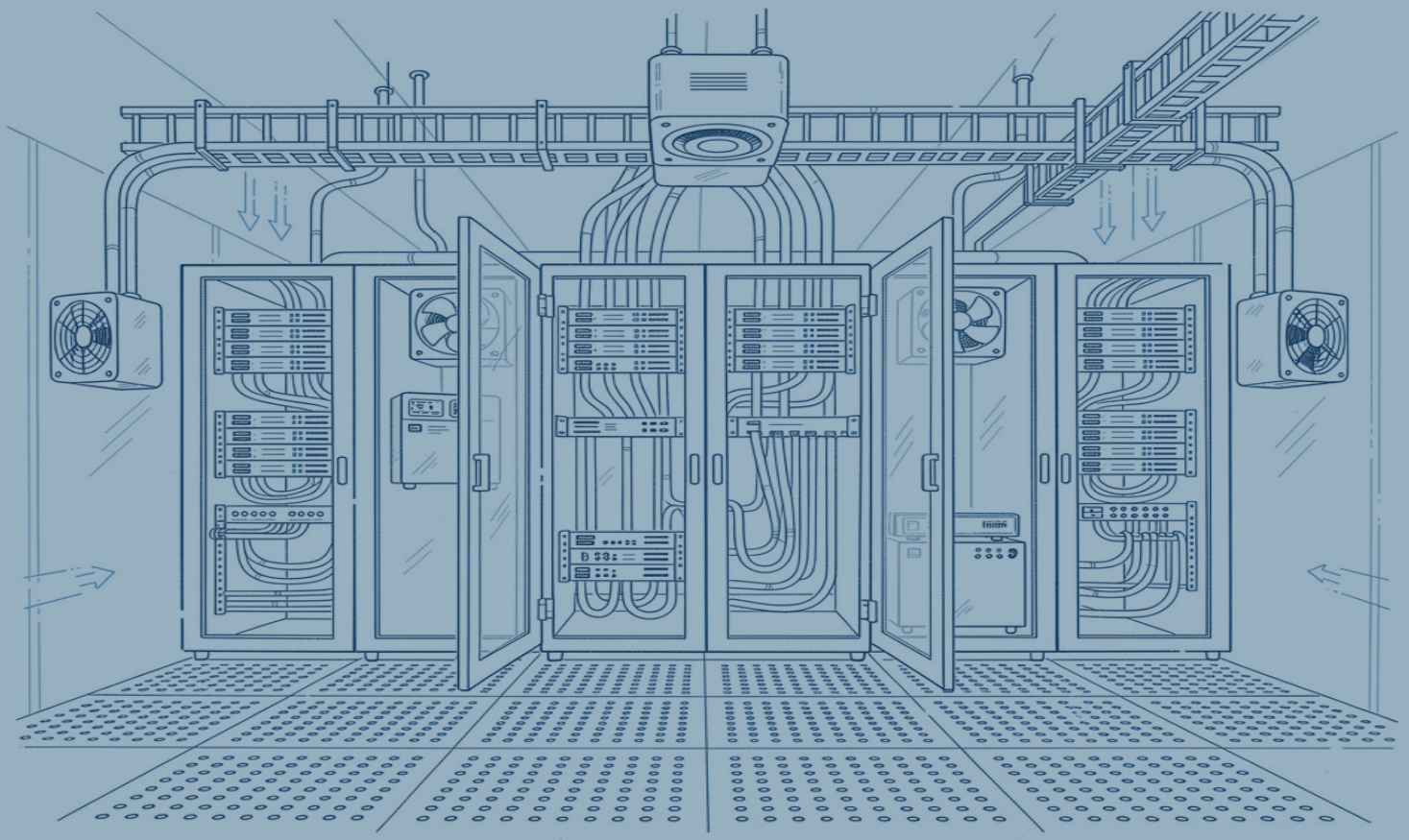
Bjumper

Retrofitting en Data Centers

Modernización de infraestructuras críticas sin comprometer la disponibilidad



Introducción

La infraestructura de datos es el sistema nervioso de cualquier organización moderna. Cada transacción, cada proceso crítico de negocio, cada comunicación depende de que los datos estén disponibles, seguros y accesibles en tiempo real. En este contexto, los centros de datos (CPD) ya no son simples salas de servidores: son activos estratégicos de primer orden.

Sin embargo, la realidad es que una gran parte de los data centers en operación hoy fueron diseñados hace más de una década, cuando las demandas tecnológicas, las cargas de trabajo y los requisitos de eficiencia eran radicalmente distintos. La irrupción de la inteligencia artificial, el edge computing, los servicios en la nube híbrida y la explosión de datos han convertido estas infraestructuras en cuellos de botella potenciales para el crecimiento del negocio.

El retrofitting, la modernización de un data center existente sin necesidad de una nueva construcción desde cero, emerge como la respuesta estratégica y económicamente viable a este desafío. Este ebook ofrece una guía técnica completa sobre qué implica un proyecto de retrofitting, por qué la disponibilidad de la información es un activo crítico no negociable, cuáles son los principales riesgos asociados y cómo mitigarlos con éxito.

¿Para quién es esta guía?

Este documento está dirigido a responsables de infraestructura IT, administradores de sistemas, arquitectos de data center e ingenieros de operaciones que se enfrentan a decisiones de modernización de sus CPDs o que necesitan comprender el alcance técnico y estratégico de un proceso de retrofitting.

¿Qué es el retrofitting en Data Centers?

Definición y concepto

El término retrofitting proviene del inglés y hace referencia al proceso de actualizar, mejorar o modernizar los componentes de una instalación existente con el fin de extender su vida útil, mejorar su rendimiento y adaptarla a nuevos requisitos sin necesidad de construir una nueva infraestructura desde cero.

Aplicado al mundo de los centros de datos, **el retrofitting implica la renovación parcial o total de sistemas críticos**, eléctricos, de refrigeración, de conectividad, de seguridad, mientras la instalación permanece en operación. Este aspecto es, precisamente, el que define la complejidad y la criticidad del proceso: se trabaja sobre una «instalación viva», donde cualquier error puede traducirse en pérdida de servicio.

Retrofitting vs. Greenfield: dos aproximaciones diferentes

Es importante diferenciar el retrofitting de un proyecto greenfield (construcción de un nuevo data center desde cero):

Críterio	Retrofitting	Greenfield
Inversión inicial	Moderada	Muy elevada
Tiempo de ejecución	Semanas o meses	12–24 meses
Riesgo operacional	Alto (instalación viva)	Bajo
Continuidad de servicio	Crítica durante el proceso	No aplica
Flexibilidad de diseño	Limitada a la estructura existente	Total
Impacto ambienta	Bajo (reutilización)	Alto (nueva construcción)
Ideal para...	Optimizar activos existentes	Nuevas capacidades y ubicaciones

Bjumper

¿Cuándo es el momento de hacer retrofitting?

Existen señales inequívocas de que un data center ha alcanzado el límite de su ciclo de vida operativo sin actualización:

- Los sistemas de climatización no consiguen mantener las temperaturas de operación seguras con las densidades de carga actuales.
- El PUE (Power Usage Effectiveness) supera 1.8, indicando una eficiencia energética deficiente.
- Los sistemas de alimentación ininterrumpida (UPS) tienen más de 10 años y no cuentan con soporte del fabricante.
- La infraestructura eléctrica no puede asumir cargas superiores a los 5 kW/rack cuando el mercado exige densidades de 10–30+ kW/rack para workloads de IA.
- Los tiempos de respuesta ante incidencias se incrementan por la dificultad de obtener repuestos de componentes obsoletos.
- El data center no cumple con las normativas vigentes de seguridad, eficiencia energética o protección de datos.

Dato clave

Según estudios recientes del sector, más del 40% de los centros de datos en operación tienen limitaciones significativas en su distribución eléctrica, lo que incrementa el riesgo de fallos críticos y reduce su capacidad de adaptación a nuevas cargas de trabajo.

El contexto actual por qué el retrofitting es urgente

El sector de los centros de datos atraviesa una transformación sin precedentes. La demanda de capacidad de procesamiento crece a tasas que ninguna nueva construcción puede satisfacer por sí sola, haciendo del retrofitting no una opción, sino una necesidad estratégica.

La explosión de datos e inteligencia artificial

La adopción masiva de IA generativa, machine learning y big data ha incrementado drásticamente la densidad de potencia en los data centers. Mientras un centro tradicional opera con 3–5 kW/rack, las cargas de IA requieren entre 10 y 30 kW/rack, y los entornos más avanzados superan los 100 kW/rack.

Esta evolución hace que muchos data centers diseñados hace apenas una década necesiten importantes actualizaciones eléctricas y de refrigeración para soportar las nuevas demandas..

La escasez de suelo y energía acelera el retrofitting

En los principales hubs de data center europeos (Madrid, Frankfurt, Ámsterdam, Londres, Dublín) la disponibilidad de suelo con acceso a suficiente potencia eléctrica es cada vez más limitada. Además, los plazos para licencias, conexión a red y construcción de nuevas instalaciones suelen superar los 24–36 meses.

Ante esta realidad, el retrofitting de instalaciones existentes permite ampliar capacidad en ubicaciones estratégicas con plazos de ejecución radicalmente menores, aprovechando la infraestructura de red y los accesos ya establecidos.

Bjumper

La presión regulatoria y ESG

La normativa europea en materia de eficiencia energética (EN 50600, Directiva de Eficiencia Energética, regulaciones Net Zero) exige que los operadores de data center mejoren progresivamente sus indicadores de sostenibilidad. Un PUE alto o el uso de sistemas de refrigeración obsoletos no solo genera sobrecostes operativos, sino que puede convertirse en un obstáculo regulatorio y reputacional.

El retrofitting bien ejecutado no solo moderniza la infraestructura técnica: abre la puerta a la obtención de certificaciones TIER y sellos de sostenibilidad que incrementan el valor del activo.

>40%

de los DC tienen limitaciones eléctricas críticas

40%

de la energía consume la climatización en CPDs tradicionales

Áreas críticas de intervención

Un proyecto de retrofitting abarca múltiples disciplinas técnicas que deben abordarse de forma coordinada. La modernización de un sistema en aislamiento, sin tener en cuenta sus interdependencias con el resto de la infraestructura, puede generar nuevos problemas o trasladar el cuello de botella a otro punto del sistema.

Sistemas de climatización y control térmico

La refrigeración es uno de los subsistemas más críticos y más costosos de un data center. En instalaciones tradicionales, los sistemas HVAC (Heating, Ventilation and Air Conditioning) basados en aire no son capaces de gestionar las densidades de potencia que exigen los workloads modernos.

Tecnologías de modernización aplicables:

Refrigeración líquida directa (Direct Liquid Cooling / DLC)	Conduce el calor generado por los procesadores directamente mediante agua o dieléctricos, sin necesidad de mover grandes volúmenes de aire. Indispensable para densidades superiores a 20 kW/ rack.
In-row cooling	Unidades de refrigeración integradas en los propios pasillos de rack, que reducen la distancia entre la fuente de calor y el punto de extracción.
Free cooling	Aprovechamiento del aire exterior en condiciones climáticas favorables para reducir el consumo de los sistemas de refrigeración mecánica.
IA Climate Management	Sistemas de control climático basados en inteligencia artificial que predicen y previenen puntos calientes antes de que se produzcan, optimizando el consumo energético en tiempo real.

Bjumper

Impacto en PUE

La actualización de los sistemas de climatización puede reducir el PUE desde valores típicos de 1.8–2.2 en instalaciones antiguas hasta 1.2–1.4 en instalaciones modernizadas, lo que representa ahorros de entre el 15% y el 40% en el coste energético anual.

Infraestructura cléctrica y sistemas UPS

La fiabilidad del suministro eléctrico es la piedra angular de la disponibilidad de un data center. Un fallo en el sistema de alimentación no tiene solución técnica posible si la infraestructura eléctrica no cuenta con la redundancia adecuada.

Elementos clave en la modernización eléctrica:

Sustitución de UPS obsoletos:

los sistemas de alimentación ininterrumpida de tecnología convencional (doble conversión en línea con tecnología IGBT) deben ser reemplazados por modelos de última generación con mayor eficiencia (>98% en modo ECO) y mejor gestión de la batería.

Actualización de PDUs (Power Distribution Units):

las unidades de distribución inteligentes permiten la monitorización en tiempo real del consumo por rack y la detección temprana de anomalías.

Modernización de cuadros de baja tensión:

adaptación de la capacidad de distribución a las nuevas densidades de carga requeridas.

Generadores de respaldo:

revisión y actualización de los grupos electrógenos para garantizar la autonomía y la capacidad de arranque en el tiempo establecido por los SLAs.

Arquitectura de distribución eléctrica redundante (2N, N+1):

diseño de la red de distribución para eliminar puntos únicos de fallo en la cadena eléctrica.

Cableado y conectividad

La conectividad es el sistema vascular del data center. Un cableado desordenado o con tecnologías obsoletas no solo limita el rendimiento de la red, sino que genera resistencias al flujo de aire que impactan directamente en la eficiencia térmica del CPD.

- Migración a fibra óptica de alta densidad (OS2, OM5) para backbone de alta velocidad.
- Implantación de patch panels de alta densidad con gestión inteligente del cableado.
- Reorganización de rutas de cable para optimizar el flujo de aire y reducir la carga térmica.
- Actualización a conectividad 25G, 100G y 400G para soportar las necesidades de ancho de banda de workloads modernos.

Sistemas de seguridad física y lógica

La modernización de la seguridad en un data center no puede limitarse al plano IT. La seguridad perimetral, el control de acceso y la detección de incendios son subsistemas que deben actualizarse en paralelo con el resto de la infraestructura.

- Sistemas de control de acceso biométrico y por tarjeta de proximidad con registro de auditoría.
- CCTV de alta resolución con retención de imágenes conforme a normativa.
- Sistemas de detección precoz de incendios (VESDA) y supresión por agentes limpios.

La disponibilidad como activo crítico

En la economía digital, la disponibilidad de la información no es una característica deseable: es un requisito operativo fundamental. Los sistemas de negocio, ERP, CRM, plataformas de comercio electrónico, sistemas bancarios, servicios de salud, dependen de la disponibilidad continua de datos para funcionar. Cuando el acceso a la información se interrumpe, el impacto se produce de forma inmediata y en cascada.

El coste real del tiempo de inactividad

Las cifras asociadas al downtime de data centers ponen en perspectiva la importancia crítica de la disponibilidad y, por tanto, la relevancia de abordar los proyectos de retrofitting con la máxima garantía de continuidad:

>$500K
coste por hora para grandes empresas

$1.5 Tr
de Fortune 500 pierden por downtime anual

Según el Oxford Economics Study, el coste promedio del downtime para una empresa de tamaño medio asciende a 9.000 dólares por minuto o 540.000 dólares por hora.

Para empresas de gran escala en sectores críticos como banca, salud o comercio electrónico, el impacto puede superar los 5 millones de dólares por hora cuando se contabilizan los costes directos, el daño reputacional, las penalizaciones por SLA y el impacto en la cotización.

Los cinco niveles de impacto del downtime

1 Impacto económico directo

Pérdida de ingresos por transacciones no completadas, costes de recuperación, penalizaciones contractuales por incumplimiento de SLAs y horas extras del equipo técnico dedicadas a la restauración del servicio.

2 Impacto reputacional

La confianza de clientes, partners e inversores se erosiona con cada incidente de disponibilidad. En sectores regulados, los reportes de incidentes son públicos y tienen consecuencias directas sobre la percepción de la marca.

3 Impacto en la continuidad operativa

Los procesos de negocio que dependen de sistemas IT se paralizan, generando efectos en cascada que se extienden más allá del tiempo de inactividad técnico. El tiempo necesario para restaurar el estado operativo completo siempre supera el tiempo de inactividad registrado.

4 Impacto regulatorio y de cumplimiento

En sectores regulados (finanzas, salud, infraestructuras críticas), un incidente de disponibilidad puede desencadenar investigaciones regulatorias, multas y la obligación de implementar medidas correctoras bajo supervisión.

5 Impacto en la seguridad

Los incidentes de disponibilidad provocados por ciberataques (ransomware, DDoS) combinan la pérdida de servicio con la exposición de datos, multiplicando el impacto total.

La disponibilidad no es negociable

El estándar TIER IV del Uptime Institute garantiza una disponibilidad del 99,9995% (menos de 26 minutos de inactividad al año). Un data center no modernizado difícilmente puede aspirar a estos niveles de disponibilidad, poniendo en riesgo los compromisos de SLA con clientes y el cumplimiento normativo.

Disponibilidad durante el propio proceso de retrofitting

Uno de los paradojas centrales del retrofitting es que la modernización de un data center debe realizarse sin interrumpir los servicios que este alberga. Esto convierte el proyecto en una operación de alta precisión que requiere:

- Planificación exhaustiva de ventanas de mantenimiento y procedimientos de corte controlado.
- Redundancia transitoria: implementación de capacidad de respaldo temporal antes de intervenir sobre los sistemas primarios.
- Commissioning progresivo: validación de cada nuevo sistema antes de transferir cargas desde el sistema antiguo.
- Procedimientos de rollback: planes documentados para revertir intervenciones en caso de comportamiento inesperado.
- Monitorización intensificada durante todo el período de ejecución del proyecto.

Principales riesgos de un proyecto de retrofitting

El retrofitting es, por definición, un proyecto de alto riesgo. Trabajar sobre una infraestructura en producción, con servicios críticos activos, introduce una complejidad que no existe en los proyectos de nueva construcción. La identificación, evaluación y mitigación de riesgos es el factor diferencial entre un proyecto exitoso y un incidente grave.

Riesgo 1: Pérdida de disponibilidad durante la intervención

El principal riesgo de un proyecto de retrofitting es la interrupción no planificada del servicio. Este riesgo se materializa cuando:

- Una intervención sobre un sistema que se creía aislado afecta a otros sistemas en producción.
- El tiempo de una ventana de mantenimiento se sobrepasa sin haber completado el trabajo previsto.
- Un nuevo sistema instalado presenta un fallo durante el período de burn-in.
- Un procedimiento de conmutación no se ejecuta según lo planificado.

Mitigación: diseño de una arquitectura de ejecución por fases con redundancia transitoria garantizada en cada paso. Simulacros de las operaciones más críticas en entornos de prueba o en réplicas de la infraestructura antes de ejecutar en producción.

Riesgo 2: Incompatibilidad entre sistemas nuevos y existentes

La integración de nuevos equipos en una infraestructura existente puede generar incompatibilidades que no son evidentes en la fase de diseño. Los protocolos de comunicación de los nuevos sistemas de monitorización pueden no ser compatibles con los sistemas de gestión existentes, las especificaciones eléctricas pueden no coincidir exactamente, o los nuevos sistemas de refrigeración pueden generar dinámicas de flujo de aire inesperadas.

Mitigación: auditoría técnica exhaustiva previa al diseño, con levantamiento detallado de todos los sistemas existentes. Uso de análisis CFD (Computational Fluid Dynamics) para simular el comportamiento térmico del data center tras las modificaciones previstas.

Riesgo 3: Riesgos asociados a la refrigeración líquida

La implementación de sistemas de refrigeración líquida, necesaria para densidades alta, introduce riesgos específicos que no existen en sistemas de refrigeración por aire. Las fugas de líquido refrigerante en proximidad de equipos eléctricos son potencialmente catastróficas.

- Compatibilidad de materiales: no todos los materiales de las instalaciones existentes son compatibles con los agentes refrigerantes utilizados en los nuevos sistemas.
- Gestión del condensado: los sistemas de refrigeración líquida generan condensación que debe ser gestionada adecuadamente.
- Monitorización de fugas: es imprescindible implementar sistemas de detección de fugas en todos los puntos de conexión.
- Mantenimiento preventivo: los sistemas de refrigeración líquida requieren protocolos de mantenimiento más rigurosos que los sistemas de aire.

Alerta: fugas en cooling líquido

Durante 2025 se documentaron incidentes de parada de clusters causados por fallos en la gestión de refrigeración líquida. Muchos sistemas fueron instalados sin considerar plenamente la compatibilidad de materiales, los protocolos de monitorización y los procedimientos de mantenimiento preventivo.

Riesgo 4: Escasez de personal especializado

La demanda de profesionales especializados en infraestructuras de data center supera con creces la oferta disponible. La ejecución de un proyecto de retrofitting complejo requiere perfiles con experiencia específica en cada uno de los sistemas intervenidos, lo que limita la disponibilidad de equipos capaces de asumir proyectos de esta magnitud con las garantías necesarias.

Mitigación: planificación anticipada del proyecto con suficiente tiempo para identificar y comprometer a los equipos técnicos adecuados. Definición clara de las responsabilidades de cada proveedor y establecimiento de mecanismos de coordinación entre ellos.

Riesgo 5: Riesgos en cascada

Los incidentes en data centers raramente son consecuencia de un único fallo. Los escenarios de mayor impacto suelen ser el resultado de fallos en cadena: un fallo de red que retrasa la respuesta a una alerta, combinado con una vulnerabilidad en un sistema de control de climatización, que deriva en una parada de emergencia. Este tipo de incidentes son los más difíciles de prevenir y los más costosos en términos de tiempo de recuperación.

- Análisis de árbol de fallos (FTA) y FMEA (Failure Mode and Effects Analysis) para identificar escenarios de fallo en cascada antes del inicio de las obras.
- Implementación de sistemas de monitorización con detección de anomalías para identificar patrones de fallo emergentes.
- Segmentación de la red de gestión para limitar el radio de impacto de incidentes de ciberseguridad.

Riesgo 6: Gestión del conocimiento y documentación

Uno de los riesgos menos visibles, pero más frecuentes, en los proyectos de retrofitting es la falta de documentación actualizada de la infraestructura existente. La ausencia de planos as-built actualizados, de inventarios de activos precisos o de procedimientos operativos documentados puede convertir una intervención rutinaria en una operación de alto riesgo.

La información sobre la infraestructura es en sí misma un activo crítico: sin datos precisos sobre qué hay instalado, cómo está configurado y de qué depende cada sistema, es imposible planificar con seguridad ninguna intervención. Antes de iniciar cualquier proyecto de retrofitting, es imprescindible realizar un levantamiento exhaustivo del estado actual.

Metodología y buenas prácticas

La diferencia entre un proyecto de retrofitting exitoso y uno que genera incidentes reside en la metodología de ejecución. Una planificación rigurosa, el uso de herramientas de análisis avanzadas y la experiencia de los equipos son los factores determinantes del resultado.

Fase 1: Auditoría y assessment previo

Ningún proyecto de retrofitting debe iniciarse sin un levantamiento exhaustivo del estado actual de la infraestructura. Esta fase incluye:

1. Inventario completo de activos: catalogación de todos los equipos con su modelo, antigüedad, estado de soporte del fabricante y capacidad remanente.
2. Análisis de consumo energético: medición del PUE actual e identificación de los principales focos de ineficiencia.

3. Evaluación de la infraestructura eléctrica: análisis de la capacidad de distribución, la calidad de la potencia y el estado de los sistemas de protección.
4. Assesment de la infraestructura de refrigeración: análisis térmico del CPD para identificar puntos calientes y evaluar la capacidad de los sistemas de climatización.
5. Revisión de la documentación existente: verificación de la actualidad y precisión de los planos, diagramas y procedimientos.
6. Análisis de riesgos: evaluación de la criticidad de cada sistema y de los escenarios de fallo potenciales.

Fase 2: Información confiable como base del análisis

Antes de modelar o diseñar cualquier intervención, es imprescindible contar con datos precisos y actualizados del estado real de la infraestructura. Aquí es donde un sistema DCiM (Data Center Infrastructure Management) se convierte en una herramienta central: no solo registra el inventario de activos, sino que correlaciona en tiempo real datos de consumo eléctrico, temperatura, capacidad de rack y carga de los sistemas de climatización.

Sin esta base de información confiable, cualquier análisis posterior parte de suposiciones. Con ella, es posible identificar con precisión qué sistemas están operando cerca de sus límites, dónde se concentra el riesgo térmico y qué capacidad real queda disponible antes de la intervención.

Fase 3: Diseño del plan de ejecución por fases

La clave para mantener la disponibilidad durante un retrofitting es la ejecución por fases. Cada fase debe:

- Estar claramente delimitada en alcance, tiempo y recursos.
- Comenzar con el despliegue de capacidad de respaldo antes de intervenir sobre los sistemas primarios.

- Incluir criterios de aceptación definidos (pruebas de validación) antes de proceder a la siguiente fase.
- Contar con un procedimiento de rollback documentado y probado.
- Definir el equipo responsable de la monitorización continua durante la intervención.

Fase 4: Commissioning y validación

El commissioning, el proceso de verificación y validación de que todos los sistemas instalados funcionan correctamente, tanto de forma individual como en conjunto, es la garantía final de que el retrofitting ha sido exitoso. Un commissioning riguroso incluye:

- Pruebas de los sistemas individualmente (Factory Acceptance Test y Site Acceptance Test).
- Pruebas de integración entre sistemas (eléctrico, climatización, seguridad, monitorización).
- Pruebas de escenarios de fallo: simulación de los fallos más críticos para verificar que los sistemas de protección actúan según lo previsto.
- Documentación as-built: actualización de todos los planos y documentos técnicos para reflejar el estado real de la infraestructura tras la modernización.

Aquí de nuevo el DCiM juega un papel fundamental.

Normativas y certificaciones

Un proyecto de retrofitting bien ejecutado es una oportunidad para alinear la infraestructura del data center con los estándares internacionales más exigentes. La obtención de certificaciones reconocidas no solo valida la calidad de la modernización, sino que representa un activo diferencial de cara a clientes, socios e inversores.

El estándar TIER del Uptime Institute

El sistema de clasificación TIER del Uptime Institute es el estándar de referencia global para la evaluación de la disponibilidad y la redundancia de los data centers:

Nivel	Característica clave	Disponibilidad	Downtime máx.
TIER I	Infraestructura básica	99,671%	28,8 h/año
TIER II	Componentes redundantes	99,741%	22,0 h/año
TIER III	Mantenimiento concurrente	99,982%	1,6 h/año
TIER IV	Tolerante a fallos	99,9995%	0,4 h/año

ISO/IEC 27001 — seguridad de la información

La norma ISO/IEC 27001 establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). Un data center modernizado debe demostrar que la seguridad de la información está integrada en todos sus procesos operativos, incluyendo los físicos. La certificación ISO 27001 es exigida cada vez más frecuentemente por clientes de sectores regulados como condición de contratación.

EN 50600 — estándar europeo para data centers

La familia de normas EN 50600 (equivalente a ISO/IEC 22237) establece los requisitos técnicos y operativos para la infraestructura de data centers en Europa, incluyendo los sistemas eléctricos, de climatización, de telecomunicaciones y de seguridad. Es la referencia normativa principal para cualquier proyecto de construcción o modernización de CPD en el ámbito europeo.

BICSI — estándares de infraestructura de telecomunicaciones

Los estándares BICSI (Building Industry Consulting Service International), en particular el ANSI/BICSI 002 para data centers, son la referencia para el diseño e instalación de la infraestructura de cableado y conectividad. La certificación BICSI de los instaladores garantiza que el cableado estructurado se ejecuta conforme a las mejores prácticas del sector.

El Data Center del futuro sostenibilidad y IA

El retrofitting no es solo una respuesta a las necesidades del presente: es la palanca para posicionar el data center ante los desafíos del futuro. La sostenibilidad y la inteligencia artificial son los dos vectores que definirán la evolución de los centros de datos en los próximos años.

Hacia el Data Center Net Zero

El concepto de data center Net Zero hace referencia a instalaciones capaces de compensar su huella de carbono mediante eficiencia energética, energías renovables y reducción de emisiones.

El retrofitting es, además, una práctica sostenible, ya que reutiliza y optimiza infraestructuras existentes, evitando el impacto ambiental asociado a nuevas construcciones.

- Instalación de sistemas de energías renovables on-site (paneles solares en cubierta, acuerdos de compra de energía renovable PPA).
- Recuperación de calor residual: el calor generado por los equipos IT puede aprovecharse para calefacción de edificios adyacentes o procesos industriales.
- Sistemas de almacenamiento de energía (BESS) para optimizar el consumo y mejorar la resiliencia ante interrupciones del suministro eléctrico.
- Certificaciones de sostenibilidad: LEED, BREEAM, EU Green Deal, declaraciones de impacto ambiental.

IA climate management: la gestión climática inteligente

Una de las innovaciones más transformadoras en la gestión de data centers modernos es la aplicación de inteligencia artificial al control de los sistemas de climatización. Los sistemas de IA Climate Management analizan en tiempo real miles de variables, temperatura de entrada y salida de aire, carga de los servidores, temperatura exterior, consumo de los sistemas de refrigeración, para optimizar de forma continua el funcionamiento de los sistemas de climatización.

A diferencia de los sistemas de control tradicionales, que reaccionan a los problemas una vez que se han producido, los sistemas basados en IA son predictivos: anticipan la aparición de puntos calientes antes de que se produzcan y ajustan proactivamente los parámetros de funcionamiento para evitarlos. Esto permite reducir el consumo energético de la climatización entre un 10% y un 30% adicional respecto a los sistemas de control convencionales, al tiempo que se mejora la fiabilidad del sistema.

Edge Computing y la descentralización del procesamiento

La proliferación del edge computing, el procesamiento de datos en ubicaciones próximas al punto donde se generan, en lugar de centralizarlo en grandes data centers, está transformando la arquitectura de la infraestructura IT. El retrofitting de instalaciones existentes es especialmente relevante en este contexto: pequeños CPDs de empresa o instalaciones de colocation pueden modernizarse para convertirse en nodos de una arquitectura distribuida, sin necesidad de construir nuevas instalaciones desde cero.

Conclusión: El retrofitting como decisión estratégica

El retrofitting de data centers no es un proyecto de mantenimiento: es una decisión estratégica de negocio con implicaciones que van mucho más allá del ámbito técnico. La modernización de la infraestructura de datos es una condición necesaria para la competitividad de cualquier organización que dependa de la disponibilidad, el rendimiento y la seguridad de sus sistemas de información.

Hemos visto a lo largo de esta guía que los desafíos son significativos: trabajar sobre una instalación en producción, gestionar la complejidad de múltiples sistemas interdependientes, mitigar el riesgo de interrupciones de servicio y garantizar la continuidad de los SLAs comprometidos con los clientes. Pero también hemos visto que estos desafíos son manejables con la metodología adecuada, los equipos correctos y las herramientas apropiadas.

Las organizaciones que acometan sus proyectos de retrofitting de forma planificada, con una auditoría previa rigurosa, un diseño basado en análisis, una ejecución por fases con redundancia garantizada y un commissioning exhaustivo, no solo mitigarán los riesgos inherentes al proceso, sino que emergerán de él con una infraestructura más eficiente, más resiliente y mejor posicionada para afrontar los retos tecnológicos de los próximos años.

La información siempre debe estar disponible. Los datos son el activo más valioso de la economía digital. Proteger ese activo comienza por modernizar la infraestructura sobre la que descansa.

Algunas de las referencias de los datos utilizados:

>40% de los DC tienen limitaciones eléctricas críticas https://www.orbit.es/retos-modernizacion-data-center-y-soluciones-inaplazables/

40% de la energía consume la climatización en CPDs tradicionales https://dconceptgroup.com/que-es-el-retrofitting-data-center-guia-completa-para-la-modernizacion-de-infraestructuras/

PUE 1.8–2.2 1.2–1.4 / ahorro 15–40% https://blogespanol.se.com/centros-de-datos/2022/02/04/cual-es-la-viabilidad-de-tu-data-center-consejos-de-modernizacion-para-una-infraestructura-de-data-center-agil/

Coste downtime $9.000/min / $540.000/hora (Oxford Economics) https://heunets.com/the-hidden-costs-of-data-center-downtime-what-you-need-to-know/

>90% de grandes empresas: 1h downtime cuesta >$300K / 41% entre $1M–$5M/hora https://thenetworkinstallers.com/blog/cost-of-it-downtime-statistics/

Fortune 500 pierde $1,5 billones anuales por downtime https://bladeroom.com/the-true-cost-of-downtime-for-data-centres/

Disponibilidad TIER I–IV (Uptime Institute) https://uptimeinstitute.com/tiers