CASO DE ÉXITO

CASA BATLLÓ

Casa Batlló evoluciona su infraestructura de red con una arquitectura de alta capacidad y seguridad Zero Trust.

Casa Batlló

Casa Batlló es uno de los referentes arquitectónicos y culturales más emblemáticos de Barcelona. Obra de Antoni Gaudí y declarada Patrimonio Mundial por la UNESCO, el edificio recibe cada año a millones de visitantes y combina la conservación de un entorno histórico único con una apuesta constante por la innovación tecnológica y la excelencia operativa.

La gestión tecnológica de un entorno de estas características requiere una infraestructura de red robusta, segura y preparada para soportar servicios críticos, conectividad de alta densidad y una operativa continua.

Con este objetivo, Casa Batlló impulsó un proyecto de modernización integral de su infraestructura de red y ciberseguridad para evolucionar hacia una arquitectura más resiliente, escalable y alineada con los actuales requisitos de seguridad y rendimiento.

El reto

Modernizar una infraestructura crítica sin comprometer la operativa del edificio

Casa Batlló se enfrentaba a la necesidad de modernizar su infraestructura tecnológica para dar respuesta a un crecimiento de demanda en conectividad, seguridad y capacidad de gestión de red.
El entorno existente presentaba diversas limitaciones que condicionaban su evolución:

- Arquitectura de **seguridad perimetral** basada en firewall sin capacidades avanzadas de inspección y protección frente a amenazas actuales.
- Acceso remoto basado en **VPN tradicional**, sin control contextual ni segmentación granular por usuario o recurso.
- **Core de red** con limitaciones de escalabilidad y rendimiento, dificultando el crecimiento de los servicios corporativos.
- **Electrónica de acceso** heterogénea y obsoleta, con falta de estandarización tecnológica.
- **Backbone entre armarios** con enlaces de 1 Gbps, limitando la transmisión de tráfico interno.

El objetivo del proyecto era claro: diseñar una infraestructura segura, escalable, redundada y preparada para el crecimiento futuro, tanto en capacidad como en seguridad perimetral y segmentación de red

La solución

Arquitectura integral de red, seguridad y conectividad de nueva generación

Desde INSTEL se ha diseñado e implantado una arquitectura integral basada en tres capas: seguridad, core y acceso, junto con una modernización completa del backbone de comunicaciones.

Seguridad perimetral y acceso Zero Trust

Se ha implantado una plataforma de ciberseguridad basada en firewalls de nueva generación Fortinet FortiGate 200G en configuración de alta disponibilidad (HA), proporcionando:

- **Inspección avanzada de tráfico** en capa 7 (NGFW).
- **Servicios de seguridad integrados**: IPS, antivirus, web filtering, control de aplicaciones y protección frente a amenazas avanzadas.
- **Arquitectura redundante** para garantizar disponibilidad del servicio.

Como evolución clave del modelo de acceso remoto, se ha sustituido la VPN tradicional por una **arquitectura ZTNA (Zero Trust Network Access):**

- Acceso basado en identidad y contexto.
- Conexión bajo demanda exclusivamente al recurso solicitado.
- Eliminación de túneles VPN permanentes.
- Gestión centralizada mediante agente cloud.

Este modelo reduce significativamente la superficie de ataque y refuerza el control sobre usuarios, dispositivos y aplicaciones.

La solución

Arquitectura integral de red, seguridad y conectividad de nueva generación

Infraestructura física: backbone de alta capacidad sobre fibra OM5

Se ha renovado la infraestructura de cableado estructurado, implantando una arquitectura basada en:

- **Fibra óptica OM5 de CommScope** para la red corporativa.
- Mantenimiento de **OM4 para entornos audiovisuales** específicos.
- Despliegue de subsistemas verticales y horizontales de fibra de alta densidad.
- Conectividad mediante **trunks MPO de alta capacidad**.
- Interconexión entre armarios evolucionada de **1 Gbps a 20 Gbps**.

Esta actualización elimina cuellos de botella y prepara la infraestructura para futuros crecimientos de demanda.

"Uno de los cambios más relevantes ha sido la evolución del modelo de acceso remoto hacia una arquitectura Zero Trust basada en ZTNA. Pasamos de un entorno con VPN tradicional a un modelo mucho más seguro, donde el acceso a los recursos se realiza de forma dinámica y controlada. Esto, junto con la renovación del core y la electrónica de red, nos permite trabajar con una infraestructura mucho más robusta, preparada para el futuro."

Miquel Palma, Head of IT Systems and Infraestructure en Casa Batlló

La solución

Arquitectura integral de red, seguridad y conectividad de nueva generación

Electrónica de red: estandarización y salto de rendimiento

El núcleo de red ha sido completamente renovado mediante la implantación de una arquitectura homogénea basada en HPE Aruba:

- Sustitución del core legacy por **dos switches Aruba CX 8325 redundados** en alta disponibilidad mediante **tecnología VSX.**
- **Interconexión entre equipos core** con una capacidad de **200 Gbps.**
- Posibilidad de **interconexión de cabinas** de almacenamiento a **velocidades de 1/10/25/50/100 Gb.**

En la **capa de agregación** se han desplegado equipos Aruba 8300 CX, permitiendo:

- Conectividad de servidores a 10 Gbps.
- Redundancia avanzada en servicios corporativos.
- Eliminación de cuellos de botella en agregación de tráfico.

En la **capa de acceso** se ha estandarizado la electrónica con switches HPE Aruba 6200M, aportando:

- Mayor capacidad por puerto.
- Gestión centralizada de red.
- Escalabilidad y homogeneización de la infraestructura.

Beneficios

Infraestructura y rendimiento

- Multiplicación por 10 de la capacidad del backbone (de 2 Gbps a 20 Gbps), eliminando cuellos de botella entre armarios.
- Core de red redundado, garantizando alta disponibilidad y continuidad del servicio
- Conectividad de servidores evolucionada hasta 10 Gbps, frente a entornos anteriores de 1–2 Gbps.
- Infraestructura preparada para servicios de alta demanda, incluyendo almacenamiento y comunicaciones críticas.

Seguridad y acceso

- Evolución del acceso remoto hacia un modelo de Zero Trust (ZTNA), eliminando VPNs persistentes y habilitando acceso bajo demanda por recurso.
- Implantación de NGFW con inspección avanzada en capa 7, reforzando la protección frente a amenazas.
- Mayor visibilidad y control sobre usuarios, dispositivos y aplicaciones.

Operaciones y explotación

- Reducción de incidencias relacionadas con saturación o limitaciones de red.
- Mayor resiliencia gracias a la alta disponibilidad en core y seguridad.
- Simplificación de la administración mediante centralización de la infraestructura.
- Escalabilidad sin necesidad de rediseños estructurales.

www.instel.es

Galileu, 288. 08028 Barcelona
934099191 - instel@instel.es