aparece cuando esos datos se convierten en decisiones: cerrar plantas, ajustar HVAC, optimizar salas o anticipar saturaciones. Guim Crusellas -FM Cloud Director- (Mindsett), llevó esa lógica al mantenimiento predictivo: no se trata solo de saber que un activo ha fallado, sino de detectar cuándo va a fallar y actuar antes.

El hilo común fue claro: el FM ya no puede limitarse a reaccionar. Debe operar con datos fiables, accionables y vinculados al ciclo de vida del activo.

El contrato como barrera invisible

Ignasi Casamada planteó una tesis central: el principal límite de la innovación en FM probablemente ya no es tecnológico, sino contractual, económico y relacional. En España siguen predominando contratos basados en inputs, frecuencias y recursos, mientras que otros mercados más maduros llevan años trabajando con modelos orientados a outcomes, disponibilidad y ciclo de vida.

La tecnología ya está disponible. El reto del FM es crear las condiciones para que se convierta en transformación real.

La propuesta pasa por evolucionar hacia esquemas de colaboración más relacionales, con objetivos de negocio compartidos, ahorros garantizados, gainshare, fondos de reinversión en innovación y una gobernanza menos punitiva y más orientada a la evolución. El Optima Vested Strategic Model™ aparece aquí como una vía para convertir al proveedor en partner real, no en mero ejecutor.

Tres aprendizajes operativos

1. La adopción tecnológica no equivale a transformación: sin integración, los datos quedan aislados.
2. Los pilotos deben tener hipótesis, baseline, KPIs y decisión de escalado desde el inicio.
3. La innovación exige contratos que premien resultados, no solo horas, frecuencias o recursos.

Qué medir de verdad

El coloquio final añadió matices relevantes. Luis Morejón -Uber- subrayó que, para innovar, hacen falta contratos largos, pilotos constantes y una visión del proveedor como socio. También defendió la satisfacción del empleado como outcome principal. Vicente Herguido -BBVA- aportó una advertencia práctica: compartir ahorros es deseable, pero exige definir contra qué baseline se calculan y cómo se demuestra el valor ante Finanzas. Anabella Nahón -Air Liquide- señaló otro resultado clave: simplificar toda la operativa que no pertenece al core de negocio, como es la satisfacción del cliente interno.

La jornada concluyó con la idea clara de que la innovación en FM no depende solo de encontrar la mejor tecnología. Necesita crear las condiciones para que esa tecnología pueda probarse, integrarse, medirse y escalarse. Por ello es clave dar cabida a modelos de contratos que permitan ese espacio para la innovación, desde la transparencia y la voluntad de colaboración.

“La toma de una mala muestra puede llevar a una organización a una crisis de negocio y regulatoria”

La acreditación ISO 17025, tradicionalmente asociada al laboratorio, se extiende ahora a una fase hasta hace poco invisible: la toma de muestras. Eli Bosch, es CEO de The Sampling Solutions (TSS), primer laboratorio de toma de muestras acreditado por ISO 17025 por ENAC en España y que ayuda a garantizar que el dato sobre el que se toman decisiones críticas sea sólido desde el origen.

¿Qué implicaciones tienen los nuevos reales decretos para los Facility Managers?
El principal cambio es que el control del agua y de Legionella deja de ser un cumplimiento documental para convertirse en un sistema de gestión del riesgo con la entrada de en vigor del RD 487/2022 para la prevención y control de la legionelosis y del RD 3/2023. Las organizaciones ya no solo deben disponer de resultados analíticos; deben demostrar que las decisiones se apoyan en datos técnicamente fiables. Y eso empieza mucho antes del laboratorio: empieza en la muestra.

¿Por qué la toma de muestras ha adquirido tanta relevancia?
Es el origen del dato. Ningún análisis puede corregir una muestra mal tomada o poco representativa. Es una fotografía de la instalación. Si esa fotografía está distorsionada, también lo estarán las decisiones que se adopten a partir de ella. En otras palabras: una mala muestra puede conducir a una mala decisión.

Muchos proveedores ya toman muestras. ¿Qué cambia realmente?
La diferencia está en poder demostrar que la muestra es representativa, trazable y obtenida bajo procedimientos controlados, con los incrementos de frecuencias es probable que no den abasto. Con el nuevo contexto regulatorio, ya no es solo quién analiza, sino quién toma la muestra. Ahí es donde la acreditación ISO 17025 adquiere un papel determinante.

¿Qué riesgos asume un Facility Manager si este proceso no está bien controlado?
El primero es tomar decisiones basadas en información poco fiable. El segundo es generar una falsa sensación de seguridad. Pero probablemente el más importante es el riesgo reputacional y regulatorio. Ante una inspección o un incidente, la cuestión ya no es únicamente el resultado obtenido, sino cómo se obtuvo y qué garantías existen sobre su validez.

¿Puede afectar esto a la reputación profesional del Facility Manager?
Sin duda. El Facility Manager gestiona activos críticos donde cualquier incidente puede afectar a personas, operaciones y reputación corporativa. Su responsabilidad no termina al contratar un proveedor. También debe garantizar que los sistemas de control sean sólidos, auditables y defendibles. La capacidad de anticipar riesgos antes de que se materialicen forma parte de su valor profesional.

¿Existe también un riesgo para la continuidad del negocio?
Sí, y es muy directo. Un incidente relacionado con el agua puede provocar restricciones operativas, tratamientos de emergencia, cierres parciales y pérdida de confianza. En hoteles puede traducirse en cancelaciones. En hospitales, afectar la operativa asistencial. En residencias, generar una crisis reputacional especialmente sensible.

La continuidad de negocio depende cada vez más de la capacidad de prevenir y demostrar control.

¿Por qué es tan importante la trazabilidad en ISO 17025?
Porque permite reconstruir todo el recorrido de la muestra: quién la tomó, cuándo, dónde, cómo se conservó y cómo se transportó. Sin trazabilidad, el dato pierde capacidad de defensa técnica. Con ella, se convierte en evidencia objetiva capaz de respaldar decisiones, auditorías e inspecciones.

¿Qué preguntas debería hacer un Facility Manager a un proveedor de muestreo?

¿Cómo garantizan la competencia técnica del personal que realiza el muestreo? ¿Cómo aseguran la trazabilidad completa de cada muestra? ¿Qué mecanismos utilizan para garantizar que el proceso se realiza de forma homogénea y reproducible? Las respuestas suelen reflejar rápidamente el nivel de madurez técnica del proveedor.

¿Qué deberían revisar los Facility Managers en sus contratos con proveedores?
Deben entender claramente dónde empieza y termina la responsabilidad de cada actor. La organización sigue necesitando demostrar que el proceso de control fue adecuado. Por ello, es fundamental revisar quién realiza el muestreo, qué competencias tiene el personal, qué procedimientos se aplican y qué nivel de trazabilidad existe. Especialmente en organizaciones multisite, la homogeneidad del proceso es clave para garantizar resultados comparables y defendibles.

¿Qué consejo daría a los responsables de instalaciones?
Que dejen de ver la toma de muestras como una tarea administrativa. Es el punto de partida de cualquier decisión posterior. La calidad del dato condiciona la calidad de la gestión del riesgo. La pregunta que debería hacerse es sencilla: ¿podría defender técnicamente su sistema de control si mañana tuviera una inspección o un incidente?

Ciberseguridad, Inteligencia Artificial y continuidad operativa en edificios inteligentes bajo el enfoque del Esquema Nacional de Seguridad

La evolución hacia edificios inteligentes ha transformado la gestión de infraestructuras urbanas. Sistemas de climatización (HVAC), control de accesos, videovigilancia (CCTV) o gestión energética están cada vez más interconectados, aportando eficiencia y sostenibilidad.

Sin embargo, este modelo introduce un reto crítico: garantizar la ciberseguridad y la continuidad operativa, especialmente en un contexto donde la inteligencia artificial (**IA**) cobra protagonismo y donde normativas como el Esquema Nacional de Seguridad (**ENS**) y **NIS2** se vuelven determinantes.

Amenazas emergentes en entornos inteligentes

A las amenazas tradicionales (ransomware, accesos no autorizados, ataques DoS) se suman riesgos asociados a la IA cada vez más frecuentes y sofisticados con un incremento de 600% de uso de IA en ciberataques

En el año 2025 el 81% del malware analizado era capaz de causar una interrupción en los sistemas OT y se han incrementado un 146% en escenarios OT con impacto físico.

Continuidad operativa y Esquema Nacional de Seguridad: un marco obligatorio

El **ENS** establece los principios básicos y requisitos mínimos para proteger la información y los servicios en el sector público e infraestructuras críticas, no solo en cliente, sino también en proveedores que colaboran y prestan servicios con él.

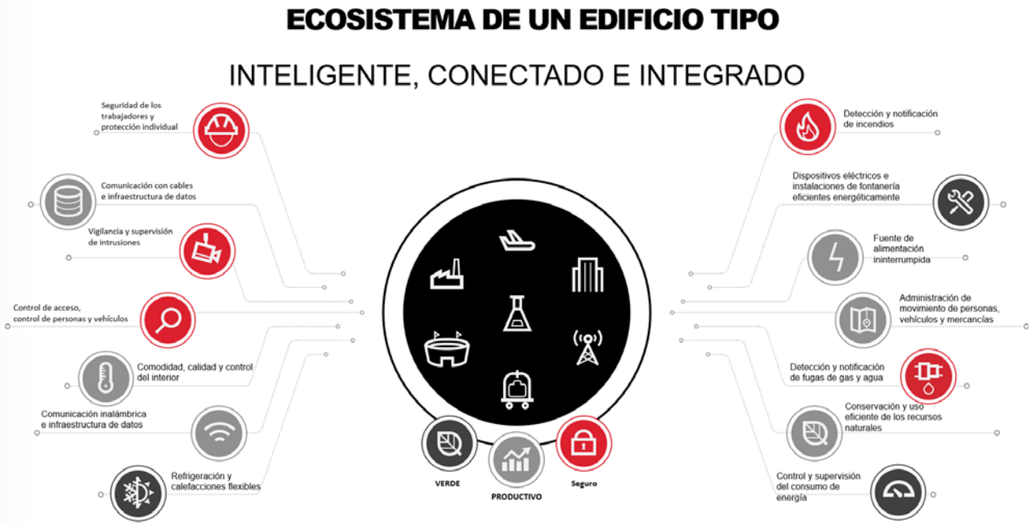
El **ENS** introduce un enfoque basado en la gestión del riesgo y la categorización de sistemas (básica, media, alta), lo que implica definir medidas de seguridad proporcionales al impacto que tendría un incidente en la continuidad del servicio. Nuestra categorización como Alta en el ENS, nos capacita no solo para prestar soluciones y sino poder ofrecer un servicio que cumpla estos requerimientos.

En la práctica, esto significa que la operación de un edificio inteligente debe considerar la ciberseguridad como un requisito de servicio esencial, no solo tecnológico, algo que pocas veces se tiene en cuenta.

Impacto del ENS

La aplicación del ENS se traduce en requisitos concretos que afectan al diseño y operación de los sistemas:

- **Segmentación de redes IT/OT.**
- **Control de accesos remotos securizados.**
- **Principio de Monitorización continua**, principal medida en el ENS enfocada a la detección y respuesta ante actividades o comportamientos anómalos. Evaluación permanente del estado de la seguridad de los activos, para detectar vulnerabilidades e identificar deficiencias de configuración
- **Gestión de incidentes**, incluyendo notificación y recuperación, tanto solución como servicio.
- **Auditorías periódicas de ciberseguridad.** Básico para poder tener trazabilidad de las mejoras implementadas y poder tener una cuantificación del riesgo de cada instalación



Además, el **ENS** exige garantizar principios como la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, todos ellos esenciales para la continuidad operativa.

Monitorización y respuesta alineadas con ENS

El ENS requiere capacidades de detección temprana y respuesta ante incidentes. En edificios inteligentes, esto implica evolucionar hacia modelos de operación donde se monitoricen tanto sistemas OT como modelos de IA.

Las organizaciones deben:

- Detectar anomalías en sistemas y algoritmos
- Definir planes de contingencia y operación en modo degradado
- Garantizar la recuperación rápida de servicios críticos

La continuidad operativa deja de depender únicamente de redundancias físicas y pasa a depender también de la resiliencia digital.

Dentro del ciclo de vida completo de ciberseguridad, incluyendo agentes de todos los fabricantes y sistemas operativos que puedan encontrarse en una instalación, **Honeywell** proporciona una visión holística, siendo el único proveedor que puede cubrir el ciclo completo de ciberseguridad con plataforma propia de monitorización de activos como **Cyber Insights** y poder ofrecer no solo la solución, sino el servicio asociado. Esto es vital, porque podemos tener las herramientas apropiadas, pero si el cliente no sabe explotarlas correctamente, por muy buena que sea la solución instalada, no valdrá para nada. Aquí es donde **Honeywell** se destaca frente a sus principales competidores y aporta un valor añadido fundamental para los clientes.

Conclusión, tenemos que ampliar el foco del alcance de ciberseguridad, Enfoque Integral

La adopción de un enfoque integral del **ENS** —que combine seguridad por diseño, gobernanza de la IA y cumplimiento normativo— permitirá a las organizaciones no solo reducir riesgos, sino también construir infraestructuras resilientes y confiables. En un entorno cada vez más automatizado, la continuidad operativa dependerá directamente de la capacidad para integrar seguridad, tecnología y regulación de forma coherente y aquí es donde Honeywell ofrece un valor diferencial.

Honeywell

Rubén Moreno
Sr Territory Manager Cybersecurity
Southern & Eastern Europe

Del primer contacto a la última intervención: la nueva era de la experiencia de cliente

La experiencia de cliente ha dejado de ser un elemento diferencial para convertirse en un elemento estratégico para las organizaciones. Sin embargo, muchas compañías continúan operando con modelos fragmentados: canales desconectados, equipos desalineados y procesos que obligan al cliente a repetir información constantemente. Una realidad especialmente visible en organizaciones donde la atención al cliente y el servicio de campo *(field service)* siguen funcionando como estructuras independientes.

Durante el webinar organizado por Minsait (Indra Group) en mayo de 2026, se abordó uno de los grandes retos actuales: cómo evolucionar hacia modelos integrales capaces de ofrecer una atención continua, inteligente y centrada en el cliente.

El coste de una experiencia fragmentada para el negocio

Cada retraso en la resolución de una incidencia o cada interacción repetitiva supone mucho más que una ineficiencia operativa, generan pérdida de confianza y deterioran la experiencia del cliente.

Esta desconexión impacta directamente en indicadores clave como la satisfacción, la fidelización y el cumplimiento de los acuerdos de nivel de servicio SLA (Acuerdo de Nivel de Servicio, por sus siglas en inglés).

Una visión integral de experiencia

La transformación pasa por conectar todo el ciclo de servicio en una experiencia continua. En este contexto, Indra Group impulsa modelos integrales donde la experiencia fluye desde el primer contacto hasta la resolución final.

La inteligencia artificial (IA) contribuye a automatizar tareas, permite conectar procesos, anticipa necesidades y aporta contexto en tiempo real para mejorar cada interacción. El objetivo es construir experiencias relevantes y satisfactorias en todos los puntos de contacto.

Tecnología conectada para generar valor

Para materializar esta visión, Indra Group trabaja con plataformas líderes como Microsoft Dynamics 365, Salesforce o Genesys, integradas dentro de arquitecturas orientadas a eliminar silos y orquestar toda la experiencia de cliente.

Cada retraso en la resolución de una incidencia o cada interacción repetitiva supone mucho más que una ineficiencia operativa, generan pérdida de confianza y deterioran la experiencia del cliente.

Las organizaciones que avanzan hacia modelos integrales consiguen mejorar la resolución en el primer contacto, reducir tiempos de gestión y minimizar las interacciones repetitivas que generan frustración.

Además, contempla la capacidad de conectar ecosistemas, integrar información y transformar los datos en acciones útiles para negocio y operaciones.

Resultados tangibles y medibles

Las organizaciones que avanzan hacia modelos integrales consiguen mejorar la resolución en el primer contacto, reducir tiempos de gestión y minimizar las interacciones repetitivas que generan frustración.

En el ámbito del *field service*, esto se traduce en técnicos mejor preparados, más resoluciones en la primera visita y una optimización global de recursos y desplazamientos.

El resultado es una mayor eficiencia operativa, una reducción de costes, un mejor cumplimiento de los SLA y un incremento de la satisfacción y fidelización de clientes. Estudios del sector apuntan a mejoras de hasta un 30 % en las resoluciones a la primera.

Sectores donde el cambio ya es una realidad

Esta evolución ya es una realidad en numerosos sectores. En *utilities*, permite anticipar incidencias masivas y establecer comunicaciones proactivas que reducen la presión sobre los centros de atención.

En servicios de mantenimiento, facilita la evolución desde modelos reactivos hacia estrategias predictivas basadas en datos. Y en instalaciones y servicios técnicos, aporta trazabilidad completa de cada intervención. Porque cuando un técnico dispone de información contextualizada, capacidad de actuación y visibilidad completa del caso, la experiencia cambia por completo.

Más allá de la tecnología

Adoptar un modelo integral implica también una transformación organizativa, lo que significa unificar canales, conectar equipos, integrar datos y establecer mecanismos de mejora continua basados en métricas reales de la experiencia de cliente, que no termina cuando se registra una incidencia, sino cuando el cliente percibe que su necesidad ha sido resuelta de forma satisfactoria.

En la nueva economía de la experiencia, las organizaciones líderes no son únicamente las más rápidas, también son aquellas capaces de acompañar mejor a sus clientes durante todo el proceso.

Desde Indra Group, el objetivo es ayudar a las organizaciones a evolucionar hacia experiencias conectadas, inteligentes y sin fricciones, donde cada interacción aporte valor y cada proceso contribuya a fortalecer la relación con el cliente.

MINSAIT

Nela Villalibre
Responsable de Desarrollo de Negocio de Costumer Xperience (Indra Group)

IFMA™ España Chapter
International Facility Management Association

FMM FACILITY MANAGEMENT MAGAZINE

Especial #FM_Ciberseguridad

#FM_Ciberseguridad

Entrevista

“Muchos FM consideran la ciberseguridad como un asunto solo de IT o de seguros, y esa percepción es peligrosa”

Dra. Erika A. Pärn (NYU Abu Dhabi), **Jeffrey Saunders** (Centro Tecnológico Nacional de Defensa de Dinamarca) y el **Prof. Borja García de Soto** (NYU Abu Dhabi)

“La colaboración entre Facility Management y ciberseguridad será estructural dentro de la gestión empresarial”

Javier Ordúñez miembro del Comité Técnico del Cyber Resilience Centre de ISMS Forum y subdirector de Resiliencia Operativa y Gestión de Crisis en Mapfre, y a **Mar Tie**, subdirectora de Seguridad de las Instalaciones en Mapfre.

Artículo

Ciberseguridad en edificios: cuando la gestión de instalaciones se convierte en una cuestión estratégica

CyberMadrid, Clúster de Ciberseguridad de Madrid.

Opinión

Cuando la continuidad operativa depende de la ciberseguridad

Josep Guasch. Presidente de ASCICAT – Asociación de Ciberseguridad de Cataluña.

FM y ciberseguridad en la continuidad operativa

Rosa Ortuño. CEO de OptimumTIC.

Entrevista

DRA. ERIKA A. PÄRN, JEFFREY SAUNDERS Y EL PROF. BORJA GARCÍA DE SOTO

«Muchos FM consideran la ciberseguridad como un asunto solo de IT o de seguros, y esa percepción es peligrosa»

La creciente digitalización de los edificios y las infraestructuras está transformando el Facility Management, al tiempo que introduce nuevos desafíos relacionados con la seguridad de los sistemas conectados. En este contexto, la ciberseguridad ha pasado de ser una preocupación limitada a los departamentos de TI a convertirse en una cuestión estratégica para los Facility Managers y los responsables de la continuidad operativa.

Para comprender mejor esta realidad, la International Facility Management Association (IFMA) publicó recientemente Brechas de ciberseguridad en la administración de las instalaciones [1], el estudio más completo hasta la fecha sobre los riesgos cibernéticos en el sector. Basado en 372 encuestas realizadas a profesionales de más de cien países y respaldado por una innovadora metodología de análisis comparativo, el informe identifica las principales combinaciones de factores que aumentan la vulnerabilidad de las organizaciones ante incidentes de ciberseguridad que afectan a los sistemas de gestión de edificios.

Para profundizar en los resultados de esta investigación y analizar sus implicaciones para el futuro del Facility Management, conversamos con los autores del estudio: la Dra. Erika A. Pärn (NYU Abu Dhabi), Jeffrey Saunders (Centro Tecnológico Nacional de Defensa de Dinamarca) y el profesor Borja García de Soto (NYU Abu Dhabi). **Este es un resumen de una entrevista completa en inglés que pueden leer en este enlace**.

1. Esta investigación fue financiada parcialmente por el Centro de Ciberseguridad de la Universidad de Nueva York en Abu Dabi (CCS-AD), financiado por Tamkeen a través de la subvención G1104 del Instituto de Investigación de NYU Abu Dabi, y por el Center for Sand Hazards and Opportunities for Resilience, Energy, and Sustainability (SHORES), financiado por Tamkeen a través de la subvención CG013 del Instituto de Investigación de NYU Abu Dabi.

Dra. Erika A. Pärn (NYU Abu Dhabi)

“ Aunque la ciberseguridad se ha convertido en una prioridad en los sectores de TI e infraestructuras críticas, su incidencia en el FM ha recibido mucha menos atención, a pesar de la rápida digitalización de edificios y lugares de trabajo”.

Jeffrey Saunders: Mi interés surge de años de investigación sobre el futuro del trabajo y los espacios laborales. A medida que los activos físicos se conectaban cada vez más mediante la digitalización, quedó claro que los Facility Managers tendrían que proteger tanto los activos digitales como los físicos. Cuando más tarde me incorporé a IFMA, surgió una pregunta natural: ¿cómo estaban afectando las brechas de ciberseguridad a la profesión de Facility Management? Erika y Borja eran los socios ideales para responderla.

¿Qué les motivó a realizar esta investigación sobre las brechas de ciberseguridad en Facility Management?
Erika A. Pärn & Borja García de Soto: Nos encontramos repetidamente con una importante brecha tanto en la investigación como en la práctica. Aunque la ciberseguridad se ha convertido en una prioridad en los sectores de TI e infraestructuras críticas, su incidencia en el FM ha recibido mucha menos atención, a pesar de la rápida digitalización de edificios y lugares de trabajo. Las instalaciones son ecosistemas digitales cada vez más complejos, pero no existía una comprensión integral de cómo se producen las brechas de seguridad en la práctica. Nuestro objetivo era proporcionar a los profesionales del FM información práctica basada en evidencias, en lugar de recomendaciones genéricas. La colaboración con IFMA y el alcance a más de 15.000 profesionales en todo el mundo nos permitió hacerlo con rigor.

¿Por qué la ciberseguridad se está convirtiendo en un tema tan crítico para los Facility Managers?
EP & BGdS: Los Facility Managers son ahora responsables de vastos ecosistemas digitales que incluyen sistemas de gestión de edificios, dispositivos IoT conectados, controles de acceso, redes de seguridad contra incendios, plataformas energéticas y gemelos digitales. Una brecha de ciberseguridad ya no es solo un problema de datos; puede interrumpir las operaciones, comprometer sistemas de seguridad vitales y exponer información sensible. Al mismo tiempo, normativas como el GDPR y la CCPA han incrementado las consecuencias legales y reputacionales de estos incidentes.

“Las organizaciones también necesitan una mayor coordinación entre los equipos de instalaciones, TI, seguridad física, compras, gestión de riesgos y dirección. Las amenazas ya no pueden gestionarse en compartimentos estancos. ”.

Jeffrey Saunders
(Centro Tecnológico Nacional de Defensa de Dinamarca)

JS: Los edificios se están convirtiendo en entornos inteligentes que recopilan datos de forma continua, automatizan decisiones e interactúan con los sistemas centrales del negocio. Si estos sistemas se ven comprometidos, el impacto puede extenderse mucho más allá de las redes de TI, afectando a la seguridad, la ocupación y la continuidad del negocio. La ciberseguridad forma ya parte del deber de diligencia del Facility Manager y exige una colaboración más estrecha con TI, gestión de riesgos, recursos humanos y alta dirección.

¿Cuáles son las capacidades internas más importantes que deberían desarrollar las organizaciones?
EP & BGdS: Nuestra investigación destacó tres prioridades. En primer lugar, el conocimiento sobre ciberseguridad debe integrarse en toda la plantilla. En segundo lugar, las organizaciones necesitan políticas formales que cubran la tecnología operativa y los sistemas de edificios, no solo la infraestructura informática tradicional. En tercer lugar, es esencial contar con planes de respuesta ante incidentes. La preparación en ciberseguridad no es una medida aislada, sino una capacidad organizativa multicapa.

JS: Las organizaciones también necesitan una mayor coordinación entre los equipos de instalaciones, TI, seguridad física, compras, gestión de riesgos y dirección. Las amenazas ya no pueden gestionarse en compartimentos estancos. El lugar de trabajo es simultáneamente un entorno físico y digital, y las organizaciones necesitan una postura de seguridad integrada que refleje esta realidad.

¿Qué hallazgos de la investigación les resultaron más preocupantes?
EP & BGdS: Las configuraciones más preocupantes fueron aquellas organizaciones sometidas a fuertes presiones externas —como cambios tecnológicos rápidos o exigencias del mercado— pero que carecían de preparación interna. Estas organizaciones tienden a reaccionar en lugar de anticiparse. También nos llamó la atención que algunas organizaciones altamente preparadas siguieran sufriendo incidentes. Esto sugiere que las organizaciones más maduras cuentan con mejores capacidades de detección y, por tanto, identifican incidentes que otras menos preparadas quizá ni siquiera perciben.

JS: Las organizaciones deben asumir que las brechas ocurrirán. La verdadera medida de la resiliencia no es evitar todos los ataques, sino minimizar los daños, mantener las operaciones críticas y recuperarse rápidamente.

¿Hasta qué punto los riesgos de ciberseguridad en Facility Management son organizativos más que tecnológicos?
EP & BGdS: En gran medida son organizativos. La tecnología importa, sin duda, pero los factores más estrechamente asociados a las brechas fueron la gobernanza, la conciencia de las amenazas, la preparación y la cultura organizativa. Las personas, los procesos y la gobernanza no son elementos secundarios de la ciberseguridad: son su núcleo.

JS: Muchas vulnerabilidades se encuentran en vacíos organizativos. Cuestiones como quién es propietario de un sistema de gestión de edificios, quién autoriza el acceso de proveedores o quién es responsable de las actualizaciones son, fundamentalmente, problemas de gobernanza. La ciberseguridad pertenece a toda la organización, no a un único departamento.

¿Qué papel desempeñan las lagunas de conocimiento y la falta de concienciación en ciberseguridad?
EP & BGdS: Las carencias de conocimiento fueron una de las barreras más importantes identificadas. Las organizaciones con bajos niveles de concienciación son menos capaces de reconocer amenazas o responder eficazmente. Los programas de formación y sensibilización deben considerarse inversiones en infraestructura básica, no iniciativas opcionales.

JS: La falta de concienciación también retrasa la detección. En Facility Management, los incidentes suelen manifestarse primero como anomalías operativas, como comportamientos inusuales en un sistema de gestión de edificios o en una plataforma de control de accesos. El personal no necesita convertirse en experto en ciberseguridad, pero sí debe saber reconocer señales de alerta y escalar las preocupaciones adecuadamente.

¿Cómo deberían responder las organizaciones a la turbulencia tecnológica y a las presiones del mercado?
EP & BGdS: Las presiones externas no pueden controlarse, pero sí la preparación interna. Toda nueva tecnología —ya sea una red IoT, un gemelo digital, una plataforma en la nube o un sistema de gestión de edificios— debería ir acompañada de una evaluación de impacto en ciberseguridad. La seguridad debe integrarse desde el inicio en los procesos de adquisición e implantación.

JS: La ciberseguridad debe tratarse como parte de la gestión del cambio. Las organizaciones no solo deben preguntarse qué valor aporta una tecnología, sino también qué nuevas dependencias y vulnerabilidades introduce.

¿Participan suficientemente los Facility Managers en la estrategia de ciberseguridad?
EP & BGdS: En nuestra experiencia, no. Muchos profesionales de FM siguen considerando la ciberseguridad como un asunto de TI o algo cubierto por los seguros. Esta percepción es cada vez más peligrosa porque los Facility Managers supervisan muchos de los sistemas operativos que son objetivo de los atacantes. Necesitan tener un lugar en la mesa donde se toman las decisiones de gobernanza de la ciberseguridad.

JS: Estoy completamente de acuerdo. El lugar de trabajo del futuro exige responsabilidad y visibilidad compartidas entre departamentos.

> “Tecnologías como la automatización impulsada por IA, las plataformas FM en la nube y los gemelos digitales ofrecen un enorme valor, pero también introducen nuevas vulnerabilidades”.

Prof. Borja García de Soto (NYU Abu Dhabi)

¿Qué activos o sistemas suelen subestimar más las organizaciones?
EP & BGdS: Los sistemas de gestión y automatización de edificios siguen siendo algunos de los activos más infravalorados. Muchas organizaciones cuentan con políticas más sólidas para los sistemas de TI tradicionales que para plataformas HVAC, control de accesos, seguridad contra incendios o gestión energética. Los gemelos digitales representan otra preocupación emergente, ya que crean réplicas virtuales detalladas de activos físicos que pueden convertirse en objetivos valiosos para los atacantes. Las relaciones con la cadena de suministro también constituyen puntos de exposición significativos que suelen recibir una atención insuficiente.

¿Qué primeros pasos prácticos recomendarían para mejorar la preparación en ciberseguridad?
EP & BGdS: En primer lugar, elaborar un inventario completo de los activos conectados, incluidos sistemas de edificios, dispositivos IoT, gemelos digitales y conexiones con terceros. En segundo lugar, asegurarse de que las políticas de ciberseguridad cubran explícitamente la tecnología operativa. En tercer lugar, invertir en programas de formación y sensibilización en toda la organización.

JS: Añadiría un cuarto paso: mejorar la coordinación. Los equipos de FM deben trabajar estrechamente con TI, compras, gestión de riesgos y seguridad para clarificar la propiedad de los sistemas, las responsabilidades y los procedimientos de respuesta. Muchas vulnerabilidades existen simplemente porque no está claro quién es responsable de qué.

¿Cómo ven la evolución de la relación entre edificios inteligentes, transformación digital y ciberseguridad?

EP & BGdS: La superficie de ataque seguirá ampliándose a medida que los edificios se conecten cada vez más con distritos inteligentes, microrredes e infraestructuras urbanas. Tecnologías como la automatización impulsada por IA, las plataformas FM en la nube y los gemelos digitales ofrecen un enorme valor, pero también introducen nuevas vulnerabilidades. La ciberseguridad debe evolucionar al mismo ritmo que la transformación digital.

JS: La ciberseguridad se convertirá cada vez más en un requisito de diseño y no en una reflexión posterior. Un edificio inteligente en el que no se puede confiar no es realmente inteligente. Las organizaciones más exitosas comprenderán que la ciberseguridad y la transformación digital son prioridades complementarias, no competidoras.

¿Qué mensaje les gustaría compartir con los miembros de IFMA España?
EP & BGdS: La ciberseguridad no es simplemente un asunto de TI; es una cuestión de liderazgo en Facility Management. Las organizaciones más resilientes no son necesariamente las que disponen de mayores presupuestos, sino aquellas en las que la concienciación forma parte de la cultura, las responsabilidades están claramente definidas y las personas comprenden lo que está en juego. Los caminos hacia la vulnerabilidad son cada vez mejor conocidos, lo que significa que los caminos hacia la resiliencia también están al alcance.

JS: No esperen a sufrir una brecha para convertir la ciberseguridad en una prioridad. Los Facility Managers se sitúan en la intersección entre edificios, personas, tecnología y continuidad del negocio, lo que les otorga un papel estratégico en la resiliencia organizativa. Las conversaciones adecuadas deben producirse ahora, antes de que un incidente obligue a ello.

Referencia de investigación publicada

Pärn, E. A., Sonkor, M. S., García de Soto, B. y Kookalani, S. (2026). *Pathways to Cyber Peril: Ten Configurational Routes to Cybersecurity Breaches in the FM Industry. Journal of Information Technology in Construction (ITcon)*, 31, 332–352. https://doi.org/10.36680/j.itcon.2026.014

Proxima Publicación

Securing Twin Systems — Pärn & García de Soto. Available on Amazon Kindle and in print, expected late July 2026.

Sobre los autores

Dra. Erika A. Pärn
Investigadora científica en la División de Ingeniería de la Universidad de Nueva York Abu Dhabi (NYUAD), dentro del grupo de investigación S.M.A.R.T. Construction, y colaboradora de investigación en la Universidad de Cambridge. Su trabajo se centra en sistemas de gemelos digitales, riesgos de ciberseguridad en el entorno construido, gestión digital de activos y la intersección entre BIM y resiliencia cibernética. Esta investigación fue apoyada por el Centro de Ciberseguridad de NYUAD (CCS-AD) y el centro SHORES, financiado por Tamkeen.

Jeffrey Saunders
Director de Tecnología del Centro Tecnológico Nacional de Defensa de Dinamarca. Aporta una amplia experiencia práctica en gestión del riesgo cibernético en infraestructuras críticas y sectores de instalaciones. Anteriormente fue Director de Investigación de IFMA, donde contribuyó al desarrollo de estudios y liderazgo intelectual sobre el futuro del Facility Management, la transformación digital, los cambios en el lugar de trabajo y el riesgo digital en edificios digitalizados.

Prof. Borja García de Soto
Profesor asociado de Ingeniería Civil y Urbana en la Universidad de Nueva York Abu Dhabi y profesor asociado de la Red Global de NYU Tandon. Dirige el grupo de investigación S.M.A.R.T. Construction en NYUAD, donde sus investigaciones se centran en automatización y robótica para la construcción, gemelos digitales para el entorno construido, ciberseguridad en arquitectura, ingeniería y construcción (AEC), IA y grandes modelos de lenguaje aplicados a la construcción, Lean Construction y BIM.

Entrevista

JAVIER ORDÚÑEZ Y MAR TIE

MIEMBRO DEL COMITÉ TÉCNICO DEL CYBER RESILIENCE CENTRE DE ISMS FORUM Y SUBDIRECTOR DE RESILIENCIA OPERATIVA Y GESTIÓN DE CRISIS EN MAPFRE Y SUBDIRECTORA DE SEGURIDAD DE LAS INSTALACIONES EN MAPFRE

“La colaboración entre Facility Management y ciberseguridad será estructural dentro de la gestión empresarial”

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector.

Javier Ordúñez forma parte del Comité Técnico de Ciberresiliencia de ISMS Forum, donde trabajan en la generación de conocimiento práctico y en la difusión de buenas prácticas orientadas a fortalecer la capacidad de las organizaciones para anticipar, resistir y recuperarse ante incidentes, especialmente aquellos con impacto en la continuidad operativa. Su trayectoria profesional en los últimos años ha estado estrechamente vinculada a la resiliencia operativa y a la gestión de crisis, asumiendo diferentes responsabilidades en esta materia dentro de su organización.

Mar Tie, por su parte, cuenta con una amplia experiencia en seguridad física y responsabilidad directa sobre la seguridad de las instalaciones y aporta una visión complementaria centrada en la protección de infraestructuras, activos críticos y entornos operativos.

Desde su experiencia, ¿por qué la ciberseguridad ha pasado de ser una cuestión estrictamente tecnológica para convertirse en una prioridad de negocio y continuidad operativa?
Porque probablemente estemos ante una de las pocas amenazas capaces de comprometer gravemente la continuidad de una organización en muy poco tiempo. A diferencia de otros riesgos, un incidente de ciberseguridad puede materializarse de forma simultánea en múltiples frentes: tecnológico, operativo, reputacional e incluso legal.

Hoy en día, un ataque puede dejar inoperativos sistemas críticos, bloquear el acceso a instalaciones, interrumpir la cadena de suministro o impedir la prestación de servicios esenciales. Esto convierte a la ciberseguridad en un riesgo existencial en determinados escenarios.

Por ello, ha dejado de ser una cuestión técnica para convertirse en una prioridad de negocio:

El Facility Management está directamente implicado en la gestión de activos y servicios que son críticos para la continuidad de la operación.

no se trata solo de proteger sistemas, sino de garantizar que la organización pueda seguir funcionando.

¿Qué riesgos están viendo hoy con más frecuencia en organizaciones que dependen de infraestructuras, edificios conectados o entornos de trabajo digitalizados?
Destacamos la creciente convergencia entre entornos IT y OT, que amplía la superficie de ataque de forma significativa. Entre los riesgos más relevantes observamos: Accesos indebidos a sistemas de gestión de edificios (BMS) y a los edificios en sí. Dispositivos IoT desplegados sin controles adecuados. Ataques ransomware con impacto transversal. Accesos remotos de proveedores sin supervisión suficiente. Falta de segmentación entre redes corporativas y operacionales

A ello se suma un escenario especialmente crítico como es el riesgo de blackout, ya sea provocado por causas físicas o como consecuencia de un ciberincidente. La interrupción del suministro eléctrico o de sistemas energéticos puede paralizar completamente la operativa de edificios e infraestructuras, generando un efecto cascada sobre toda la organización.

Muchas empresas siguen asociando la ciberseguridad únicamente a sistemas informáticos o protección de datos. ¿Qué aspectos suelen quedar fuera de esa visión?
Quedan fuera, en gran medida, todos los sistemas que gestionan el entorno físico: climatización, energía, control de accesos o videovigilancia. Estos activos forman parte del ecosistema digital, pero no siempre se gestionan bajo criterios de ciberseguridad.

También se tiende a infravalorar la dependencia de terceros, la falta de visibilidad sobre activos

conectados o la ausencia de integración entre seguridad física y lógica. Desde la alta dirección, es clave entender que el riesgo es transversal y afecta al conjunto de la operación, no solo a los sistemas de información.

En el ámbito de los edificios y espacios de trabajo, ¿qué papel juegan sistemas como el control de accesos, videovigilancia, BMS o IoT dentro del mapa de riesgos?
Son elementos críticos dentro del perímetro real de la organización. Estos sistemas pueden convertirse en vectores de entrada si no están adecuadamente protegidos, pero además tienen la capacidad de generar impacto directo sobre la operativa.

Por ejemplo, la manipulación de un sistema BMS puede afectar al funcionamiento del edificio; un control de accesos comprometido puede alterar la seguridad física; y dispositivos IoT vulnerables pueden facilitar accesos no autorizados a la red corporativa.

En definitiva, son activos que tradicionalmente se han gestionado desde el ámbito operativo, pero que hoy forman parte inseparable del riesgo cibernético.

¿Hasta qué punto un incidente de ciberseguridad puede comprometer la operativa física de una organización?
En muchos casos, de forma total. La interdependencia entre sistemas digitales y físicos hace que un incidente de ciberseguridad pueda traducirse directamente en una crisis operativa.

Por ejemplo, un ataque que afecte a los sistemas de control de accesos puede impedir la entrada de empleados o proveedores a una instalación crítica; o al contrario, dejar la instalación completamente accesible a cualquier. Del mismo modo, la indisponibilidad de un sistema de gestión de edificios puede comprometer la climatización, el suministro energético o incluso la seguridad del inmueble.

En sectores como el industrial, sanitario o de infraestructuras críticas, este tipo de impacto puede paralizar completamente la actividad o afectar a la prestación de servicios esenciales. Un ejemplo claro sería el de un Centro de Proceso de Datos (CPD): la interrupción o manipulación de los sistemas de climatización podría provocar un sobrecalentamiento de los equipos y comprometer su funcionamiento, afectando de forma directa a los servicios que soporta.

¿Está ganando el Facility Management peso como actor clave en la continuidad operativa?
Sí, y de forma muy tangible. El Facility Management está directamente implicado en la gestión de activos y servicios que son críticos para la continuidad de la operación: energía, accesos, seguridad física, mantenimiento o infraestructuras técnicas.

Esto se traduce en responsabilidades concretas dentro de la gestión del riesgo, como: Mantener actualizado el inventario de activos físicos y conectados y someterlos a pruebas de vulnerabilidad. Asegurar la correcta operación de sistemas críticos, especialmente todo lo relativo al entorno de comunicaciones. Coordinar la gestión de proveedores que actúan sobre estos activos. Participar en planes de continuidad y ejercicios de simulación de crisis. Detectar incidencias operativas con posible origen o impacto cibernético.

En este sentido, el FM deja de ser únicamente un área de soporte para convertirse en un actor clave en la prevención y respuesta ante incidentes.

Los riesgos ya no están segmentados por funciones. La falta de coordinación entre áreas genera zonas grises que pueden convertirse en vulnerabilidades.

¿Por qué es importante que los profesionales de FM trabajen coordinados con IT, seguridad, riesgos o compliance?
Porque los riesgos ya no están segmentados por funciones. La falta de coordinación entre áreas genera zonas grises que pueden convertirse en vulnerabilidades.

La colaboración permite tener una visión integral del riesgo, mejorar la detección y respuesta ante incidentes, alinear políticas y asegurar una gestión coherente de activos y accesos. En entornos complejos y altamente conectados, la resiliencia solo se consigue mediante una aproximación transversal.

¿Qué papel desempeñan los proveedores y terceros en este contexto?
La cadena de suministro es uno de los principales puntos críticos para las organizaciones. De hecho, de poco sirve contar con sistemas propios robustos y resilientes si los terceros que gestionan o acceden a las infraestructuras no lo son.

En el ámbito del Facility Management, esta dependencia es especialmente relevante, ya que muchos servicios esenciales están externalizados y los proveedores suelen tener acceso directo —físico o remoto— a sistemas críticos.

Por ello, la gestión del riesgo de terceros se convierte en un elemento clave, incluyendo evaluaciones de seguridad, requisitos contractuales claros, control y monitorización de accesos e integración en los planes de continuidad y respuesta. En definitiva, la resiliencia debe extenderse a toda la cadena de suministro.

¿Qué señales deberían observar los responsables de FM para detectar una exposición creciente al riesgo?
Algunos indicadores relevantes incluyen el incremento de activos conectados sin inventario actualizado. Accesos remotos sin controles robustos. Sistemas obsoletos o sin mantenimiento. Falta de segmentación de redes. Dependencia elevada de proveedores sin supervisión. Ausencia de planes de continuidad o pruebas de crisis y de vulnerabilidad. Estas señales suelen anticipar un aumento de la exposición al riesgo si no se abordan de forma proactiva.

Organismos como el World Economic Forum señalan que ciberataques e interrupciones de infraestructuras críticas como riesgos globales.

¿Cómo imaginan la evolución de la relación entre Facility Management y ciberseguridad en los próximos años?
Estamos ante un cambio estructural. La digitalización de los edificios y la creciente interconexión de sistemas hacen que la ciberseguridad sea un componente inherente a la gestión de infraestructuras.

Además, organismos como el World Economic Forum vienen señalando de forma recurrente los ciberataques y las interrupciones de infraestructuras críticas como algunos de los principales riesgos globales. Este contexto refuerza la necesidad de abordar de forma integrada los entornos físicos y digitales.

En los próximos años veremos una mayor integración entre Facility Management, IT y seguridad, la aparición de perfiles más híbridos y un enfoque cada vez más centrado en la resiliencia operativa. La colaboración entre Facility Management y ciberseguridad no será puntual, sino estructural dentro de la gestión empresarial.

Javier Ordúñez
Miembro del Comité Técnico del Cyber Resilience Centre de ISMS Forum y subdirector de Resiliencia Operativa y Gestión de Crisis en Mapfre

Mar Tie
Subdirectora de Seguridad de las Instalaciones en Mapfre

Artículo

CYBERMADRID. CLÚSTER DE CIBERSEGURIDAD DE MADRID

Ciberseguridad en edificios: cuando la gestión de instalaciones se convierte en una cuestión estratégica

La digitalización de los edificios ha dejado de ser una promesa para convertirse en una realidad operativa. Climatización, iluminación, control de accesos, videovigilancia, ascensores, sensores IoT o sistemas de gestión energética forman ya parte de un ecosistema conectado que mejora la eficiencia y la sostenibilidad, pero también amplía la superficie de exposición a amenazas digitales.

La ciberseguridad ya no es solo una cuestión del departamento de IT. Afecta directamente a la continuidad de negocio, a la operativa diaria de las instalaciones y, en determinados entornos, incluso a la seguridad de las personas. Así lo señalan los expertos consultados por CyberMadrid, Clúster de Ciberseguridad de Madrid, que coinciden en una idea central: el edificio inteligente debe empezar a entenderse como una infraestructura digital crítica.

"El edificio se ha convertido en un sistema informático más, pero casi nadie lo gestiona como tal", advierten desde Minery Report. La conexión de sistemas de climatización, accesos, videovigilancia o iluminación con redes corporativas y servicios en la nube ha difuminado las fronteras entre operación, tecnología y seguridad. Actitud-TI lo resume de forma clara: "un edificio inteligente es un objetivo digital crítico".

El problema, sin embargo, no siempre está en ataques sofisticados. Muchas vulnerabilidades nacen de fallos cotidianos: paneles de gestión accesibles desde Internet, dispositivos sin actualizar, credenciales débiles, redes sin segmentar o accesos remotos de proveedores externos abiertos durante años. SECUR0 apunta precisamente a estos elementos como vectores habituales de entrada, mientras VSISTEMAS subraya la falta de separación entre redes corporativas, redes de invitados y sistemas IoT como uno de los errores más frecuentes.

En este contexto, el riesgo deja de limitarse al robo de información. Un atacante no necesita comprometer el núcleo corporativo para generar impacto: basta con dejar fuera de servicio el control de accesos, la climatización de un centro de datos o los sistemas de videovigilancia para afectar gravemente a la actividad de una organización.

Por eso, la resiliencia se ha convertido en el nuevo indicador de madurez. Para Claudia Veas, gerente general para Europa de Inside Security, la ciberseguridad debe integrarse en la estrategia de negocio porque permite reducir impactos operacionales, financieros y reputacionales. Secure&IT coincide en que debe incorporarse desde el diseño de cualquier proyecto, no como una capa añadida al final. Desde Minery Report lo expresan así: "La pregunta no es si te van a atacar, sino cuánto tiempo puedes seguir funcionando cuando ocurra".

Esa capacidad de respuesta depende menos de tener más tecnología y más de contar con inventarios actualizados, redes segmentadas, copias de seguridad, planes de continuidad, protocolos de respuesta y simulacros reales. Un plan que nunca se ha probado, recuerdan los expertos, difícilmente servirá cuando llegue el incidente.

La irrupción de la inteligencia artificial, el crecimiento del IoT y la convergencia con sistemas OT añaden una nueva dimensión al problema. La IA mejora la capacidad defensiva, pero también facilita fraudes más creíbles, phishing sin errores evidentes y suplantaciones de voz o imagen. "La inteligencia artificial lo está cambiando todo y muy rápido", señalan desde Secure&IT. Minery Report añade que "cada sensor barato es un punto de entrada potencial que rara vez recibe actualizaciones".

Vodafone Empresas aporta una visión complementaria: estas tecnologías permiten gestionar edificios con mucha más precisión, anticipar incidencias y optimizar recursos. Como ejemplo, destaca su proyecto desarrollado junto a la Diputación de Valladolid, con 792 sensores instalados en 44 edificios públicos de 42 municipios. La clave, según la compañía, está en acompañar esta conectividad con seguridad desde el diseño, segmentación entre entornos IT y OT, control de accesos y monitorización continua.

El reto no es únicamente técnico. También es organizativo. Durante años, Facility Management ha gestionado instalaciones, IT ha gestionado redes y la seguridad del espacio intermedio ha quedado en una zona gris. "La seguridad de lo que hay en medio no es de nadie", resumen desde Minery Report. Esa frontera es precisamente la que empieza a exigir nuevos modelos de gobernanza.

Marina Cuervo, de Q-Mission, habla de un cambio estructural: la convergencia entre seguridad física, ciberseguridad, gestión de instalaciones y riesgo digital requiere liderazgo multidisciplinar, colaboración público-privada y profesionales preparados para operar en esa intersección.

La ciberseguridad ya no es solo una cuestión del departamento de IT. Afecta directamente a la continuidad de negocio, a la operativa diaria de las instalaciones e incluso a la seguridad de las personas.

VSISTEMAS coincide en que la coordinación entre gestores de infraestructuras, proveedores tecnológicos, responsables de seguridad y equipos cyber será decisiva en los próximos años.

A ello se suma la presión regulatoria. Marcos como NIS2 están obligando a muchas organizaciones a tratar la ciberseguridad como un asunto de dirección y no como una cuestión meramente informática. Pero el gran desafío sigue siendo el talento. Q-Mission alerta de que "seguimos formando profesionales de ciberseguridad para un mundo que ya no existe" y defiende modelos basados en formación continua, escenarios reales y evaluación por competencias operativas.

El concepto de edificio seguro, por tanto, está cambiando. Ya no basta con hablar de incendios, evacuación, accesos o protección física. La seguridad incluye también sistemas, datos, comunicaciones, proveedores, sensores, redes y capacidad de recuperación.

La oportunidad para el Facility Management es enorme: integrar la ciberseguridad como parte natural de la gestión de instalaciones. Porque el futuro de los edificios inteligentes no dependerá solo de cuántos dispositivos conectados incorporen, sino de si son capaces de operar de forma segura, resiliente y coordinada.

Como resume Marina Cuervo, Co-Chairman/Global CRO de Q-Mission, "el futuro de la ciberseguridad en infraestructuras y edificios no lo decidirán las herramientas. Lo decidirán las personas que sepan usarlas".

CyberMadrid
Clúster de Ciberseguridad de Madrid

Opinión

JOSEP GUASCH

PRESIDENTE DE ASCICAT - ASSOCIACIÓ DE CIBERSEGURETAT DE CATALUNYA

Cuando la continuidad operativa depende de la ciberseguridad

Durante años, cuando hablábamos de continuidad operativa, pensábamos en incidencias técnicas, interrupciones de servicios, averías o situaciones de emergencia que podían afectar al funcionamiento normal de una organización. Hoy, sin embargo, hay un factor que ha pasado a ocupar una posición central en cualquier estrategia de continuidad: la ciberseguridad.

La digitalización ha transformado la manera en que trabajan las empresas, las administraciones públicas, los hospitales, las infraestructuras críticas y los edificios corporativos. Esta transformación nos ha aportado eficiencia, conectividad y capacidad de gestión, pero también ha incrementado considerablemente nuestra exposición a los riesgos digitales.

Cuando se produce un ciberincidente, las consecuencias van mucho más allá de la pérdida de datos. Un ataque puede paralizar servicios, interrumpir procesos críticos, afectar a la relación con clientes y ciudadanos o comprometer la prestación de servicios esenciales. Por eso, hoy hablar de continuidad operativa implica necesariamente hablar de ciberseguridad.

Desde ASCICAT observamos una realidad que se repite con frecuencia: muchas organizaciones siguen asociando la ciberseguridad exclusivamente a la tecnología, cuando en realidad sus principales retos suelen estar relacionados con las personas, los procesos y la gobernanza.

Las personas siguen siendo la primera línea de defensa

A pesar de los avances tecnológicos, una parte muy importante de los incidentes de seguridad sigue teniendo su origen en el factor humano.

Los ataques de phishing, las suplantaciones de identidad, los fraudes por correo electrónico o la obtención fraudulenta de credenciales continúan siendo algunas de las técnicas más utilizadas por los ciberdelincuentes. Y funcionan porque aprovechan un elemento difícil de proteger: la confianza de las personas.

Las organizaciones dependen cada vez más de proveedores externos, plataformas digitales, servicios gestionados y aplicaciones de terceros. Esta realidad genera nuevas oportunidades, pero también nuevos riesgos.

Los ataques de phishing, las suplantaciones de identidad, los fraudes por correo electrónico o la obtención fraudulenta de credenciales continúan siendo algunas de las técnicas más utilizadas por los ciberdelincuentes. Y funcionan porque aprovechan un elemento difícil de proteger: la confianza de las personas.

Podemos invertir en las mejores herramientas de seguridad, pero si una persona no sabe identificar un correo fraudulento o una petición sospechosa, podemos estar abriendo la puerta a los atacantes.

Por este motivo, la concienciación y la formación deben ser una prioridad estratégica. No se trata de realizar una acción puntual, sino de construir una cultura de seguridad que permita a los profesionales identificar riesgos y actuar correctamente ante situaciones cada vez más sofisticadas.

Una organización preparada es aquella en la que las personas saben reconocer una amenaza antes de que esta se convierta en un incidente.

La seguridad de los proveedores también es nuestra seguridad

Otro de los grandes retos actuales es la cadena de suministro.

Las organizaciones dependen cada vez más de proveedores externos, plataformas digitales, servicios gestionados y aplicaciones de terceros. Esta realidad genera nuevas oportunidades, pero también nuevos riesgos.

Todavía hoy encontramos entornos sensibles que utilizan aplicaciones o sistemas que no cumplen los niveles de seguridad que serían exigibles. Algunos de estos entornos dan soporte a actividades especialmente críticas, como hospitales, infraestructuras esenciales o servicios que afectan directamente a la ciudadanía.

Esto obliga a las organizaciones a ir más allá de la seguridad interna y a exigir garantías también a sus proveedores.

La ciberseguridad debe formar parte de los criterios de contratación, supervisión y evaluación de cualquier servicio tecnológico. No podemos considerar seguro un entorno si una parte relevante de sus sistemas depende de terceros que no cumplen las medidas de protección adecuadas.

El cumplimiento normativo como herramienta de mejora

Con frecuencia, normativas como el Esquema Nacional de Seguridad (ENS) o la Directiva NIS2 se perciben como una obligación reguladora más.

La realidad es que estos marcos aportan una metodología sólida para gestionar los riesgos y mejorar la resiliencia de las organizaciones. Más allá del cumplimiento legal, ayudan a definir procesos, establecer responsabilidades, identificar vulnerabilidades y crear mecanismos de respuesta ante incidentes.

Desde ASCICAT consideramos que el cumplimiento normativo debe verse como una oportunidad para profesionalizar la gestión de la seguridad y elevar los estándares de protección de nuestras organizaciones.

Un ejemplo real de resiliencia

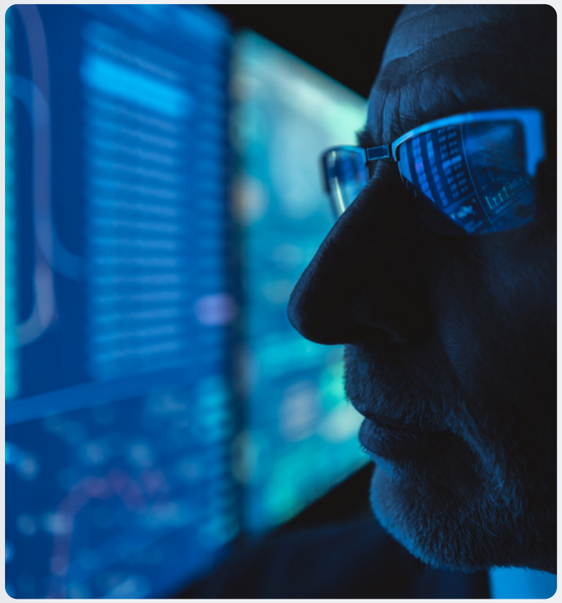
Hace unos años vivimos un caso que ilustra perfectamente la importancia de prepararse antes de que se produzca un incidente.

Una administración local catalana sufrió un ataque de ransomware durante el periodo navideño. Los atacantes consiguieron comprometer los sistemas e intentaron eliminar también las copias de seguridad disponibles para impedir cualquier recuperación y forzar el pago del rescate.

A primera vista, la situación parecía crítica. Los datos habían sido cifrados, las copias de seguridad aparentemente eliminadas y la organización se encontraba ante la posibilidad de tener que detener parte de sus servicios.

Sin embargo, la estrategia de protección implementada incorporaba mecanismos adicionales que preservaban las copias de seguridad incluso cuando estas eran borradas por los atacantes. Esta capa de protección permitió recuperar íntegramente la información y restablecer la operativa sin tener que negociar ni pagar ningún rescate.

La principal enseñanza de este caso es que la diferencia entre una crisis y una incidencia gestionable suele estar en la preparación previa. Las organizaciones que planifican su recuperación antes de sufrir un ataque son las que tienen mayor capacidad para seguir operando cuando este llega.



Prepararse para resistir

La pregunta ya no es si una organización sufrirá un intento de ataque. La pregunta es cuándo ocurrirá y hasta qué punto estará preparada para responder.

La ciberseguridad no consiste en eliminar completamente los riesgos, porque eso es imposible. Consiste en reducirlos, gestionarlos y garantizar que, cuando se produzca un incidente, la organización sea capaz de continuar operando y recuperarse con la máxima rapidez posible.

Esa es, en definitiva, la verdadera esencia de la continuidad operativa.

En un mundo cada vez más conectado, la ciberseguridad ya no es solo una cuestión tecnológica. Es una responsabilidad compartida que afecta a personas, procesos, proveedores y organizaciones. Y es también una de las garantías más importantes para asegurar que los servicios de los que dependemos cada día sigan funcionando cuando más los necesitamos.

La ciberseguridad no consiste en eliminar completamente los riesgos, porque eso es imposible. Consiste en reducirlos, gestionarlos y garantizar que, cuando se produzca un incidente, la organización sea capaz de continuar operando y recuperarse con la máxima rapidez posible.

Josep Guasch
Presidente de ASCICAT - Associació de Ciberseguretat de Catalunya

Opinión

ROSA ORTUÑO

CEO DE OPTIMUMTIC

FM y ciberseguridad en la continuidad operativa

La gestión de instalaciones (Facility Management) ha evolucionado hacia un modelo altamente digitalizado, en el que edificios inteligentes, sistemas conectados e infraestructuras tecnológicas forman parte esencial de la operativa diaria. Esta transformación ha aportado eficiencia y optimización, pero también ha introducido un nuevo vector de riesgo: la dependencia de sistemas expuestos a ciberamenazas.

En este contexto, la ciberseguridad ya no es un soporte técnico, sino un elemento estratégico para garantizar la continuidad operativa de los entornos construidos. Un incidente no solo implica una afectación sobre datos, sino que puede interrumpir servicios esenciales como accesos, climatización, energía u operaciones críticas. Por tanto, la cuestión clave ya no es si una organización sufrirá un incidente, sino si está preparada para anticiparlo y gestionarlo.

Tradicionalmente, muchas organizaciones han abordado la ciberseguridad desde un modelo reactivo, actuando cuando el problema ya había aparecido. Este enfoque resulta claramente insuficiente en un entorno donde las amenazas evolucionan constantemente. Los datos demuestran que la mayoría de las brechas no se originan en ataques sofisticados, sino en vulnerabilidades conocidas que no han sido corregidas a tiempo.

En este sentido, la actualización continua se convierte en un elemento esencial. Las vulnerabilidades conocidas, identificadas como CVE, constituyen la base de gran parte de los ataques. Cuando no se gestionan adecuadamente, los sistemas se convierten en puntos de entrada previsibles. Desde nuestra experiencia, muchas organizaciones disponen de tecnología avanzada, pero carecen de control real sobre su mantenimiento y evolución.

Por ello, desde OptimumTIC impulsamos un modelo basado en la anticipación, la predicción y la mejora continua. La ciberseguridad no puede ser estática, sino un proceso dinámico que evoluciona con el negocio, la normativa, la tecnología y las amenazas. Este enfoque implica identificación, monitorización, gestión activa de vulnerabilidades y una visión global del riesgo.

La preparación interna, la concienciación y la transversalidad son factores clave. No se trata únicamente de implantar medidas técnicas, sino de construir un modelo de gobernanza sólido, alineado con estándares internacionales y marcos como NIST, NIS2, DORA o ISO. La seguridad debe integrarse desde el diseño y formar parte de la cultura operativa.

Sin embargo, la tecnología por sí sola no es suficiente. El factor humano sigue siendo una de las principales vías de entrada de ataques,

la mayoría de las brechas no se originan en ataques sofisticados, sino en vulnerabilidades conocidas que no han sido corregidas a tiempo.

especialmente a través de técnicas como la ingeniería social, el phishing o la gestión inadecuada de credenciales. Por ello, la cultura organizativa y la formación se convierten en elementos clave, junto con medidas adaptadas a cada organización.

La formación en ciberseguridad debe ser continua, práctica y adaptada a cada perfil, teniendo en cuenta el comportamiento y la actuación de los usuarios, incorporando incluso metodologías como la gamificación. Cuando los equipos entienden los riesgos y saben cómo actuar, se reduce la probabilidad de incidentes y se mejora la capacidad de respuesta. La ciberseguridad no es solo una cuestión técnica, sino una responsabilidad compartida.

Otro aspecto fundamental es la gestión estratégica de los activos críticos. En muchos casos, las organizaciones no disponen de una visión clara de los sistemas que son esenciales para su actividad. En entornos de Facility Management, activos como los sistemas de control de edificios, las redes o los accesos pueden tener un impacto directo en la continuidad del negocio.

Identificar, clasificar y proteger estos activos es imprescindible para priorizar recursos. Sin esta clasificación, la seguridad se gestiona de forma dispersa. Desde nuestra experiencia, las organizaciones que adoptan este enfoque basado en la identificación y análisis de riesgos logran mayor resiliencia y control.

Además, la seguridad no se limita al entorno interno. El ecosistema de proveedores y terceros puede representar un riesgo si no se gestiona correctamente. La gobernanza del riesgo debe incluir toda la cadena de valor, asegurando responsabilidades claras y mecanismos de control.

En este escenario, los centros de operaciones de seguridad (SOC) desempeñan un papel fundamental. Ya no se trata únicamente de detectar incidentes, sino de anticiparlos. La monitorización continua y el análisis de vulnerabilidades de todos los activos permiten identificar riesgos antes de que se conviertan en problemas operativos.

Los nuevos marcos normativos refuerzan esta visión. Ya no es suficiente cumplir, sino demostrar control, trazabilidad y capacidad de respuesta. La ciberseguridad se convierte así en un elemento de gobernanza y confianza.

En definitiva, garantizar la continuidad operativa en entornos de Facility Management implica adoptar una estrategia integral. Priorizar la ciberseguridad interna, apostar por la actualización continua, fomentar la formación y gestionar los activos críticos son los pilares esenciales.

Porque, en un mundo digital, la ciberseguridad no es solo protección: es continuidad, confianza y sostenibilidad del negocio.

Rosa Ortuño
CEO de OptimumTIC

Asset Management y Property Management: dos funciones complementarias

Aunque suelen confundirse, Asset Management y Property Management responden a funciones distintas dentro del sector inmobiliario. Mientras el Property Management se centra en la gestión operativa diaria del activo, el Asset Management adopta una visión estratégica orientada a maximizar valor, rentabilidad y posicionamiento a largo plazo.

Gestión operativa frente a visión estratégica

En un mercado inmobiliario cada vez más profesionalizado, la diferenciación entre Asset Management y Property Management resulta fundamental para comprender cómo se gestionan realmente los activos inmobiliarios, ya que, ambas disciplinas trabajan sobre el mismo inmueble, pero lo hacen desde perspectivas, objetivos y horizontes temporales distintos.

El Property Management se enfoca principalmente en la gestión operativa y el funcionamiento diario del activo, su función consiste en garantizar que el inmueble opere correctamente, mantenga niveles adecuados de servicio y responda de forma eficiente a las necesidades de usuarios e inquilinos.

Dentro de este ámbito se incluyen tareas como coordinación de mantenimiento, gestión de incidencias, control de proveedores, seguimiento de contratos, supervisión técnica o relación con ocupantes, siendo por tanto el objetivo principal del Property Management asegurar la continuidad operativa y preservar el correcto funcionamiento del activo en el día a día.

La visión estratégica del activo

Por el contrario, el Asset Management tiene una visión más estratégica y financiera, su foco se sitúa en maximizar la rentabilidad del activo, optimizar su posicionamiento en el mercado y definir las decisiones que permitan incrementar valor a medio y largo plazo.

El Asset Manager analiza aspectos como rentas, ocupación, CAPEX, reposicionamiento, estrategia comercial, riesgos, sostenibilidad o potencial de desinversión, por lo que, no se trata únicamente de gestionar edificios, sino de gestionar inversiones inmobiliarias.

La importancia de la coordinación

En la práctica, ambas funciones deben trabajar de forma coordinada, en donde las decisiones estratégicas definidas desde Asset Management dependen en gran medida de la información operativa generada desde Property Management. Del mismo modo, una gestión diaria eficiente carece de sentido si no está alineada con los objetivos globales de rentabilidad y creación de valor.

Actualmente, muchos inversores demandan modelos de gestión cada vez más integrados, donde la visión técnica, operativa y financiera del activo se encuentren conectadas. En Afianza Real Estate, esta coordinación entre estrategia y operación resulta clave para entender el comportamiento real de los activos y detectar oportunidades de mejora tanto operativas como financieras y estratégicas.

Por otro lado, la creciente importancia de criterios ESG y eficiencia operativa ha reducido todavía más la separación tradicional entre ambas disciplinas. Aspectos como consumo energético, mantenimiento predictivo, experiencia del usuario o sostenibilidad impactan simultáneamente en la operación diaria y en la valoración futura del inmueble; un activo bien operado no siempre es un activo bien gestionado estratégicamente, pero una estrategia sólida difícilmente puede ejecutarse sin una operación eficiente.

Digitalización y creación de valor

La digitalización también está transformando esta relación gracias al uso de plataformas de gestión, sistemas de monitorización y herramientas de análisis de datos, permitiendo integrar información operativa y financiera en tiempo real y facilitando una toma de decisiones más ágil y precisa.

En muchos casos, la diferencia entre un activo que simplemente funciona y otro que realmente genera valor reside en la capacidad de coordinar ambas funciones bajo una visión común; ello ha provocado que la evolución del sector inmobiliario apunte precisamente hacia modelos de gestión más transversales, donde Asset Management y Property Management dejen de entenderse como departamentos aislados y pasen a formar parte de una estrategia unificada de creación de valor.

Afianza

Fama Systems: un modelo de crecimiento empresarial en Facility Management

Especializada en soluciones tecnológicas para la gestión integral de activos, espacios y servicios, FAMA vive desde 2021 una etapa de crecimiento excepcional y se consolida, con casi tres décadas de trayectoria, como referente en la digitalización del Facility Management en España, gracias a una plataforma flexible y un modelo basado en el rigor y el acompañamiento al cliente. Ángela García, FAMA General Manager, comparte las claves de este impulso.

¿Cómo describiría la evolución de FAMA desde 2021?
Han sido años de transformación y consolidación con una lógica clara: "crecer, sí, pero hacerlo bien". Hemos **aumentado los ingresos más de un 50%, mejorado la rentabilidad, duplicado la plantilla y abierto mercado en México**. Hemos experimentado un crecimiento progresivo y sostenido, que evidencia una estructura financiera sana y una correcta planificación a medio y largo plazo.

¿Cuáles han sido las claves del crecimiento?
Primero, una propuesta de valor enfocada en resolver problemas reales de gestión de activos, infraestructuras y servicios. Segundo, una estrategia comercial coherente, que prioriza relaciones a largo plazo. Y tercero, una ejecución alineada con esa estrategia. No hemos crecido aceleradamente, sino de forma progresiva, manteniendo los mismos estándares de calidad para cada cliente.

¿También han mejorado la rentabilidad?
El crecimiento solo tiene sentido si viene acompañado de rentabilidad. Nuestro **EBITDA ha aumentado un 64%**, lo que demuestra que estamos sabiendo convertir volumen de negocio en resultados para reinvertir y fortalecer estructura, innovar y seguir evolucionando.

El equipo ha crecido más de un 100%. ¿Cómo se gestiona una expansión así?
Con mucha planificación y con una idea clara: las personas están en el centro. No se trata solo de contratar más, sino de incorporar los perfiles adecuados y acompañarlos desde el inicio. Es una apuesta por la profesionalización: una organización preparada para proyectos complejos sin renunciar a los estándares de servicio y eficiencia.

Han pasado de una gestión de proyectos a una gestión de producto. ¿En qué consiste?
El cambio tecnológico no solo implica nuevas herramientas, sino también un cambio de mentalidad.

Hemos evolucionado hacia una gestión de producto centrada en la mejora continua, la flexibilidad y la adaptación a las necesidades del cliente. El producto ya no es algo cerrado, sino un ecosistema vivo. Desde esa visión hemos incorporado la IA, sin ir más lejos.

¿Cómo aplican la IA?
Como herramienta de eficiencia operativa. En gestión patrimonial, por ejemplo, usamos IA generativa, visión por computadora y reconocimiento inteligente de texto para extraer datos de cualquier PDF, escaneado o manuscrito. También agilizamos el aprendizaje con un asistente virtual integrado al sistema. Todo con tecnología segura, trazable y conforme al RGPD.

FAMA es un referente en la Administración Pública. ¿Cómo se ha alcanzado ese posicionamiento?
Con muchos años de trabajo, resultados y confianza. Conocemos las necesidades del sector público y sus exigencias normativas y contamos con amplia experiencia acompañando a numerosas administraciones en sus procesos de digitalización que hoy son clientes de referencia.

¿Qué ha supuesto la expansión a México?
Un hito estratégico. Nos ha permitido diversificar y ampliar alcance geográfico y confirmar nuestra capacidad de adaptar el modelo a nuevos contextos sin perder propuesta de valor.

¿Destacaría algún avance de infraestructura tecnológica?
La renovación de nuestro CPD, ubicado en España, con tecnología de última generación, certificaciones ENS, ISO 27001 e ISO 9001, energía verde y respaldo de INCIBE, refuerza la seguridad y la confianza de los clientes, sobre todo en sectores sensibles como la Administración Pública. También hemos renovado la infraestructura de virtualización para reforzar rendimiento, capacidad y estabilidad.

¿Qué significa hoy escoger FAMA?
Cuando un cliente opta por FAMA no está haciendo una simple compra de producto: está tomando una **decisión estratégica que afecta a los costes, operativa y a las personas** de su organización. Escoger FAMA significa valorar aspectos como la **solvencia y experiencia** del proveedor, la **seguridad** de los sistemas, la apuesta por la **I+D**, la **flexibilidad y capacidad de adaptación** de la herramienta, íntegramente desarrollada por FAMA, y, sobre todo, la **cercanía y el acompañamiento del equipo humano**. Además, formar parte de un grupo cotizado en BME Growth -Cuatroochenta-, añade un plus de transparencia y confianza a nuestros clientes.

Para cerrar, ¿cuál es el propósito de FAMA en los próximos años?
Nuestro propósito es estar al lado de nuestros clientes, ayudarlos a trabajar mejor cada día y acompañarlos en su evolución digital de FM con soluciones que realmente les aporten valor. Queremos seguir creciendo de forma sostenible, ampliando nuestra presencia internacional y siendo un referente por la calidad, la cercanía y la confianza que construimos con quienes confían en FAMA.

FAMA
a Cuatroochenta product

Facility Management, IA y ciberseguridad: la convergencia que transforma la continuidad operativa

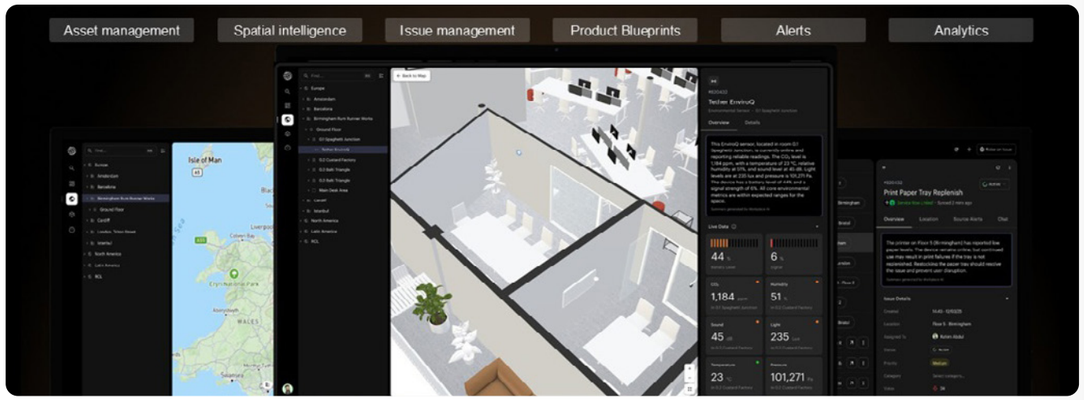
La continuidad operativa ya no depende únicamente de la redundancia tecnológica o de los planes de contingencia tradicionales. En un entorno marcado por la aceleración de la inteligencia artificial y el incremento constante de las amenazas digitales, la ciberseguridad se ha convertido en un pilar estructural dentro de las estrategias de Facility Management.

Hoy, garantizar la operatividad de un edificio, una infraestructura crítica o una organización implica también proteger sus entornos digitales, salvaguardar los datos y asegurar la capacidad de respuesta y recuperación ante cualquier incidente.

Los últimos análisis de TrendAI, compañía con la que mantenemos una alianza estratégica en el ámbito de la protección empresarial, evidencian un profundo cambio de paradigma. La compañía alerta de que los ciberataques impulsados por inteligencia artificial son cada vez más rápidos, autónomos y difíciles de detectar. De hecho, responsables tecnológicos y de negocio reconocen que únicamente consiguen identificar entre un 21% y un 40% de la actividad maliciosa vinculada a la IA, lo que pone de manifiesto un importante déficit de visibilidad y control.

Este contexto obliga a replantear la continuidad operativa desde una visión mucho más amplia e integrada. Ya no basta con prevenir interrupciones físicas: las organizaciones deben garantizar la resiliencia de sus infraestructuras híbridas, proteger los entornos cloud, on-premise y de tecnología operativa, y asegurar que sus sistemas pueden responder y recuperarse con rapidez ante cualquier incidente. La ciberresiliencia pasa así a convertirse en un objetivo prioritario para las compañías.

Para lograrlo, resulta imprescindible diseñar estrategias de ciberseguridad capaces de crear entornos más seguros y preparados para operar en la era de la inteligencia artificial. Esto requiere apoyarse en socios tecnológicos especializados que permitan mejorar la visibilidad de los sistemas, detectar vulnerabilidades, intrusiones y amenazas avanzadas, proteger modelos de IA, blindar entornos IoT y cualquier elemento conectado, además de reforzar la gobernanza de los datos y los procesos críticos.



La convergencia entre Facility Management, continuidad operativa y ciberseguridad ya es una realidad. En un escenario donde las amenazas evolucionan a gran velocidad, la resiliencia no dependerá únicamente de mantener las instalaciones en funcionamiento, sino de garantizar que toda la infraestructura tecnológica que las sustenta sea capaz de anticipar, resistir y recuperarse de cualquier ataque sin comprometer la actividad del negocio.

Para los responsables de FM, esto también implica avanzar hacia un workplace unificado que proporcione una visión centralizada y un mayor control sobre las operaciones, facilitando una gestión más eficiente, segura y resiliente de los espacios de trabajo.

La próxima evolución del workplace

Durante años, la tecnología del workplace ha evolucionado desde simples herramientas de reserva de salas hasta ecosistemas complejos que integran políticas híbridas, sensores IoT, climatización, sistemas AV, gestión de visitantes y controles de acceso. Sin embargo, aunque cada avance resolvía necesidades concretas, también añadía nuevas capas de complejidad.

Hoy, muchas organizaciones operan con múltiples plataformas desconectadas entre sí, generando fragmentación, ineficiencias y modelos de gestión reactivos. Este escenario choca directamente con las prioridades actuales de Facility Managers, CIOs y responsables de RRHH: optimizar costes, reforzar la resiliencia operativa y ofrecer una mejor experiencia al empleado. Los datos existen, pero permanecen dispersos; hay alertas, pero falta una inteligencia unificada que permita convertir esa información en decisiones ágiles y eficientes.

La próxima evolución del workplace no pasa por incorporar más herramientas, sino por conectarlas bajo una capa común de inteligencia. Con esta visión, Ricoh impulsa el concepto de "Workplace of Things", un ecosistema donde espacios, personas, activos, sensores e incidencias se integran en una única plataforma inteligente capaz de ofrecer una visión completa de las operaciones y actuar en tiempo real.

En este modelo, la tecnología deja de ser visible para convertirse en una experiencia natural y fluida: una plataforma de integración del workplace permitirá unificar todos los flujos de datos y permite anticiparse a incidencias, automatizar decisiones rutinarias y optimizar recursos mediante insights y recomendaciones impulsadas por IA.

Sobre esta base, se situará una capa de inteligencia contextual capaz de personalizar la experiencia del usuario mediante reservas conversacionales, asistencia en tiempo real y adaptación dinámica ante cambios o incidencias.

El resultado será un entorno laboral más eficiente, resiliente y sostenible, donde el workplace deja de percibirse como un coste operativo para convertirse en un activo estratégico. La verdadera revolución no será únicamente tecnológica, sino estratégica: transformar la complejidad en claridad para que las personas puedan centrarse en lo que realmente aporta valor.

RICOH
imagine. change.

Raquel Sánchez de Ron
Directora de Digital Workplace de Ricoh España

Ciberseguridad en edificios inteligentes

Cuando la infraestructura física se convierte en vector de ataque

Los edificios ya no son hormigón y cristal. Son sistemas vivos: toman decisiones, aprenden de su entorno y reaccionan en milisegundos. Pero esta inteligencia tiene un precio que pocas organizaciones han calculado del todo: cada sensor, cada actuación y cada protocolo de comunicación es una puerta potencial para un atacante.

La ciberseguridad ha dejado de ser un problema de los departamentos de IT para convertirse en el reto nuclear del Facility Management del siglo XXI.

La fusión entre los mundos OT (tecnología operacional) e IT ha creado un ecosistema de una complejidad sin precedentes. Los sistemas de climatización, control de accesos, ascensores, videovigilancia y gestión energética —todos interconectados— ya no operan en compartimentos estancos. Operan en red. Y eso significa que un único punto de vulnerabilidad puede comprometer simultáneamente la seguridad física de las personas, la continuidad operativa del edificio y la reputación de la organización que lo ocupa.

El riesgo no es hipotético. Es presente.

Un ataque exitoso sobre un sistema BMS puede manipular sensores de temperatura en un centro de datos, bloquear salidas de emergencia, desactivar alarmas contra incendios o desestabilizar la red eléctrica de una instalación crítica. El impacto no se mide solo en euros: se mide en confianza perdida, en servicios interrumpidos y, en el peor de los escenarios, en vidas humanas.

La diferencia FAMASE

Aquí es donde FAMASE aporta una diferencia real y medible. Nuestra aproximación a la gestión integral de instalaciones integra la ciberseguridad como capa transversal desde el diseño hasta la operación diaria, no como un añadido de última hora. Aplicamos una metodología que combina tres dimensiones:

Tecnología
Segmentación de redes OT/IT, cifrado de comunicaciones, gestión granular de privilegios, actualización continua de firmware y monitorización 24/7 con sistemas de detección de intrusiones

Proteger un edificio inteligente es, hoy, proteger la organización que vive dentro. Y en eso, FAMASE no improvisa: lidera.

capaces de identificar comportamientos anómalos antes de que se conviertan en incidentes.

Gobernanza
Coordinación real entre equipos de FM e IT, protocolos de actuación claros y una gobernanza transversal que elimina los silos organizativos que hacen vulnerables a la mayoría de los edificios. La seguridad no puede ser responsabilidad de un solo equipo; tiene que ser una cultura. Lectura relacionada: «Inteligencia artificial en la gestión de edificios, ¿cómo la puede utilizar un servicio de facility management?».

Personas
La mayoría de las brechas de seguridad no empiezan en un servidor. Empiezan en un error humano. Por eso, FAMASE incorpora programas de formación y concienciación para usuarios y proveedores, convirtiendo a cada persona en una línea de defensa activa.

Mejora continua frente a un riesgo que evoluciona

Lo que diferencia a FAMASE no es solo la capacidad técnica. Es la visión: tratamos la ciberseguridad como un proceso de mejora continua, con evaluaciones de riesgo periódicas, simulacros de incidentes y adaptación constante a un panorama de amenazas que evoluciona cada día.

En un mundo donde los edificios inteligentes acumulan datos sensibles, gestionan activos críticos y dan servicio a miles de personas, la resiliencia operativa no es opcional. Es la base sobre la que se construye todo el valor del Facility Management moderno. Lectura relacionada: «Normativas europeas que todo Facility Manager debe conocer».

FAMASE
Facility Management & Services

El edificio inteligente como infraestructura crítica: lecciones desde un campus tecnológico

Gestionar un complejo tecnológico de 7.500 m² con sedes en tres continentes obliga a replantear qué es una infraestructura crítica. Desde EDUCA EDTECH Group, con más de 120.000 estudiantes activos y operaciones 24/7, hemos aprendido que la continuidad operativa de un edificio ya no depende solo de sus sistemas físicos. Depende de su perímetro digital.

Un edificio es también una red

En un entorno cada vez más digital, más automatizado, lo disruptivo es volver a lo físico; por eso la ciberseguridad y el Facility Management están 'condenados' a entenderse. En EDUCA EDTECH Group lo sabemos bien.

Desde 2022, las instalaciones centrales de nuestro grupo tecnológico-educativo, en Granada, concentran las operaciones de un grupo con presencia en Granada, Madrid, Ámsterdam, Miami, México y Bogotá. Más de 4 millones de euros de inversión en un complejo diseñado con los últimos avances tecnológicos: climatización inteligente, sistemas de monitorización, conectividad distribuida. Un entorno pensado para la eficiencia operativa. Y, por esa misma razón, un entorno con una superficie de ataque que hace diez años no existía.

La frontera entre gestión del edificio y ciberseguridad ha desaparecido. Hoy, un sistema BMS comprometido es también un incidente de seguridad.

Cuando la ciberseguridad es también FM

El Facility Manager tradicional gestionaba activos físicos pero la realidad es que vivimos en un mundo líquido en el que la frontera de lo digital y lo analógico cada vez es más permeable. Hoy, el Facility Manager gestiona activos físicos conectados: un sistema BMS comprometido no solo genera una incidencia de mantenimiento, puede paralizar el acceso a las instalaciones, alterar las condiciones ambientales de los servidores o inhabilitar los protocolos de seguridad perimetral. **La frontera entre la gestión del edificio y la gestión de la ciberseguridad ha desaparecido.**

En nuestra organización, la coordinación entre el equipo de IT, el CISO y el responsable de instalaciones no es opcional, es un proceso protocolizado. Cualquier nuevo dispositivo conectado a la infraestructura del edificio -desde una cámara hasta un sensor de temperatura- pasa por un protocolo de evaluación de riesgos antes de integrarse en la red.

La amenaza no siempre llega por donde se espera

En nuestra experiencia, los vectores de ataque más frecuentes no son los más sofisticados, son los más cotidianos: un proveedor de mantenimiento que conecta un dispositivo no autorizado, una actualización de firmware pendiente en un sistema de control, un acceso remoto habilitado para diagnóstico que nadie desactivó. La complejidad de un edificio inteligente multiplica los puntos de entrada, y con ellos, la exposición.

Por eso la respuesta no es solo tecnológica, es organizativa. Esto eleva la exigencia hacia el FM que, no teniendo la obligación de saber de ciberseguridad –bastantes áreas de conocimiento acumula ya-, sí que debe tener como prioridad crítica su relación con el responsable de ciberseguridad de la organización. Deben compartir un lenguaje común, protocolos conjuntos y una visión unificada de qué significa continuidad operativa cuando el edificio y la red son la misma cosa.

Resiliencia como diseño, no como reacción

Lo que hemos aprendido gestionando un campus tecnológico con operaciones continuas es que la resiliencia no se improvisa. Se diseña. Significa tener identificados los sistemas críticos cuya caída detiene la operación, establecer redundancias, y haber ensayado los escenarios de fallo antes de que ocurran, siempre de la mano del FM, que es la primera línea de defensa en numerosas ocasiones.

El facility manager del futuro -y ya del presente- necesita entender de superficies de ataque tanto como de eficiencia energética. No para convertirse en un experto en ciberseguridad, sino para saber cuándo llamar al CISO y qué preguntarle.

Structuralia
Engineering eLearning

Daniel Cabrera
Chief Information Security Officer, EDUCA EDTECH Group

Los Sistemas de Gestión de la Iluminación, grandes aliados de la gestión de instalaciones

Este tipo de sistemas permiten maximizar la productividad y bienestar del usuario, así como minimizar costes energéticos y de mantenimiento

La gestión de instalaciones (*facility management*, en inglés) necesita aliados. Esta disciplina empresarial que integra a personas, espacios, procesos y tecnologías para garantizar el funcionamiento eficiente de los edificios se debe apoyar en todas aquellas herramientas que le permitan **optimizar sus infraestructuras y reducir costes** al mismo tiempo que se maximiza la productividad y el bienestar del usuario. Y la iluminación puede ser una de las más relevantes.

Actualmente, la normativa UNE-EN 52120-1:2022 regula la eficiencia energética de los edificios en España y respalda el uso de sistemas de control inteligente de la iluminación. Entre las principales ventajas de estas plataformas se encuentra el máximo aprovechamiento de la luz natural, así como un mayor ahorro y eficiencia y, en definitiva, **una automatización y optimización de los procesos** que nos acerca más a los edificios y las ciudades inteligentes, presente y futuro de nuestra sociedad.

VIVARES de LEDVANCE, el aliado natural de la gestión de instalaciones

En **LEDVANCE** creemos que no es suficiente con iluminar; es necesario garantizar que el Sistema de Gestión de la Iluminación responda con precisión ante cualquier imprevisto. Por ello, **VIVARES** permite a los profesionales encargados de la gestión de la instalación alcanzar una infraestructura fiable y eficiente.

En LEDVANCE creemos que no es suficiente con iluminar; es necesario garantizar que el Sistema de Gestión de la Iluminación responda con precisión ante cualquier imprevisto.

Una automatización y optimización de los procesos que nos acerca más a los edificios y las ciudades inteligentes, presente y futuro de nuestra sociedad.

VIVARES de **LEDVANCE** integra desde unidades de control hasta luminarias, sensores y acopladores de pulsador. Además, su configuración es rápida y sencilla a través de web o móvil.

Este sistema es compatible con el control mediante cableado gracias a la tecnología DALI-2 y con la configuración inalámbrica a través de **Zigbee 3.0**. Asimismo, ofrece una serie de servicios en la nube adicionales que van desde la optimización del consumo energético hasta la prevención de los costes de mantenimiento y los diagnósticos de error para garantizar un óptimo funcionamiento del sistema.

Dentro de **VIVARES** contamos con **DIRECT EASY**, el Sistema de Gestión de la Iluminación sencillo e inalámbrico diseñado especialmente para los profesionales de la industria. Esta solución es ideal para cualquier tipo de proyecto y destaca por permitir la configuración rápida y sencilla de luminarias y accesorios a través de una aplicación móvil gracias a la tecnología **Bluetooth** sin necesidad de pasarela adicional.

En **LEDVANCE** ofrecemos así soluciones que son aliadas naturales de la gestión de instalaciones. Sistemas de Gestión de la Iluminación de última generación que garantizan la seguridad y prevención, así como el ahorro y la eficiencia.

LEDVANCE

Vacway: más de 30.000 taquillas inteligentes liderando los espacios de alta afluencia en Europa

El ecosistema tecnológico que convierte la gestión de espacios de ocio en una ventaja competitiva

De la fricción al flujo: por qué nació Vacway

Cuando una persona llega a un parque temático, un estadio o una estación de esquí, no viene a gestionar complicaciones: viene a disfrutar. Sin embargo, el primer contacto suele ser exactamente eso, una cola, una taquilla oxidada, una llave física que se pierde una fricción que empaña lo que debería ser el inicio de una experiencia memorable.

Vacway nació para eliminar esa fricción. Trabajamos desde dentro de los espacios de ocio de mayor afluencia de Europa, analizando flujos operativos y detectando los puntos exactos donde la experiencia se rompe antes de empezar. Hoy, con **más de 30.000 unidades instaladas en más de 10 países europeos**, somos el ecosistema tecnológico de referencia para operadores que quieren transformar sus procesos complementarios en una ventaja real. Una solución que encuentra su aplicación natural en los sectores que gestiona el Facility Manager: **espacios de ocio y entretenimiento, hoteles y resorts, grandes inmuebles corporativos e instalaciones deportivas.**

Con más de 30.000 unidades en Europa, Vacway demuestra que automatizar la experiencia del visitante no es un lujo: es la nueva ventaja competitiva.

Un ecosistema, múltiples soluciones

Nuestro producto principal son los VACWAYlockers: taquillas inteligentes que permiten al visitante guardar sus pertenencias en **menos de un minuto**, sin llaves físicas, con acceso inmediato desde la propia puerta gracias a Quick Access, un sistema único en el mercado europeo. Pero Vacway no es solo una empresa de taquillas.

El ecosistema incluye VACWAYkiosk para la venta de entradas y fast passes en autoservicio; soluciones de **Food & Beverage** para agilizar pedidos y reducir tiempos de espera en restauración; y **VACWAYwaterproof**, un sistema exclusivo de protección de móviles mediante funda sellada al vacío, diseñado para entornos acuáticos. Todo conectado a **VACWAYmanagement**, la plataforma cloud que permite al operador controlar ventas, incidencias y rendimiento en tiempo real.

Donde más se nos necesita

Vacway opera en los entornos donde la afluencia masiva convierte cada minuto en un activo crítico: parques temáticos y acuáticos, estaciones de esquí, estadios deportivos, museos de alta afluencia y recintos feriales. En todos estos espacios el reto es el mismo **eliminar colas, automatizar servicios y generar nuevas fuentes de ingreso** y nuestra solución responde a los tres frentes a la vez.

El Facility Manager es una figura clave en este proceso. Es quien define los estándares operativos del espacio, gestiona los flujos de personas y evalúa qué tecnología puede mejorar la eficiencia global de las instalaciones. Vacway entiende ese rol: nuestras soluciones se integran en la operativa existente con mínima intervención y ofrecen uptime del 99,7% gracias a baterías internas. Pero lo que realmente marca la diferencia es la inteligencia de datos: a través de VACWAYmanagement, el FM puede evaluar en tiempo real el rendimiento de cada activo, medir el impacto de la inversión, analizar la conversión de uso y tomar decisiones informadas respaldadas por métricas reales.

Un modelo adaptado a cada operador

La flexibilidad comercial es otra de nuestras señas de identidad. Ofrecemos tanto la **venta directa** del equipamiento con licencia de software y mantenimiento adicionales, el **alquiler**, y el **revenue-share**, donde Vacway asume la inversión inicial y comparte los ingresos generados con el operador. Esto elimina las barreras de entrada y permite que cualquier espacio acceda a tecnología de primer nivel desde el primer día.

Vacway

Cuando el edificio se conecta, la seguridad no puede quedarse fuera

Imagina que un lunes por la mañana tu sistema de control de accesos deja de responder. El proveedor tarda horas en acusar recibo. Mientras tanto, nadie sabe si el fallo es técnico o algo peor. Esa situación, que algunos facility managers ya han vivido en sus propias instalaciones, tiene un origen muy concreto: se tomó la decisión de conectar, pero no se preguntó cómo. Digitalizar el FM no tiene vuelta atrás, y no debería tenerla. Pero hacerlo bien exige algo más que elegir el sistema con mejor demo.

Tu edificio ya vive en la red

Hace no tanto, gestionar un edificio significaba controlar lo que se podía ver y tocar: mantenimiento, limpieza, espacios, consumos. Hoy, buena parte de esa gestión pasa por sistemas que intercambian datos en tiempo real: lockers de paquetería que reportan cada movimiento al sistema central, control de accesos que vive en la nube, climatización que aprende de patrones de uso, contadores que envían lecturas sin que nadie tenga que ir a leerlos. Todo eso tiene un valor enorme para la operación, y nadie que haya trabajado con ello quiere renunciar a él. Pero cada uno de esos sistemas abre una ventana hacia la red de la empresa. Y una ventana mal cerrada es una oportunidad para quien no debería entrar.

El riesgo no está en la tecnología. Está en quién la diseña.

Aquí es donde muchos debates sobre ciberseguridad en FM pierden el foco. El problema no es conectarse: es hacerlo con un proveedor que no ha pensado en lo que pasa después. La diferencia entre un sistema seguro y uno que genera un problema real está en decisiones concretas que se toman mucho antes de la instalación: dónde se guardan los datos y bajo qué legislación, cómo se cifra cada comunicación, qué acceso real tiene el proveedor a tu red una vez que el sistema está en marcha, qué ocurre si hay una actualización de firmware y nadie avisa. Esas preguntas no son técnicas. Son preguntas de gestión, y el facility manager tiene todo el derecho —y la responsabilidad— de hacerlas.

La ciberseguridad no se gestiona el día del incidente: se diseña antes, en el contrato y en la arquitectura del sistema que conectas a tu edificio.

5 PREGUNTAS ANTES DE FIRMAR

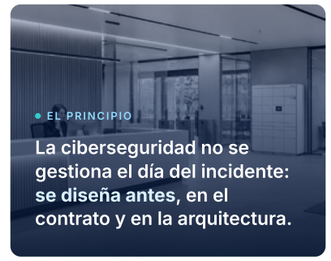
01
¿Qué pasa si el sistema pierde conexión con la nube?
El edificio debe seguir funcionando en local.
Si la respuesta no es clara, el riesgo operativo es real.

02
¿Tiene certificaciones vigentes (ISO 9001 / ISO 27001)?
Pide los certificados en vigor, no la mención.
Si los tiene, los aporta sin problema.

03
¿Dónde se alojan los datos y bajo qué marco?
Servidores en la UE simplifican GDPR y NIS2.
Eliminan riesgos de soberanía digital.

04
¿Qué acceso remoto exige y cómo lo aísla?
El perímetro se define desde el diseño.
Un proveedor serio no lo improvisa después.

05
¿Cómo se registran los accesos, usuarios y técnicos?
Debe existir un registro auditable.
Saber qué pasó, cuándo y quién estuvo implicado.



No necesitas ser experto en tecnología para poder alinearte con el equipo de IT

Un FM no necesita entender de arquitecturas de software para tomar buenas decisiones tecnológicas. Necesita saber qué pedir. Que el proveedor tenga certificaciones como ISO 27001 es la evidencia de que existe un protocolo definido para gestionar la seguridad de tus datos si algo falla. Que opere bajo el marco regulatorio europeo —GDPR, NIS2— reduce el riesgo de que los datos de la empresa acaben bajo jurisdicciones que no controlas. Que el sistema esté diseñado para seguir funcionando aunque pierda conexión con la nube es la diferencia entre un incidente menor y un edificio bloqueado.

En entornos donde las auditorías de seguridad son exigentes —banca, salud, industria, consultoría... — hemos comprobado que la confianza con los proveedores tecnológicos no se construye en el momento de la venta. Se construye en la operación diaria, en la transparencia ante una incidencia y en la capacidad de demostrar, con documentación real, que se han hecho los deberes.

El facility manager, y el equipo de IT que lo respalda, que pregunta dónde están sus datos y cómo se protegen no están siendo excesivos. Está haciendo su trabajo.

columat

Carmen Velasco
Head of Marketing & Growth en Columat

Facility Management y edificios inteligentes: nuevas herramientas para una gestión más eficiente

Cómo la digitalización mejora la gestión de accesos y los servicios al ocupante

La continuidad operativa se ha convertido en uno de los principales retos de la gestión de edificios. Más allá del correcto funcionamiento de las instalaciones técnicas, los responsables de Facility Management deben garantizar que los servicios que utilizan diariamente empleados, visitantes y usuarios funcionen de forma ágil, segura y eficiente.

En este contexto, la digitalización está transformando procesos tradicionalmente vinculados a la recepción, el control de accesos o la gestión de incidencias. La incorporación de nuevas tecnologías permite optimizar recursos, mejorar la experiencia del ocupante y disponer de una mayor trazabilidad de las operaciones.

Accesos más eficientes

La gestión de accesos ha evolucionado notablemente en los últimos años. Los sistemas actuales, mediante conserjería remota y aplicación móvil, permiten gestionar autorizaciones temporales, controlar entradas y salidas y ofrecer diferentes niveles de acceso según el perfil del usuario.

La integración de estos sistemas inteligentes facilita una gestión más flexible de visitantes, proveedores y personal autorizado, al tiempo que genera registros que permiten conocer y analizar el uso de los espacios.

Estas herramientas resultan especialmente útiles en edificios corporativos, complejos sanitarios, hoteles o instalaciones con elevada afluencia de personas, donde la agilidad operativa es factor clave.

La digitalización de los servicios al ocupante

La tecnología también está modificando la forma en que los usuarios interactúan con los servicios del edificio. La posibilidad de gestionar accesos, comunicar incidencias o realizar autorizaciones desde una aplicación móvil simplifica procesos que tradicionalmente requerían atención presencial.

Este modelo contribuye a mejorar la experiencia del ocupante y permite a los gestores disponer de información centralizada para optimizar la prestación de los servicios.

La digitalización no sustituye la atención personal cuando esta es necesaria, sino que permite dedicar más tiempo a aquellas tareas que aportan un mayor valor añadido a la operación.

Horizon by Calordom: tecnología aplicada a la gestión diaria

Horizon by Calordom es una solución orientada a la gestión inteligente de accesos y servicios en edificios. A través de una aplicación móvil y tecnologías basadas en inteligencia artificial, permite gestionar autorizaciones, controlar accesos, facilitar la comunicación con usuarios y optimizar la recepción de paquetería mediante lockers inteligentes.

La solución contribuye a mejorar la trazabilidad de las operaciones y a simplificar procesos cotidianos tanto para gestores como para usuarios, alineándose con la creciente digitalización del sector inmobiliario y del Facility Management.

https://www.calordom.com/servicio-conserje-virtual/

El reto creciente de la paquetería

El aumento del comercio electrónico ha convertido la recepción de paquetería en un servicio cada vez más relevante dentro de muchos edificios. La gestión manual de paquetes genera tareas administrativas, necesidades de almacenamiento y posibles incidencias asociadas a las entregas.

La incorporación de lockers inteligentes y sistemas digitales de gestión permite mejorar la trazabilidad de los envíos, optimizar los espacios disponibles y ofrecer una mayor flexibilidad a los usuarios para recoger sus paquetes cuando lo necesiten.

Además de mejorar la experiencia del ocupante, estas soluciones contribuyen a reducir cargas operativas y a aumentar la eficiencia de la gestión diaria.

Tecnología al servicio de la continuidad operativa

La aplicación de inteligencia artificial y sistemas conectados permite detectar eventos relevantes, automatizar determinadas tareas y generar información útil para la toma de decisiones. Sin embargo, el verdadero valor de estas herramientas no reside únicamente en la tecnología, sino en su capacidad para facilitar la labor diaria de los responsables de la gestión del edificio.

La digitalización de procesos como el control de accesos, la gestión de autorizaciones o la recepción de paquetería reduce tareas administrativas, mejora la trazabilidad de las operaciones y minimiza incidencias asociadas a la gestión diaria. Esto permite a los facility managers y gestores de activos dedicar más tiempo a actividades estratégicas y de mayor valor añadido.

Además, disponer de información centralizada y registros actualizados facilita la coordinación con proveedores, mejora la capacidad de respuesta y contribuye a una gestión más eficiente de los recursos disponibles.

En un entorno cada vez más exigente, la combinación de gestión inteligente de accesos, digitalización de servicios y soluciones para la recepción de paquetería se consolida como un aliado para reforzar la continuidad operativa y mejorar la eficiencia de los edificios.

Ángeles Sánchez
Responsable Proyecto Calordom

Servicio Nilfisk, la clave para la continuidad operativa en entornos conectados

En el FM actual, la continuidad operativa ha dejado de ser un concepto teórico para convertirse en una prioridad de negocio. La capacidad de una organización para mantener sus operaciones ante cualquier interrupción depende en gran medida de la gestión de sus activos físicos. En este contexto, la limpieza profesional juega un papel más estratégico de lo que tradicionalmente se ha considerado. La disponibilidad de los equipos, su correcto mantenimiento y su integración en entornos conectados influyen directamente en la resiliencia operativa de una instalación.

El coste real de la no continuidad

Las cifras evidencian la magnitud del reto. Se estima que el *downtime* no planificado genera pérdidas de hasta 1,4 billones de dólares anuales en grandes compañías a nivel global. Además, el mantenimiento reactivo puede ser entre tres y cinco veces más costoso que el preventivo.

Más allá del impacto económico, las interrupciones afectan directamente a la calidad del servicio, los acuerdos de nivel de servicio (SLA) y la reputación de las organizaciones: hasta el 44% de las empresas reconoce que el *downtime* compromete su capacidad de cumplir compromisos operativos.

En este escenario, el servicio deja de ser un soporte técnico para convertirse en un componente crítico dentro de los planes de continuidad de negocio.

Del mantenimiento a la resiliencia operativa

El rol del FM ha evolucionado hacia la gestión integral del riesgo. Según IFMA, es un actor clave en la identificación de riesgos, la implementación de medidas preventivas y la garantía de la resiliencia de la infraestructura.

Esto implica un cambio de paradigma: **el mantenimiento ya no consiste únicamente en reparar equipos, sino en anticipar fallos, minimizar impactos y asegurar la continuidad de los procesos críticos.**

En entornos industriales o técnicos —como alimentación, farmaquímica, manufacturera o metalúrgica— este enfoque es aún más relevante. La gestión del polvo o de residuos, especialmente en entornos ATEX, no solo afecta a la eficiencia, sino que puede comprometer la seguridad de toda la instalación si no se gestiona correctamente.

Equipos conectados: nuevas oportunidades, nuevos riesgos

La digitalización ha impulsado una nueva generación de activos conectados. Sensores, plataformas IoT y sistemas de monitorización permiten optimizar el mantenimiento y mejorar la toma de decisiones.

De hecho, el mantenimiento predictivo puede reducir costes entre un 25% y un 40% y disminuir significativamente el *downtime*. Sin embargo, esta conectividad introduce un nuevo desafío: la ciberseguridad.

El servicio ha dejado de ser un soporte técnico para convertirse en una pieza clave en la continuidad operativa y la resiliencia de las organizaciones.

Los equipos conectados forman parte del ecosistema digital de la organización, y su vulnerabilidad puede tener consecuencias operativas. Los ataques a dispositivos IoT han aumentado de forma significativa en los últimos años —con crecimientos superiores al 80% en intentos de brecha— y pueden afectar directamente a sistemas físicos, provocando paradas de producción o fallos en infraestructuras críticas.

El reto del talento en mantenimiento

La evolución hacia modelos conectados y predictivos plantea también un desafío humano. Se estima que más del 60% de los responsables de mantenimiento tiene dificultades para encontrar perfiles técnicos cualificados, especialmente en tecnologías digitales.

Para el FM, esto implica reforzar la formación y apostar por *partners* capaces de aportar no solo servicio técnico, sino también conocimiento experto y acompañamiento en entornos cada vez más complejos.

Descubre por qué Nilfisk es el partner que va más allá del servicio

En este contexto, el servicio debe garantizar no solo el funcionamiento técnico del equipo, sino también su integración segura dentro de la infraestructura digital.

El papel de Nilfisk

Nilfisk ha evolucionado su modelo de servicio para responder a este nuevo entorno, integrándolo como un pilar clave dentro de la continuidad operativa de sus clientes. A través de acuerdos de mantenimiento adaptados, soluciones de gestión de flotas, formación de operarios y asistencia técnica especializada, la compañía contribuye a maximizar la disponibilidad y el rendimiento de los equipos.

Este enfoque permite al FM contar con mayor visibilidad, control y capacidad de anticipación sobre sus activos, alineando el servicio con los objetivos de eficiencia, seguridad y resiliencia.

Porque hoy, en un entorno donde los activos están cada vez más conectados y las interrupciones tienen un impacto inmediato, la continuidad operativa no depende solo de evitar fallos, sino de anticiparlos, gestionarlos y protegerlos en todo momento.

NILFISK

El Grupo EULEN impulsa una nueva etapa con el nombramiento de María Álvarez Becerril como Vicepresidenta Ejecutiva

La compañía apuesta por un modelo de liderazgo basado en el conocimiento del negocio, las personas y la visión internacional.

El Grupo EULEN, líder en la prestación de servicios especializados a empresas, ha anunciado el nombramiento de María Álvarez Becerril como nueva Vicepresidenta Ejecutiva. Esta decisión se enmarca en la apuesta por seguir afianzando una organización sólida, ágil y preparada para afrontar los retos de crecimiento y transformación en todos los mercados donde opera.

La incorporación de María Álvarez Becerril representa, además, la continuidad de un proyecto empresarial familiar con más de 60 años de historia, comprometido con la excelencia y la visión de largo plazo.

María Álvarez Becerril se incorporó al Grupo EULEN en 2015 y, desde entonces, ha desarrollado su trayectoria en distintas áreas y geografías de la compañía, participando en proyectos estratégicos tanto en España como en Portugal y Perú. Hasta su actual nombramiento, ocupaba la Dirección Corporativa de Recursos Humanos, posición desde la que ha liderado iniciativas vinculadas a cultura, liderazgo, talento y transformación organizativa, impulsando una visión de las personas como eje estratégico para el crecimiento y la sostenibilidad de la compañía. Este nombramiento supone la incorporación de la tercera generación de la familia Álvarez a la más Alta Dirección de la Compañía.

Graduada en Administración y Dirección Internacional de Empresas, cuenta además con formación ejecutiva en dirección de personas y liderazgo por el Centro de Estudios Garrigues y el IE Business School.

Con este nombramiento, el Grupo EULEN consolida una organización preparada para afrontar los retos futuros desde la experiencia, la cercanía al negocio y una firme apuesta por las personas.

El reto del talento en mantenimiento

El Grupo EULEN es líder en nuestro país en la prestación de servicios a empresas, con el objetivo de ofrecer a la sociedad servicios innovadores que aportan soluciones útiles, de calidad y más eficientes. Está especializado en las actividades de limpieza, seguridad, servicios auxiliares (de logística, generales y de telemarketing), FSM (Facility Services & Management), servicios sociosanitarios, mantenimiento integral, trabajo temporal y medio ambiente. Fundada en 1962 en Bilbao, la compañía está presente en 11 países y el volumen de ventas consolidadas supera los 1.800 millones de euros, con una plantilla global de 72 000 personas.

El Grupo EULEN está adherido al Pacto Mundial y firmemente comprometido con la sociedad a través del desarrollo de políticas socialmente responsables: integración laboral de colectivos desfavorecidos, conciliación de la vida familiar y profesional para su personal de estructura, con la obtención del certificado efr, patrocinio y mecenazgo de la cultura y el arte, protección del medio ambiente, etc.

Patrocinadores IFMA España

Patrocinadores Oro

FRACTTAL

INFRASPEAK

Patrocinadores Plata

CBRE

genera facility services

FOVASA facility services

ISS

serveo

Patrocinadores Bronce

AMBILAMP

CPS

delikia fresh

Honeywell

INDEL FACILITIES S.A.

Limcamar

mediterráneo

MINSAIT

optima facility

OTIS

pre zero

TDGI

selecta

SPACEWELL

the mail company 25 AÑOS

VIGILANT

Empresas colaboradoras

acciona Service

Afianza

antana spaces design & build

aquaservice

ARMONIA

aspor ENGINEERING

BACHMANN We power your life

calordom

columat

CT ACTIVA

elecnor

GRUPO EULEN

FAMA

FAMASE facility Management & Services

Foot Analytics

FUTURE MOTORS

HEXAGON

IC

IMAN

Lacera

LEDVANCE

LOXONE

MEGABLOK

eFM ENGAGING PLACES

monolitic

NILFISK

ojmar

Planon Building Connections

JURADO

RICOH imagine. change.

ROSMIMAN makes it simple

SDV & Partners

GRUP MEDIAPRO

Sifu

SIGE21

sodexo

SPOLUZ LIGHTING

Structuralia

TTR MECHANICAL

Vacway TECH IT SIMPLE

ZEMPER

IFMA España Chapter
International Facility Management Association

Pº de la Habana 9-11
28036 Madrid
(+34) 636 066 027 / (+34) 682 682 653
www.ifma-spain.org