

Dónde y cómo opera un data center

Selección del site, análisis de riesgos y operaciones confiables: los fundamentos que determinan la resiliencia real de una instalación crítica



Introducción

Un data center puede tener el mejor diseño técnico del mercado y aun así fallar sistemáticamente si está ubicado en el lugar equivocado o si sus operaciones no están a la altura de su infraestructura. La ubicación del site y la calidad de las operaciones son dos variables que los equipos técnicos tienden a dar por resueltas, cuando en realidad son las que más frecuentemente determinan la resiliencia real de una instalación crítica.

Este e-book aborda estas dos dimensiones desde una perspectiva operativa. La primera parte analiza los criterios de selección de site y el mapa de riesgos que todo profesional debe conocer antes de decidir dónde construir o dónde ubicar sus sistemas. La segunda parte cubre el modelo de operaciones confiables: el ciclo de vida del DC, la estructura organizativa, los procedimientos y las herramientas de gestión que transforman una infraestructura en una operación fiable.

EN ESTE EBOOK

Lo que encontrarás en este e-book

Los 8 factores clave de selección de site

- Taxonomía completa de desastres naturales y antrópicos
- Cómo leer un índice de riesgo
- Ciclo de vida del DC y ventanas de renovación
- Estructura organizativa de operaciones
- SOP, MOP y EOP: los tres tipos de procedimiento
- ITIL, CMMS, DCIM y BAS: las herramientas de gestión
- Documentación mínima obligatoria
- Programa de formación por perfil

01CAPÍTULO

La ubicación del site

La decisión más permanente

De todas las decisiones que se toman en el ciclo de vida de un data center, la elección de la ubicación es probablemente la más difícil de revertir. Un sistema de refrigeración se puede modernizar, un UPS se puede sustituir, pero cambiar la ubicación física de un data center es una operación de tal complejidad que en la práctica equivale a construir uno nuevo.

Por eso el análisis de site debe ser exhaustivo, sistemático y documentado antes de tomar cualquier decisión de inversión. Existen ocho factores principales que deben evaluarse.

1.1 Los ocho factores de selección de site

Factor	Qué evaluar	Riesgo si se ignora
Acceso a energía eléctrica	Fiabilidad del proveedor, redundancia de circuitos y rutas de alimentación independientes desde subestaciones distintas	Dependencia de una única fuente; sin fallback ante corte prolongado
Acceso a telecomunicaciones	Disponibilidad de múltiples operadores y rutas físicas de fibra diversificadas	Punto único de falla en conectividad; sin alternativa ante corte de fibra
Adyacencias de propiedades	Instalaciones industriales, militares, químicas o de alto riesgo en el entorno inmediato	Exposición a incendios, explosiones o contaminación de fuentes externas

Factor	Qué evaluar	Riesgo si se ignora
Estabilidad sísmica y del subsuelo	Tipo de suelo, actividad sísmica histórica, proximidad a fallas geológicas	Daño estructural ante sismo; colapso de infraestructura del edificio
Llanura de inundación	Historial de inundaciones, cota del terreno, proximidad a ríos o costa	Inundación catastrófica sin posibilidad de respuesta operativa
Calidad del aire	Concentración de partículas, gases industriales, actividad volcánica o urbana próxima	Contaminación acelerada del hardware; corrosión prematura de circuitos
Acceso al agua	Disponibilidad para sistemas de refrigeración (Chiller, torres) y extinción de incendios	Limitación en tecnologías de enfriamiento; riesgo en caso de incendio
Acceso al transporte	Mínimo dos vías de acceso independientes desde arteria principal	Imposibilidad de acceso del personal o equipos en emergencia

■ 1.2 El acceso a energía: el factor más crítico

De los ocho factores, el acceso a energía eléctrica de calidad es el que más condiciona la viabilidad del proyecto. La evaluación debe ir más allá de confirmar que existe suministro eléctrico en la zona: debe analizar la fiabilidad histórica del proveedor, la posibilidad de alimentar el site desde dos subestaciones diferentes mediante rutas físicamente separadas, y la disponibilidad de tensión en media o alta tensión que permita reducir la dependencia de transformaciones intermedias.

Redundancia de alimentación eléctrica

CLAVE

La mejor práctica es disponer de dos alimentaciones desde subestaciones eléctricas diferentes, con rutas físicas completamente separadas (incluyendo canalizaciones subterráneas distintas). Un site alimentado desde dos puntos de la misma subestación no tiene redundancia real: un fallo en la subestación afecta a ambas alimentaciones simultáneamente.

2

Para recordar

subestaciones distintas, con rutas físicas separadas: la única forma de tener redundancia eléctrica real.

02CAPÍTULO

El mapa de riesgos

Conocer para anticipar

La selección de site no puede hacerse sin un análisis sistemático de los riesgos asociados a la ubicación. Estos riesgos se dividen en dos grandes categorías: desastres naturales y desastres antrópicos (causados por la actividad humana). Ambas categorías pueden actuar de forma independiente o encadenada, y ambas tienen el potencial de comprometer definitivamente la operación de un data center.

■ 2.1 Taxonomía de desastres naturales

Categoría	Tipos	Impacto típico en DC
Desastres geológicos	Terremotos, erupciones volcánicas, corrimientos de tierra	Daño estructural del edificio, corte de servicios, contaminación por cenizas volcánicas
Desastres hidrológicos	Inundaciones, tsunamis, erupciones límnicas	Inundación de instalaciones, corte de acceso, daño irreversible de equipos
Desastres climáticos	Huracanes, tornados, olas de calor, sequías, tormentas severas	Corte de energía prolongado, daño físico del edificio, fallo de sistemas de enfriamiento
Incendios naturales	Incendios forestales, fulminaciones	Daño estructural, contaminación por humo, corte de acceso
Clima espacial	Tormentas geomagnéticas solares	Interferencias electromagnéticas, daño a sistemas eléctricos no protegidos

■ 2.2 Desastres antrópicos: la amenaza que se construye cerca

Los desastres antrópicos son especialmente relevantes porque muchos de ellos son identificables y evitables en la fase de selección de site. Un data center ubicado junto a una instalación química industrial, en el cono de aproximación de un aeropuerto o a menos de 100 metros de una autopista de alta densidad de tráfico de mercancías peligrosas está asumiendo riesgos que ningún sistema de redundancia interno puede compensar.

Los peligros antrópicos se dividen en dos grupos:

- **Peligros sociológicos:** terrorismo, crimen organizado, disturbios civiles, conflictos armados. Determinan los requisitos de seguridad física y el nivel de exposición pública del site.
- **Peligros tecnológicos:** instalaciones industriales de alto riesgo, bases militares, almacenamiento de materiales peligrosos, rutas de transporte de sustancias inflamables o explosivas, proximidad a pistas de aviación.

El riesgo de las adyacencias

ATENCIÓN

Un caso real documentado en el manual muestra un data center con múltiples riesgos simultáneos en un radio reducido: autopista a menos de 100 metros, zona industrial de alto riesgo, cono de aproximación de pista de aviación y almacenamiento de municiones de una base de la fuerza aérea. Ninguno de estos riesgos es visible en un análisis exclusivamente técnico del edificio. Solo un análisis geográfico y de adyacencias los revela.

■ 2.3 Índices de riesgo como herramienta de decisión

Existen índices de riesgo públicos que cuantifican de forma sistemática la exposición de cada territorio a desastres naturales y antrópicos. El índice INFORM (Index for Risk Management), desarrollado por la ONU y la Unión Europea, es uno de los más completos y está disponible públicamente.

Estos índices permiten comparar ubicaciones potenciales de forma objetiva y documentar la decisión de site con criterios trazables. Para un data center de misión crítica, la consulta de índices de riesgo no es opcional: es parte del proceso de due diligence del proyecto.

Los desastres naturales se encadenan

CLAVE

Una característica frecuentemente subestimada es que los desastres naturales pueden encadenarse: un terremoto puede generar un tsunami; una sequía puede causar incendios forestales que a su vez degraden la calidad del aire. El análisis de riesgos debe considerar estos escenarios compuestos, no solo los eventos individuales.

<100 m

Para recordar
de una autopista con mercancías peligrosas: un riesgo que ninguna redundancia interna puede compensar.

03 CAPÍTULO

El ciclo de vida del data center

Planificar para décadas, renovar cada pocos años

Un data center estratégico está diseñado para operar entre 20 y 30 años. En ese periodo, los sistemas de cableado duran entre 15 y 25 años, pero los servidores y sistemas de almacenamiento se renuevan cada 3 a 5 años. Esta asimetría es fundamental para entender cómo debe gestionarse un data center a lo largo del tiempo.

3.1 Vida útil por capa de infraestructura

Capa	Vida útil típica	Implicación operativa
Data center estratégico (edificio e infraestructura)	20 – 30 años	Las decisiones de diseño tienen un impacto de décadas. Los errores de site o de capacidad son muy costosos de corregir
Sistema de cableado estructurado	15 – 25 años	Debe planificarse para soportar múltiples generaciones de equipos TI. La capacidad del cableado debe anticipar densidades futuras
Servidores y sistemas de almacenamiento	3 – 5 años	El ciclo de refresh de TI es continuo. La infraestructura debe poder absorber cambios de densidad y configuración sin obras mayores
PCs de escritorio	3 – 5 años	Impacto limitado en la infraestructura del DC directamente
Portátiles	2 – 3 años	Impacto limitado en la infraestructura del DC directamente

■ 3.2 El ciclo de renovación cada 5 años

Cada 5 años aproximadamente, un data center bien gestionado debe pasar por un ciclo de revisión y renovación que puede incluir desde la actualización de equipos TI hasta la sustitución de sistemas de infraestructura (UPS, CRAC/ CRAH, switchgear). Aproximadamente cada 15 años, puede ser necesaria una renovación mayor que implique reemplazos significativos de sistemas y posiblemente una actualización de la arquitectura.

Este ciclo de vida tiene una implicación directa en la planificación presupuestaria: un data center que no tiene un plan de renovación documentado está acumulando deuda técnica que en algún momento se materializará como un fallo o como una obsolescencia que compromete la capacidad de escalar.

Las fases del ciclo de vida

CLAVE

~90%
de la vida de
un data center
transcurre en
operaciones

1

Planificación

2

Diseño

3

Construcción

4

Puesta en marcha (commissioning)

5

Operación continua

- Refresh de TI cada 3-5 años
- Renovación mayor cada 15 años

04CAPÍTULO

Operaciones confiables

El triángulo que sostiene la disponibilidad

Las operaciones de un data center se sostienen sobre tres pilares interdependientes: el personal, los procedimientos y la documentación. La gestión integra y supervisa estos tres elementos. Ninguno de los tres puede compensar las deficiencias de los otros dos: un equipo excelente sin procedimientos genera inconsistencias; unos procedimientos perfectos sin personal formado son papel mojado.

■ 4.1 Estructura organizativa de operaciones

La organización de operaciones de un data center se estructura en dos ramas principales bajo la dirección de IT Operations:

Rama	Función	Subáreas
Facility Management	Gestión de la infraestructura física del DC	Engineering (edificio, eléctrico, mecánico) + Maintenance (edificio, eléctrico, mecánico)
IT Management	Gestión de los sistemas de información y telecomunicaciones	IT Infrastructure (Telco/Networking, Computing/Storage, Disaster Recovery) + Technical Support (Call Center)

Adicionalmente, existen funciones de soporte que son externas a la cadena de mando directa pero imprescindibles para las operaciones: el CISO (responsable de ciberseguridad), el equipo de Seguridad física y el equipo de Health & Safety. Estas funciones deben estar formalmente integradas en los procesos operativos, no tratarse como entidades independientes.

■ **4.2 Los tres tipos de procedimiento: SOP, MOP y EOP**

Uno de los conceptos más importantes en la gestión de operaciones de un data center es la distinción entre los tres tipos de procedimientos. Confundirlos o usarlos de forma intercambiable es uno de los errores más frecuentes en equipos de operaciones sin formación formal.

Tipo	Nombre completo	Propósito	Cuándo se usa
SOP	Standard Operating Procedure (Procedimiento Operacional Estándar)	Define una rutina recurrente y procesos críticos. Puede ser funcional o administrativo	Operaciones rutinarias: rondas de inspección, apertura/cierre de sala, recepción de equipos, gestión de visitantes
MOP	Method of Procedure (Método de Procedimiento)	Procedimiento detallado paso a paso para una intervención específica. Más detallado que el SOP	Intervenciones técnicas planificadas: sustitución de UPS, mantenimiento de CRAC, modificación de configuración eléctrica
EOP	Emergency Operating Procedure (Procedimiento de Operación de Emergencia)	Procedimiento para un modo de fallo potencial o fallo conocido	Emergencias: fallo de UPS, activación del sistema contra incendios, corte de energía no planificado, activación de EPO

El EOP que no se practica no funciona

ATENCIÓN

Un EOP es inútil si el personal no lo ha practicado antes de que ocurra la emergencia. Los EOPs deben incluir simulacros periódicos (drills) con toda la plantilla operativa, incluyendo escenarios de fallo de UPS, incendio en sala y activación accidental de EPO. La frecuencia recomendada es al menos una vez al año por escenario.

■ **4.3 Herramientas de gestión operativa**

Las operaciones de un data center moderno requieren herramientas específicas para gestionar el flujo de trabajo de procedimientos, el seguimiento de activos y el control de los sistemas de infraestructura. Existen cuatro categorías principales:

Herramienta	Nombre completo	Función principal
ITIL	Information Technology Infrastructure Library	Marco de buenas prácticas para la gestión del cambio de activos, el nivel de prestación del servicio y el registro de incidentes con sus causas y consecuencias
CMMS	Computerized Maintenance Management System	Programación, asignación y seguimiento de todas las actividades de mantenimiento de las instalaciones. Calcula KPIs de gestión de mantenimiento (MTBF, MTTR)
DCIM	Data Center Infrastructure Management	Maximiza el uso eficiente de las capacidades de energía, refrigeración y espacio. Proporciona visibilidad en tiempo real de toda la infraestructura del DC

Herramienta	Nombre completo	Función principal
BAS	Building Automation System	Software que permite controlar los sistemas del edificio de forma automatizada (HVAC, iluminación, acceso, seguridad)
DMS	Document Management System	Almacenamiento, recuperación y flujo de aprobación de toda la documentación del DC

DCIM: la herramienta que lo ve todo

CLAVE

El DCIM es la herramienta con mayor impacto operativo en un data center moderno. Integra datos de energía, refrigeración, espacio y activos en una única plataforma, permitiendo tomar decisiones informadas sobre capacidad, eficiencia y planificación. Un DC sin DCIM opera parcialmente a ciegas: puede gestionar los sistemas individualmente, pero no tiene visibilidad del comportamiento integrado de la infraestructura.



Para recordar
simulacro al año, como mínimo, por cada escenario de emergencia.

05 CAPÍTULO

Documentación y formación

La memoria institucional del DC

La documentación de un data center no es un requisito burocrático: es la memoria institucional que permite que las operaciones sean consistentes, auditables y transferibles. Un data center que opera sin documentación actualizada está en riesgo permanente de que el conocimiento crítico resida exclusivamente en las personas, no en los sistemas.

5.1 Documentación mínima obligatoria

El sistema documental de un data center debe mantener registro actualizado de los siguientes elementos:

- **Dibujos as-built:** planos actualizados que reflejan el estado real de la instalación, no el diseño original.
- **Base de datos de activos:** inventario completo de todos los equipos con sus características técnicas, fechas de instalación y garantías.
- **Alcance del trabajo de mantenimiento preventivo:** descripción detallada de todas las tareas de mantenimiento planificadas.
- **Programa de mantenimiento:** calendario de todas las intervenciones preventivas con asignación de responsables.
- **Normas de trabajo en instalaciones críticas:** reglas de seguridad y procedimientos específicos para trabajar en entornos energizados o de alta disponibilidad.

- **Programa de seguridad:** políticas y procedimientos de seguridad física y ciberseguridad.
- **Lista de verificación de commissioning:** checklist de puesta en marcha para cada sistema.
- **Procedimientos y procesos:** biblioteca completa de SOPs, MOPs y EOPs.
- **Informes:** registros históricos de incidentes, mantenimientos y auditorías.

El documento más peligroso

ATENCIÓN

El plano as-built desactualizado es uno de los documentos más peligrosos en un data center. Cuando el personal interviene sobre un sistema basándose en un plano que no refleja la realidad, el riesgo de error es máximo. Mantener los as-built actualizados después de cada modificación no es opcional: es una obligación operativa.

5.2 Programa de formación por perfil

La formación del personal debe ser diferenciada según el perfil y las responsabilidades de cada rol. El manual distingue dos niveles principales:

Perfil	Contenidos de formación
Técnicos e ingenieros de campo	• Fundamentos y mejores prácticas • Teoría de operación de los equipos y sistemas principales • Módulos de formación para SOPs y MOPs • Simulacros para EOPs • Exámenes por nivel de formación
Managers y supervisores (adicionalmente)	• Data Center Management • Data Center Energy Efficiency • Data Center Operations • Data Center Design Awareness • Formación continua y asistencia a conferencias del sector

La formación no es un evento puntual en la incorporación: es un proceso continuo. Los cambios en la infraestructura, la incorporación de nuevos sistemas, las actualizaciones normativas y las lecciones aprendidas de incidentes deben traducirse en actualizaciones de los programas de formación.

Conclusión

La resiliencia empieza antes de poner el primer rack

Un data center resiliente no se construye solo con tecnología redundante. Se construye eligiendo el lugar correcto, conociendo los riesgos del entorno, estableciendo operaciones estructuradas y documentando cada decisión. Estas son las disciplinas que los equipos técnicos más frecuentemente subestiman y que más frecuentemente determinan el resultado real.

La ubicación del site es permanente. Las operaciones son continuas. La documentación es acumulativa. Ninguna de las tres puede improvisarse en el momento de la emergencia: deben estar en su lugar mucho antes de que ocurra cualquier evento no planificado.

CLAVE

Los cinco principios del DC bien ubicado y bien operado

1. La selección de site requiere análisis de ocho factores físicos y un mapa de riesgos naturales y antrópicos. Una ubicación con múltiples riesgos simultáneos no puede ser compensada por redundancia interna.
2. Los desastres naturales se encadenan. El análisis de riesgos debe contemplar escenarios compuestos, no solo eventos individuales.
3. SOP, MOP y EOP son tres documentos distintos con propósitos distintos. Confundirlos es un riesgo operativo.
4. Un EOP que no se practica no funciona. Los simulacros son obligatorios, no opcionales.
5. Los planos as-built desactualizados son tan peligrosos como un sistema sin redundancia. La documentación debe reflejar el estado real, no el diseño original.