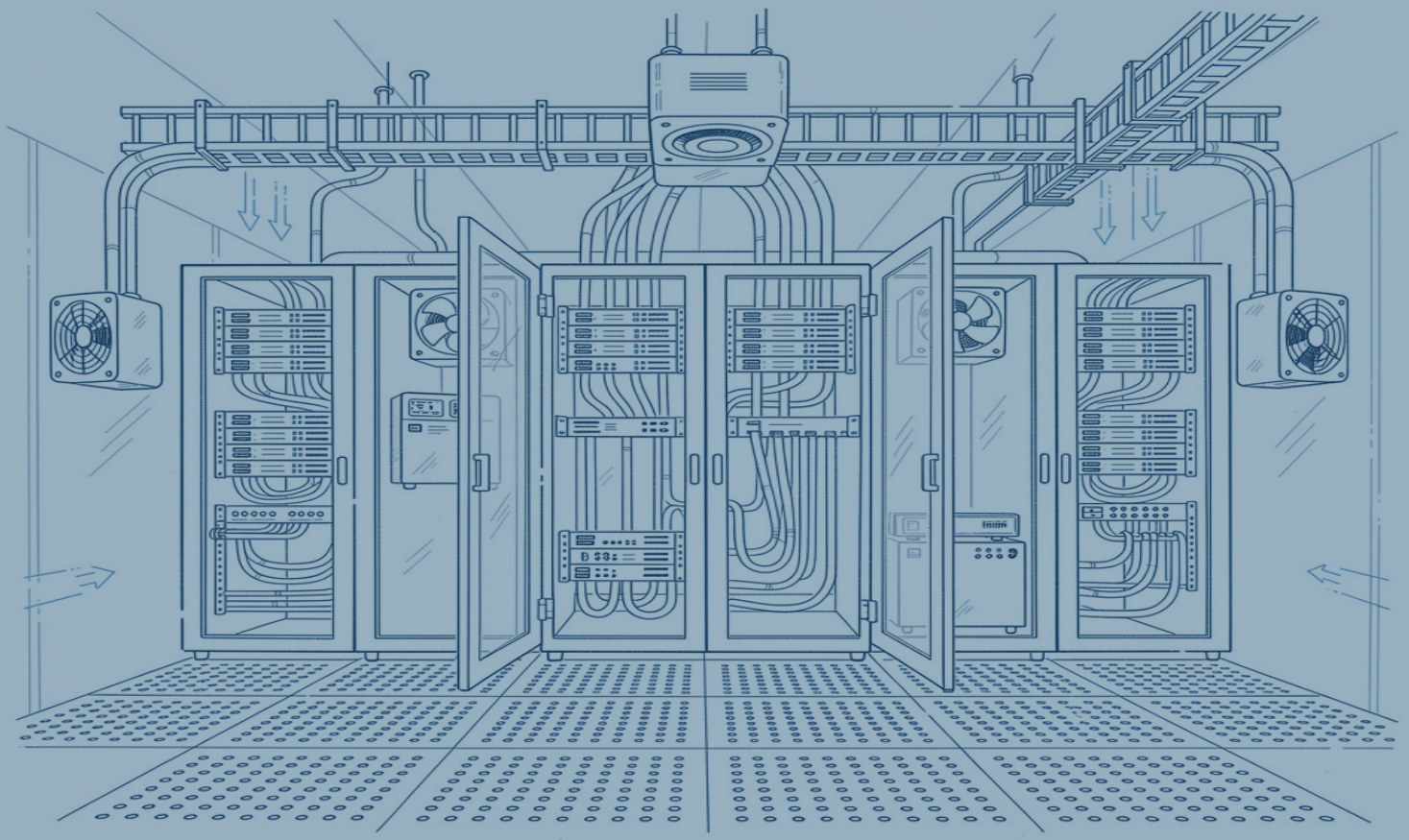
Bjumper

Retrofitting in Data Centers

Modernizing Critical Infrastructure Without Compromising Availability



Introduction

Data infrastructure is the nervous system of any modern organization. Every transaction, every critical business process, and every communication depends on data being available, secure, and accessible in real time. In this context, data centers (DCs) are no longer simple server rooms: they are top-tier strategic assets.

However, the reality is that a large portion of data centers currently in operation were designed more than a decade ago, when technological demands, workloads, and efficiency requirements were radically different. The emergence of artificial intelligence, edge computing, hybrid cloud services, and the explosion of data have turned these infrastructures into potential bottlenecks for business growth.

Retrofitting, the modernization of an existing data center without the need to build a completely new facility from scratch, emerges as the strategic and economically viable response to this challenge. This ebook provides a comprehensive technical guide on what a retrofitting project entails, why information availability is a critical non-negotiable asset, what the main associated risks are, and how to mitigate them successfully.

Who Is This Guide For?

This document is intended for IT infrastructure managers, system administrators, data center architects, and operations engineers who are facing decisions regarding the modernization of their data centers or who need to understand the technical and strategic scope of a retrofitting process.

Bjumper

What Is Retrofitting in Data Centers?

Definition and Concept

The term retrofitting comes from English and refers to the process of updating, improving, or modernizing the components of an existing installation in order to extend its useful life, improve its performance, and adapt it to new requirements without the need to build a new infrastructure from scratch..

Applied to the world of data centers, **retrofitting involves the partial or total renovation of critical systems**: electrical, cooling, connectivity, and security systems, while the facility remains operational. This aspect is precisely what defines the complexity and criticality of the process: work is carried out on a “live installation,” where any mistake can result in service loss.

Retrofitting vs. Greenfield: Two Different Approaches

It is important to differentiate retrofitting from a greenfield project (building a completely new data center from scratch):

Criteria	Retrofitting	Greenfield
Initial investment	Moderate	Very high
Execution time	Weeks or months	12–24 months
Operational risk	High (live installation)	Low
Service continuity	Critical during the process	Not applicable
Design flexibility	Limited by the existing structure	Total
Environmental impact	Low (reuse)	High (new construction)
Ideal for...	Optimizing existing assets	New capacities and locations

When Is It Time to Retrofit?

There are unmistakable signs that a data center has reached the limit of its operational life cycle without upgrades:

- Cooling systems are unable to maintain safe operating temperatures under current load densities.
- PUE (Power Usage Effectiveness) exceeds 1.8, indicating poor energy efficiency.
- Uninterruptible Power Supply (UPS) systems are more than 10 years old and are no longer supported by the manufacturer.
- The electrical infrastructure cannot handle loads above 5 kW/rack, while the market demands densities of 10–30+ kW/rack for AI workloads.
- Incident response times increase due to the difficulty of obtaining spare parts for obsolete components.
- The data center does not comply with current regulations regarding security, energy efficiency, or data protection.

Key Data

According to recent industry studies, more than 40% of operational data centers have significant limitations in their electrical distribution systems, increasing the risk of critical failures and reducing their ability to adapt to new workloads.

The Current Context: Why Retrofitting Is Urgent

The data center sector is undergoing an unprecedented transformation. Demand for processing capacity is growing at rates that no new construction project alone can satisfy, making retrofitting not just an option, but a strategic necessity.

The Explosion of Data and Artificial Intelligence

The massive adoption of generative AI, machine learning, and big data has dramatically increased power density in data centers. While a traditional facility operates at 3–5 kW/rack, AI workloads require between 10 and 30 kW/rack, and the most advanced environments exceed 100 kW/rack.

This evolution means that many data centers designed just a decade ago require major electrical and cooling upgrades to support new demands.

Land and Energy Scarcity Accelerate Retrofitting

In Europe's main data center hubs (Madrid, Frankfurt, Amsterdam, London, Dublin), the availability of land with access to sufficient electrical power is becoming increasingly limited. In addition, the timelines for permits, grid connection, and construction of new facilities usually exceed 24–36 months.

Given this reality, retrofitting existing facilities allows capacity expansion in strategic locations with significantly shorter execution timelines, leveraging already established network infrastructure and access points.

Regulatory and ESG Pressure

European regulations on energy efficiency (EN 50600, Energy Efficiency Directive, Net Zero regulations) require data center operators to progressively improve their sustainability indicators.

A high PUE or the use of obsolete cooling systems not only generates higher operational costs, but may also become a regulatory and reputational obstacle.

A well-executed retrofitting project not only modernizes technical infrastructure: it also opens the door to obtaining TIER certifications and sustainability labels that increase the value of the asset.

>40%

data centers have critical electrical limitations.

40%

of energy consumption in traditional data centers.

Critical Areas of Intervention

A retrofitting project encompasses multiple technical disciplines that must be addressed in a coordinated manner. Modernizing one system in isolation, without considering its interdependencies with the rest of the infrastructure, may create new problems or shift the bottleneck elsewhere in the system.

Cooling Systems and Thermal Control

Cooling is one of the most critical and costly subsystems in a data center. In traditional facilities, air-based HVAC (Heating, Ventilation, and Air Conditioning) systems are not capable of handling the power densities required by modern workloads.

Applicable Modernization Technologies:

Direct Liquid Cooling (DLC)	Transfers the heat generated by processors directly through water or dielectric fluids, eliminating the need to move large volumes of air. Essential for densities above 20 kW/rack.
In-row cooling	Cooling units integrated directly into rack aisles, reducing the distance between the heat source and the extraction point.
Free cooling	Uses outside air under favorable climate conditions to reduce the energy consumption of mechanical cooling systems.
IA Climate Management	AI-based climate control systems that predict and prevent hot spots before they occur, optimizing energy consumption in real time.

Impact on PUE

Upgrading cooling systems can reduce PUE from typical values of 1.8–2.2 in legacy facilities to 1.2–1.4 in modernized environments, representing energy savings of between 15% and 40% annually.

Electrical Infrastructure and UPS Systems

The reliability of the power supply is the cornerstone of data center availability. A failure in the power system has no possible technical solution if the electrical infrastructure lacks adequate redundancy.

Key Elements in Electrical Modernization

Replacement of Obsolete UPS Systems:

Conventional UPS systems (online double-conversion technology with IGBT replaced by next-generation models with higher efficiency (>98% in ECO mode) and improved battery management.

PDU (Power Distribution Unit) Upgrades:

Smart distribution units enable real-time rack-level consumption monitoring and early anomaly detection.

Low-Voltage Switchboard Modernization:

Adaptation of distribution capacity to support the higher load densities required.

Backup Generators:

Review and upgrade of generator sets to guarantee autonomy and startup capacity within the timeframe established by SLAs.

Redundant Electrical Distribution Architecture (2N, N+1):

Design of the electrical distribution network to eliminate single points of failure in the power chain.

Cabling and Connectivity

Connectivity is the vascular system of the data center. Disorganized cabling or obsolete technologies not only limit network performance but also create airflow resistance that directly impacts the thermal efficiency of the facility.

- Migration to high-density fiber optics (OS2, OM5) for high-speed backbone infrastructure
- Deployment of high-density patch panels with intelligent cable management.
- Reorganization of cable routes to optimize airflow and reduce thermal load.
- Upgrade to 25G, 100G, and 400G connectivity to support modern workload bandwidth requirements.

Physical and Logical Security Systems

Modernizing security in a data center cannot be limited to the IT layer alone. Perimeter security, access control, and fire detection systems are subsystems that must be upgraded in parallel with the rest of the infrastructure.

- Biometric and proximity-card access control systems with audit logging.
- High-resolution CCTV systems with image retention compliant with regulations.
- Early fire detection systems (VESDA) and clean-agent suppression systems..

Availability as a Critical Asset

In the digital economy, information availability is not a desirable feature: it is a fundamental operational requirement. Business systems, ERP platforms, CRM solutions, e-commerce platforms, banking systems, and healthcare services all depend on continuous data availability to function.When access to information is interrupted, the impact is immediate and cascading.

The Real Cost of Downtime

The figures associated with data center downtime put the critical importance of availability into perspective and therefore highlight the importance of carrying out retrofitting projects with the highest guarantees of continuity:

>$500K
Cost per hour for large enterprises

$1.5 Tr
Fortune 500 companies lose annually due to downtime

According to the Oxford Economics Study, the average downtime cost for a medium-sized company amounts to $9,000 per minute or $540,000 per hour.

For large-scale enterprises in critical sectors such as banking, healthcare, or e-commerce, the impact can exceed $5 million per hour when direct costs, reputational damage, SLA penalties, and stock market impact are considered.

The Five Levels of Downtime Impact

1 Direct Financial Impact

Loss of revenue due to incomplete transactions, recovery costs, contractual SLA penalties, and overtime hours for technical teams dedicated to service restoration.

2 Reputational Impact

The trust of customers, partners, and investors erodes with every availability incident. In regulated industries, incident reports are public and directly affect brand perception.

3 Operational Continuity Impact

Business processes dependent on IT systems are paralyzed, creating cascading effects that extend beyond the technical downtime itself.
The time required to restore full operational status always exceeds the recorded downtime.

4 Regulatory and Compliance Impact

In regulated sectors (finance, healthcare, critical infrastructure), an availability incident may trigger regulatory investigations, fines, and mandatory corrective measures under supervision.

5 Security Impact

Availability incidents caused by cyberattacks (ransomware, DDoS) combine service disruption with data exposure, multiplying the total impact.

Availability Is Non-Negotiable

The Uptime Institute's TIER IV standard guarantees 99.9995% availability (less than 26 minutes of downtime per year).
A non-modernized data center can hardly aspire to achieve these levels of availability, putting customer SLA commitments and regulatory compliance at risk.

Availability During the Retrofitting Process Itself

One of the central paradoxes of retrofitting is that a data center must be modernized without interrupting the services it hosts. This turns the project into a high-precision operation requiring:

- Exhaustive planning of maintenance windows and controlled shutdown procedures.
- Temporary redundancy: deployment of backup capacity before intervening in primary systems.
- Progressive commissioning: validation of each new system before migrating loads from the legacy system.
- Rollback procedures: documented plans to reverse interventions in case of unexpected behavior.
- Enhanced monitoring throughout the entire execution period of the project.

Main Risks of a Retrofitting Project

Retrofitting is, by definition, a high-risk project. Working on a production infrastructure with active critical services introduces complexity that does not exist in new-build projects.
The identification, evaluation, and mitigation of risks are the key differentiators between a successful project and a major incident.

Risk 1: Loss of Availability During Intervention

The primary risk of a retrofitting project is unplanned service interruption.
This risk materializes when:

- An intervention on a supposedly isolated system affects other production systems.
- A maintenance window exceeds the allocated time without completing the planned work..
- A newly installed system fails during the burn-in period.
- A switching procedure is not executed as planned.

Mitigation: Design a phased execution architecture with guaranteed temporary redundancy at every step. Conduct simulations of the most critical operations in test environments or infrastructure replicas before executing them in production.

Risk 2: Incompatibility Between New and Existing Systems

Integrating new equipment into existing infrastructure can generate incompatibilities that are not evident during the design phase.
The communication protocols of new monitoring systems may not be compatible with existing management systems, electrical specifications may not match exactly, or new cooling systems may create unexpected airflow dynamics.

Mitigation: Conduct an exhaustive technical audit before design, including detailed mapping of all existing systems.
Use CFD (Computational Fluid Dynamics) analysis to simulate thermal behavior after the planned modifications.

Risk 3: Risks Associated with Liquid Cooling

The implementation of liquid cooling systems, necessary for high-density environments, introduces specific risks that do not exist in air-cooling systems. Coolant leaks near electrical equipment can be potentially catastrophic.

- Material compatibility: not all materials in existing installations are compatible with the cooling agents used in new systems.
- Condensation management: liquid cooling systems generate condensation that must be properly managed.
- Leak monitoring: leak detection systems must be implemented at all connection points.
- Preventive maintenance: liquid cooling systems require stricter maintenance protocols than air systems.

Warning: Liquid Cooling Leaks

During 2025, cluster shutdown incidents caused by failures in liquid cooling management were documented.
Many systems were installed without fully considering material compatibility, monitoring protocols, and preventive maintenance procedures

Risk 4: Shortage of Specialized Personnel

Demand for professionals specialized in data center infrastructure far exceeds the available supply.
Executing a complex retrofitting project requires profiles with specific expertise in each system involved, limiting the availability of teams capable of handling projects of this magnitude with the necessary guarantees.

Mitigation: Plan projects sufficiently in advance to identify and secure the appropriate technical teams.
Clearly define the responsibilities of each supplier and establish coordination mechanisms among them.

Risk 5: Cascading Risks

Incidents in data centers are rarely caused by a single failure.
The highest-impact scenarios are usually the result of cascading failures: a network failure that delays the response to an alert combined with a vulnerability in a climate control system that results in an emergency shutdown.
These types of incidents are the most difficult to prevent and the most expensive in terms of recovery time.

- Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) to identify cascading failure scenarios before work begins.
- Implementation of monitoring systems with anomaly detection to identify emerging failure patterns.
- Segmentation of the management network to limit the impact radius of cybersecurity incidents.

Risk 6: Knowledge Management and Documentation

One of the least visible but most common risks in retrofitting projects is the lack of updated documentation for the existing infrastructure.
The absence of updated as-built drawings, accurate asset inventories, or documented operating procedures can turn a routine intervention into a high-risk operation.

Information about infrastructure is itself a critical asset: without accurate data about what is installed, how it is configured, and what each system depends on, it is impossible to safely plan any intervention.
Before starting any retrofitting project, it is essential to carry out a comprehensive assessment of the current state.

Methodology and Best Practices

The difference between a successful retrofitting project and one that generates incidents lies in the execution methodology.

Rigorous planning, the use of advanced analysis tools, and the experience of the teams involved are the determining factors of the outcome.

Phase 1: Audit and Preliminary Assessment

No retrofitting project should begin without a comprehensive assessment of the current infrastructure state.This phase includes:

1. Complete asset inventory: cataloging all equipment with model, age, manufacturer support status, and remaining capacity.
2. Energy consumption analysis: measurement of current PUE and identification of major inefficiency points.

3. Electrical infrastructure evaluation: analysis of distribution capacity, power quality, and protection system status.
4. Cooling infrastructure assessment: thermal analysis of the data center to identify hotspots and evaluate cooling system capacity.
5. Review of existing documentation: verification of the accuracy and relevance of diagrams, drawings, and procedures.
6. Risk analysis: evaluation of the criticality of each system and potential failure scenarios.

Phase 2: Reliable Information as the Basis for Analysis

Before modeling or designing any intervention, it is essential to have accurate and updated information about the actual condition of the infrastructure.
This is where a DCIM (Data Center Infrastructure Management) system becomes a central tool: it not only records the asset inventory but also correlates real-time data on electrical consumption, temperature, rack capacity, and cooling system load.

Without this reliable information base, any subsequent analysis starts from assumptions.
With it, it becomes possible to precisely identify which systems are operating near their limits, where thermal risk is concentrated, and what actual capacity remains available before intervention.

Phase 3: Designing the Phased Execution Plan

The key to maintaining availability during retrofitting is phased execution.
Each phase must:

- Have clearly defined scope, timeline, and resources.
- Begin with the deployment of backup capacity before intervening in primary systems.

- Include defined acceptance criteria (validation tests) before proceeding to the next phase.
- Include a documented and tested rollback procedure.
- Define the team responsible for continuous monitoring during the intervention.

Phase 4: Commissioning and Validation

Commissioning, the process of verifying and validating that all installed systems operate correctly both individually and together, is the final guarantee that retrofitting has been successful.
Rigorous commissioning includes:

- Individual system testing (Factory Acceptance Test and Site Acceptance Test).
- Integration testing among systems (electrical, cooling, security, monitoring).
- Failure scenario testing: simulation of the most critical failures to verify that protection systems respond as expected.
- As-built documentation: updating all plans and technical documents to reflect the actual state of the infrastructure after modernization.

Here again, DCIM plays a fundamental role.

Standards and Certifications

A properly executed retrofitting project is an opportunity to align data center infrastructure with the most demanding international standards.

Obtaining recognized certifications not only validates the quality of modernization but also represents a differentiating asset for customers, partners, and investors.

Uptime Institute TIER Standard

The Uptime Institute's TIER classification system is the global reference standard for evaluating data center availability and redundancy.

Level	Key Characteristic	Availability	Max Downtime
TIER I	Basic infrastructure	99,671%	28,8 h/year
TIER II	Redundant components	99,741%	22,0 h/year
TIER III	Concurrent maintainability	99,982%	1,6 h/year
TIER IV	Fault tolerant	99,9995%	0,4 h/year

ISO/IEC 27001 — Information Security

The ISO/IEC 27001 standard establishes the requirements for an Information Security Management System (ISMS).
A modernized data center must demonstrate that information security is integrated into all operational processes, including physical security.
ISO 27001 certification is increasingly required by customers in regulated industries as a prerequisite for contracting services.

EN 50600 — European Standard for Data Centers

The EN 50600 family of standards (equivalent to ISO/IEC 22237) establishes technical and operational requirements for data center infrastructure in Europe, including electrical, cooling, telecommunications, and security systems.
It is the primary regulatory reference for any data center construction or modernization project within Europe.

BICSI — Telecommunications Infrastructure Standards

BICSI standards (Building Industry Consulting Service International), particularly ANSI/BICSI 002 for data centers, are the reference for the design and installation of cabling and connectivity infrastructure.
BICSI certification for installers guarantees that structured cabling is implemented according to industry best practices.

The Data Center of the Future: Sustainability and AI

Retrofitting is not only a response to present-day needs: it is the lever that positions the data center for future challenges.

Sustainability and artificial intelligence are the two forces that will define the evolution of data centers in the coming years.

Toward the Net Zero Data Center

The Net Zero data center concept refers to facilities capable of offsetting their carbon footprint through energy efficiency, renewable energy, and emissions reduction.

Retrofitting is also a sustainable practice because it reuses and optimizes existing infrastructure, avoiding the environmental impact associated with new construction.

- Installation of on-site renewable energy systems (rooftop solar panels, renewable energy PPAs)
- Waste heat recovery: heat generated by IT equipment can be reused for heating nearby buildings or industrial processes.
- Battery Energy Storage Systems (BESS) to optimize energy consumption and improve resilience during power interruptions.
- Sustainability certifications: LEED, BREEAM, EU Green Deal, environmental impact declarations..

AI Climate Management: Intelligent Climate Control

One of the most transformative innovations in modern data center management is the application of artificial intelligence to cooling system control.
AI Climate Management systems analyze thousands of variables in real time — inlet and outlet air temperature, server load, outside temperature, cooling system consumption — to continuously optimize cooling system operation.

Unlike traditional control systems, which react after problems occur, AI-based systems are predictive: they anticipate the emergence of hotspots before they occur and proactively adjust operating parameters to prevent them.
This enables an additional 10% to 30% reduction in cooling energy consumption compared to conventional control systems while improving overall system reliability.

Edge Computing and Processing Decentralization

The rise of edge computing — processing data closer to where it is generated instead of centralizing it in large data centers — is transforming IT infrastructure architecture.
Retrofitting existing facilities is especially relevant in this context: small enterprise data centers or colocation facilities can be modernized to become nodes within a distributed architecture, without the need to build entirely new facilities.

Conclusion: Retrofitting as a Strategic Decision

Data center retrofitting is not a maintenance project: it is a strategic business decision with implications far beyond the technical sphere.

Modernizing data infrastructure is a necessary condition for the competitiveness of any organization that depends on the availability, performance, and security of its information systems.

Throughout this guide, we have seen that the challenges are significant: working on a live production facility, managing the complexity of multiple interdependent systems, mitigating the risk of service interruptions, and guaranteeing continuity of customer SLAs.But we have also seen that these challenges are manageable with the right methodology, the right teams, and the right tools.

Organizations that undertake their retrofitting projects with proper planning, rigorous preliminary audits, analysis-based design, phased execution with guaranteed redundancy, and exhaustive commissioning will not only mitigate the inherent risks of the process but will emerge with infrastructure that is more efficient, more resilient, and better positioned to face the technological challenges of the coming years.

Information must always remain available. Data is the most valuable asset in the digital economy. Protecting that asset begins with modernizing the infrastructure on which it depends.

References Used in the Document

40% of data centers have critical electrical limitations: https://www.orbit.es/retos-modernizacion-data-center-y-soluciones-inaplazables/
Cooling systems consume 40% of energy in traditional data centers: https://dconceptgroup.com/que-es-el-retrofitting-data-center-guia-completa-para-la-modernizacion-de-infraestructuras/
PUE reduction from 1.8–2.2 to 1.2–1.4 / 15–40% savings 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/
Downtime cost: $9,000/minute / $540,000/hour (Oxford Economics) https://heunets.com/the-hidden-costs-of-data-center-downtime-what-you-need-to-know/
90% of large companies 1h downtime cuesta >$300K / 41% entre $1M–$5M/hora https://thenetworkinstallers.com/blog/cost-of-it-downtime-statistics/
Fortune 500 loses $1.5 trillion annually due to downtime https://bladeroom.com/the-true-cost-of-downtime-for-data-centres/
TIER I–IV availability (Uptime Institute) https://uptimeinstitute.com/tiers