Data Center: estudio y diseño

ESTUDIO TÉCNICO PARA EL DESPLIEGUE DE UN CENTRO DE DATOS EN PARAGUAY (RG-T2785-P004)

NETWORLD CONSULTING
ICT & TELECOM REGULATORY CONSULTING

Junio 2018

Índice

Índice de figuras **3**
1 Resumen Ejecutivo **5**
2 Introducción **8**
3 Statu quo de los Centros de Datos **10**
3.1 Infraestructura actual: centros de datos y planes inmediatos previstos *10*
3.2 Benchmark. Ubicación de Centros de Datos en otros países *11*
3.3 Benchmark. Estándares para la compatibilidad de la tecnología de los centros de datos con la normativa ecológica *18*
3.4 Estándares de clasificación de los Centros de Datos *22*
4 Recomendación de ubicaciones de los Centros de Datos **44**
4.1 Amenazas exteriores *45*
5 Propuesta del Centro de Datos **50**
5.1 Exteriores *52*
5.2 Obra civil- Solución estructural *55*
5.3 Solución potencia *73*
5.4 Solución refrigeración *92*
5.5 Sistemas adicionales *99*
5.6 Descripción de las fases de la solución propuesta *110*
5.7 Gestión del proyecto *113*
5.8 Certificación del proyecto *115*
6 Partidas del proyecto **117**
7 Análisis económico y financiero. Cronograma **136**
7.1 Inventario de las inversiones a realizar acorde con el estudio técnico *136*
7.2 Cálculo de los gastos operativos en los primeros 5 años *142*
8 Definición de los principales hitos y metas **143**
9 Conclusiones y recomendaciones **144**
Anexo I – Propuesta de capacitación sobre el Estudio técnico **145**
Anexo II – Detalle Equipamiento IT **155**
Anexo III – Detalle Costos operativos **170**
Anexo IV - Recomendación de los estándares para la compatibilidad con la normativa ecológica y legal **175**
Acrónimos **177**
Bibliografía **178**

Índice de figuras

Figura 1 Centros de Datos en Sudamérica. 10
Figura 2 Centros de Datos en Paraguay (detalle de la imagen anterior) 11
Figura 3 Centros de datos en LAC 12
Figura 4 Distribución de ingresos anuales por servicio de colocation por regiones. 17
Figura 5 A grandes rasgos la mitad de la energía la consume el equipamiento TIC y la otra mitad los sistemas de soporte (alimentación y refrigeración) 18
Figura 6 Este tipo de métricas nos van a permitir conocer cómo evoluciona a eficiencia de nuestro Centro de Datos en el tiempo. 20
Figura 7 Causas de apagado no planeado en Centros de Datos. 26
Figura 8 Perfil psicrométrico de Asunción 31
Figura 9 Comparación de agentes limpios en cuanto a Seguridad en humanos. 35
Figura 10 Epicentros de los últimos eventos sísmicos sentidos en Paraguay 46
Figura 11 Requisitos de la certificación TIER en Sostenibilidad Operativa 49
Figura 12 Puerta metálica corredera para acceso de vehículos 54
Figura 13 Características cerramiento LSR 18.6E 61
Figura 14 Ejemplo estructura de cerramiento 62
Figura 15 Componentes del pasamuros 62
Figura 16 Otras posibilidades de pasamuros 63
Figura 17 Compuerta cortafuegos 64
Figura 18 Ejemplo de estructura falso suelo 65
Figura 19 Ejemplo de cerramiento de pasillo 67
Figura 20 Descripción estructura del esquema unifilar 74
Figura 21 Detalle del esquema unifilar de la fase I 74
Figura 22 Detalle del esquema unifilar de la fase II 75
Figura 23 Esquema unifilar para ambas fases (I y II) 76
Figura 24 Ejemplo de Transformador 78
Figura 25 Ejemplo de solución para Grupo electrógeno 80

Figura 26 Diferencia entre distribución por PDU tradicional y Busbar 88
Figura 27 Ejemplo de PDU inteligente 89
Figura 28 Temperatura bulbo seco Asunción 93
Figura 29 Temperatura punto de rocío Asunción 93
Figura 30 Ejemplo de unidad de climatización basado en expansión directa 95
Figura 31 Ejemplo de cerramiento de pasillo caliente 97
Figura 32 Esquema del cableado de datos estructurado 106
Figura 33 CAPEX total para la implantación del centro de datos en Paraguay 137
Figura 34 CAPEX para los 5 primeros años 141
Figura 35 Estimación del OPEX para los 5 primeros años 142
Figura 36 Propuesta de capacitación 145
Figura 37 Propuesta de agenda tentativa para la socialización del proyecto 146
Figura 38 Equipo en el Centro de Datos 147
Figura 39 Servicios demandados en entorno Nube 2015 Global. 163
Figura 40 Tamaño y frecuencia de ataques DDoS a nivel mundial en función del tiempo 167
Figura 41 Enfoque Nube Access Security Broker. 168
Figura 42 Detalle del CAPEX del Equipamiento IT 169
Figura 43 Detalle OPEX - Costo energía 170
Figura 44 Detalle OPEX - Costo agua 170
Figura 45 Detalle OPEX - Costo gasoil 171
Figura 46 Equipo en el Centro de Datos 171
Figura 47 Detalle OPEX – Costos de interconexión de fibra óptica 173
Figura 48 Estimación del OPEX para los 5 primeros años 174
Figura 49 Referencia de normativas técnicas para un centro de datos 175
Figura 50 Referencia de estándares en un centro de datos 176
Figura 51 El futuro de las métricas de eficiencia del centro de datos. 176

1 Resumen Ejecutivo

Tal y como se explica y desarrolla dentro del documento, y tras analizar el contexto en el que nos encontramos, el cual debe ser siempre el factor que más se debe tener en cuenta para implementar de manera exitosa el ambicioso proyecto que nos ocupa, vamos a destacar los siguientes aspectos clave.

En el actual contexto en el que se mueve el mundo es fundamental no quedarse atrás en cuanto a los desarrollos y tendencias tecnológicas que hoy en día imperan, puesto que traen consigo gran parte de las oportunidades para el progreso de cualquier país.

La República del Paraguay tiene un gran reto por delante de cara a proveer a sus instituciones, empresas y ciudadanos, las herramientas tecnológicas que les permitan seguir avanzando, a la vez que les ayuden a ser competitivos en el mundo global en el que estamos.

A la hora de plantear la construcción de los nuevos Centro de Datos previstos por SENATICs debemos tener muy presente algunos aspectos fundamentales, de cara a que sea la solución más idónea para la fase en la que se encuentra el país.

Hoy en día la eficiencia energética y lo que ello conlleva en cuanto al menor impacto ambiental y el aprovechamiento adecuado de los recursos, nos hace tener muy presente que todos los equipamientos sean modulares, para crecer según vayamos necesitándolos, además de muy eficientes en su rendimiento y operación. Con estas premisas podremos controlar los costos de inversión y explotación.

En base a los requerimientos planteados y considerando la información recibida, se propone la creación de un Centro de Datos de forma modular, consiguiendo asegurar una inversión inicial menor y posibilidad de crecimiento futuro sin interrupción del servicio.

Los principales criterios que nos llevan a plantear una construcción modular de un Centro de Datos para este proyecto específico en Paraguay, frente a una construcción tradicional sobre el propio terreno son:

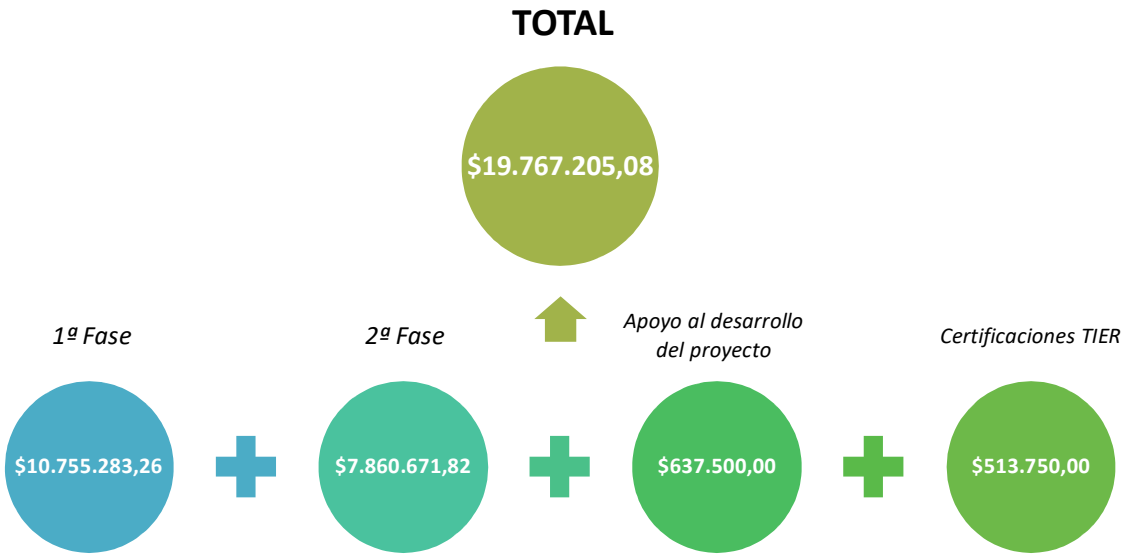
- Menor tiempo de construcción, con el consiguiente ahorro de costos.
- Reducimos el número de indefiniciones y detalles a solventar sobre la marcha en la fase de construcción, al estar todo estudiado y especificado de antemano, con las características y requerimientos solicitados. Lo que implica controlar los números de la inversión a realizar y evitar posibles sobrecostos por imprevistos.
- Facilita obtener la clasificación TIER III acordada por SENATICs para el nuevo Centro de Datos. Pudiendo conseguir con mayor garantía los certificados sobre el diseño y la construcción de los mismos, algo que siempre le va a garantizar un mayor valor y reconocimiento tanto nacional como internacional.
- La solución puede ser totalmente probada antes de ponerse en operación, y garantizar con ello el cumplimiento de los mejores y más exigentes estándares del mercado.

- Permite simular situaciones y condiciones extremas para testar el funcionamiento y operatividad del Centro de Datos antes de entrar en su fase de actividad normalizada. Con ello se evitan riesgos para el servicio y gana en reputación sobre las garantías que ofrecerán para los clientes que estén interesados en usar los servicios que se prestaran desde los mismos.
- Al poder involucrar a empresas muy especializadas, se conseguirá que expertos en las distintas materias y sistemas hagan la mejor instalación posible.
- Debemos tener presente que las instalaciones se diseñaran para trabajar de manera bastante automática y cuantas más pruebas se puedan hacer antes de ponerla en marcha mucho mejor, pues nos ofrecerá mayores garantías sobre la forma en la cual se comportará ante imprevistos.
- Todos los cableados y elementos auxiliares pueden ser probados de antemano, evitando los múltiples problemas que suelen aparecer durante las instalaciones in situ, y los consiguientes retrasos que luego, a su vez, generan prisas para entregar las obras, lo que trae consigo que algunas cosas se hagan con menos calidad, que no existan soluciones adecuadas ante ciertas coyunturas que se presentaran, etc.

Además, es muy importante tener presente:

- Considerar de manera preferente a los fabricantes de los distintos sistemas y equipamientos a emplear que tengan presencia en Paraguay. Esto permitirá, además de apoyar a las empresas que invierten en Paraguay y que generan puestos de trabajo y riqueza en el país, asegurar que durante la vida útil de dichos equipos podamos recibir el soporte adecuado, así como un costo razonable de componentes y repuestos.

Los costos que se plantean para la inversión a realizar en la construcción del centro de datos que será ubicado en Asunción, son los que se indican a continuación:



En la evaluación de los costos de inversión necesarios se han considerado todos los aspectos aportados y requeridos por SENATICs.

Una de las cuestiones fundamentales para garantizar el éxito de cualquier proyecto es tener los adecuados compañeros de viaje, para ello sugerimos poner especial cuidado a la hora de elegir **la empresa de ingeniería que apoye el desarrollo del proyecto así como la dirección facultativa durante la construcción**, **la empresa instaladora/constructora que lo ejecute** (la cual sugerimos sea una entidad muy especializada en la construcción e implementación de Centro de Datos), y **la empresa que realice todas las pruebas de puesta en marcha (commissioning) antes de comenzar con la operación** del centro de datos. A todas ellas se les debe pedir una dilatada experiencia en proyectos similares.

2 Introducción

El presente documento se enmarca en la cooperación técnica realizada entre la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), el Banco Interamericano de Desarrollo (BID) y la consultora NETWORLD CONSULTING. La componente desarrollada en este informe se centra en apoyar al Gobierno de Paraguay en el desarrollo de un Centro de Datos donde confluyan los servicios actuales y futuros de la SENATICs.

Se trata de una memoria descriptiva de la solución propuesta para el nuevo Centro de Datos que se va a desarrollar en Paraguay. Se describe la propuesta de diseño según las principales especificaciones definidas por SENATICs de lo que debería ser el futuro Centro de Datos. Las principales características del mismo serían:

- Topología Tier III
- Vida útil: 20 años
- Equipos IT:
    - 40 racks de 600x1000x42 U
    - 6 kW/rack de consumo medio
    - Máximo consumo de 10 kW/rack
    - Potencia total IT 240 kW
    - Capacidad de crecimiento de 40 racks adicionales
    - Futura potencia total IT: 480 kW
- Proyecto constructivo a desarrollar en 2 fases.

Este documento describe con el suficiente nivel de detalle para comprender el alcance de la propuesta. En el **primer capítulo** se ha incluido un resumen ejecutivo del documento y en este **segundo capítulo** la introducción al informe con la descripción de la estructura seguida.

En el **tercer capítulo** se presenta una visión global de los centros de datos a nivel internacional.

En el **cuarto capítulo** se recomiendan una serie de aspectos para la ubicación del centro de datos de acuerdo con las mejores prácticas internacionales.

En el **quinto capítulo** se expone la solución propuesta del centro de datos. Las principales partidas consideradas para el centro de procesamiento de datos son: i) Límites de diseño, ii) Solución estructural, iii) Solución potencia, iv) Solución refrigeración, v) Sistemas adicionales. Se describen los límites de diseño considerados en cuanto se refiere a dimensionamiento, normativa, estándares y buenas prácticas.

En el **sexto capítulo** se indican todas las partidas incluidas en la propuesta con una estimación de las necesidades de cada una de ellas.

En el **séptimo capítulo** se realiza el análisis económico para presentar el inventario de las inversiones a realizar acorde con este estudio técnico en los dos primeros años y un cálculo de los gastos operativos en los primeros cinco años.

En el **octavo capítulo** se definen los principales hitos y metas a cumplir durante la implementación del data center.

En el **noveno capítulo** se pretende finalizar con las principales conclusiones y recomendaciones.

Por último, antes de la sección de acrónimo y bibliografía con todas las normativas y estándares mencionados a lo largo del documento, **se anexan cuatro capítulos** con la propuesta para la capacitación sobre este estudio técnico para apoyar en la socialización de los resultados obtenidos; con un detalle de la propuesta de las partidas relativas al equipamiento IT; con un detalle de la propuesta de los costos operativos; y con la recomendación de los estándares para la compatibilidad de la normativa ecológica y legal.

3 Statu quo de los Centros de Datos

Este capítulo pretende ofrecer una visión global de los principales aspectos relacionados con los centros de datos a partir de referentes a nivel internacional. Se estudian:

- Infraestructura actual: centros de datos y planes inmediatos previstos en Sudamérica.
- Benchmark. Ubicación de centros de datos en otros países.
- Benchmark. Estándares para la compatibilidad de la tecnología de los centros de datos con la normativa ecológica.
- Estándares de clasificación de los centros de datos.

3.1 Infraestructura actual: centros de datos y planes inmediatos previstos

Si nos fijamos en los datos de las siguientes figuras podemos confirmar que el sector de los Centros de Datos (o Data Centers) se encuentra actualmente en una situación que permitirá un gran crecimiento a lo largo de los próximos años en Paraguay.

Figura 1 Centros de Datos en Sudamérica.

Fuente: Data Center Map

Figura 2 Centros de Datos en Paraguay (detalle de la imagen anterior)

Fuente: Data Center Map

La SENATICs tiene como objetivo desarrollar la infraestructura necesaria que permita disponer de un nuevo Centro de Datos ubicado en **Asunción**, para poder ofrecer a los distintos estamentos gubernamentales importantes y variados servicios, como los que actualmente ya prestan a distintos organismos.

3.2 Benchmark. Ubicación de Centros de Datos en otros países

Actualmente nos encontramos en un momento donde las principales empresas de Telecomunicaciones se están desprendiendo de sus Centros de Datos en propiedad, o al menos los segregan de sus matrices principales, para focalizarse en sus negocios de red. Esta tendencia demuestra que los actores van a estar diferenciados dejando a los que trabajan en el área de los Centro de Datos desarrollar su propia consolidación.

Aunque se trata de un dato que crece exponencialmente y de manera muy rápida, en la actualidad existen alrededor de 3700 centros de datos en el mundo situándose la mayoría en Estados Unidos (1500) y a continuación, a bastante distancia, Reino Unido (230), Alemania (170), Francia (140) y Canadá (130). El resto de países se encuentran todos por debajo de 100.

En el siguiente gráfico se muestran los centros de datos en los países del entorno de Paraguay:

Figura 3 Centros de datos en LAC

Fuente: Basado en el mapa de certificaciones de Uptime Institute

Perú		
Compañía	**Data Center**	**Localización**
BBVA	Perú CPD	Lima, Perú
GMD S.A.	GMD Cloud Data Center, Phase 1	Lima, Perú
SUNAT	Centro de Datos Lima	Lima, Perú
SUNAT	Centro de Datos Surco	Lima, Perú
Telefónica del Perú SAA	Data Center Lince CPD 1 & 2	Lima, Perú
Telefónica del Perú	Data Center Monterrico	Lima, Perú
Americatel	Data Center Olguin	Lima, Perú

Brasil		
Compañía	**Data Center**	**Localización**
Telefónica VIVO	Data Center Tambore	Sao Paulo, Brasil
Banco Santander Brasil S/A	Centro Tecnológico Campinas – DC2	Sao Paulo, Brasil
Banco Santander Brasil S/A	Centro Tecnológico Campinas – DC1	Sao Paulo, Brasil
Ascenty Data Centers Locação E Serviço LTDA	Ascenty DC Hortolândia, Phase 1	Hortolandia, Brasil
Governo do Estado do Parana	CELEPAR Data Center, Phase 1	Curitiba, Brasil
Globo.com	Globo.com Datacenter	Rio de Janeiro, Brasil
Grupo Petrópolis	Datacenter Alpha – Phase 1	Boituva, Sao Paulo, Brasil
EQUINIX Brasil	Site Tambore – SP2, Phase 3	Barueri, Sao Paulo, Brasil
Ascenty Data Centers Locação E Serviço LTDA	Ascenty DC Fortaleza	Fortaleza, Ceara, Brasil
Tribunal de Justiça do Estado do Espírito Santo	DATA CENTER - DCMPF - TJES	Vitoria, Espirito Santo, Brasil
Itau Unibanco	Centro Tecnologico Mogi Mirim-DC2	Sao Paulo, Brasil
Itau Unibanco	Centro Tecnologico Mogi Mirim-DC1	Sao Paulo, Brasil
VIVO S.A.	Data Center Tambore	Sao Paulo,SP, Brasil
Level 3 Brasil Sao Paulo	Datacenter DC - 6, DC - 7 and DC - 8	Cotia, Sao Paulo, Brasil
TOTVS S/A	Datacenter TOTVS I, Phase 1	Sao Paulo, Brasil
Matrix Data Center	DC Matrix 1	Sao Paulo, Brasil

Brasil		
Compañía	**Data Center**	**Localización**
Getnet Tecnologia	Getnet Campo Bom	Campo Bom, Rio Grande do Sul, Brasil
Ascenty Data Centers Locação E Serviço LTDA	Ascenty DC Jundiai	Sao Paulo, Brasil
Oi Cyber Data Center	Data Center SIG - Brasília - DF	Brasília, Distrito Federal, Brasil
Governo do Estado do Parana	CELEPAR Data Center	Curitiba, Brasil
CSU	CSU.ITS	Sao Paulo, Brasil
BM&F BOVESPA S.A.	DATA CENTER BM&F BOVESPA	Sao Paulo, Brasil
CODEMIG	Data Center da Secretaria de Estado de Fazenda de Minas Gerais	Belo Horizante, Brasil
CODEMIG	DC PRODEMGE - Tecnologia	Belo Horizante, Brasil
Ascenty Data Centers Locação E Serviço LTDA	Ascenty DC Campinas	Sao Paulo, Brasil
Embratel	Data Center Embratel Lapa	Sao Paulo, Brasil
Petrobras	CIPD Centro Integrado de Processamento de Dados	Rio de Janeiro, Brasil
T-Systems Brazil	T-Center	Barueri, Sao Paulo, Brasil
Ativas Data Center	Belo Horizonte, MG	Belo Horizante, Brasil

Paraguay		
Compañía	**Data Center**	**Localización**
Millicom International Cellular	Tigo Paraguay – Asunción DC	Asunción, Paraguay

Paraguay		
Compañía	**Data Center**	**Localización**
Telefónica Celular Del Paraguay	TIGO Datacenter	Asunción, Paraguay

Argentina		
Compañía	**Data Center**	**Localización**
Empresa Argentina de Soluciones Satelitales S.A. - ARSAT	Centro Nacional de Datos ARSAT	Buenos Aires, Argentina
First Data SSSA	Parque Patricios Data Center	Buenos Aires, Argentina
Bapro Medios de Pago S.A.	Provincia NET – CPD Mitre	Buenos Aires, Argentina

Chile		
Compañía	**Data Center**	**Localización**
SONDA S.A.	DC SONDA Quilicura Phases 1 & 2	Santiago, Chile
ENTEL	Ciudad de los Valles Data Center, Phase 1 & 2	Santiago, Chile
SONDA S.A.	DC SONDA Quilicura Phases 1 & 2	Santiago, Región Metropolitana, Chile
INTESIS Chile S.A.	INTESIS Datacenter	Santiago, Chile
ENTEL	Ciudad de los Valles, Phase 2-2nd Flr	Santiago, Chile
Claro Servicios Empresariales SA	Datacenter Claro Liray	Santiago, Chile
ENTEL	Ciudad de los Valles Data Center, Phase 2-1st Flr	Santiago, Chile

Chile		
Compañía	**Data Center**	**Localización**
ENTEL	Ciudad de los Valles Data Center, Phase 1	Santiago, Chile
S&A CONSULTORES ASOCIADOS CHILE S.A.	Datacenter S&A Chile, Phase 1, 2	Santiago, Región Metropolitana, Chile
ENTEL	Ciudad de Los Valles III, Phase 1	Santiago, Chile
ADESSA	Corporativo Falabella, Phase 1	Santiago, Chile

El mercado global de los servicios cloud está dominado por EE.UU. Según 451 Research, EE.UU. atesora el 63% de los ingresos globales en este tipo de servicios, mientras que Europa representa solo el 23%; y solo el 6% de los proveedores cloud son europeos, mientras que el 88% provienen de EE.UU.

Según analistas de *Mordor Intelligence*, se espera que el mercado global de Centros de Datos para colocation crecerá desde 25.000 millones de dólares en 2014 hasta alcanzar aproximadamente el doble 50.000 millones de dólares a finales de 2020, con una tasa de crecimiento anual del 16%.

Estos datos han sido ratificados por la firma 451 Research, según la cual se esperaba que el mercado de Centros de Datos destinados a colocation llegaría a 36.000 millones de dólares a nivel mundial a finales de 2017.

A pesar de su volumen, sigue siendo un mercado muy fragmentado donde los mayores jugadores que operan en dicho sector a nivel mundial no superan el 10% de cuota. De ahí que se esté produciendo un proceso de concentración/consolidación donde los operadores globales absorben operadores locales o competidores más pequeños, con el fin de poder dar servicio a una misma multinacional en diferentes países, pues es una buena ventaja competitiva además de ser muy apreciada por los clientes finales.

Norteamérica lidera el mercado de Centros de Datos para colocation con 1.294 centros en los EE.UU. solamente. Esto es seguido por el mercado europeo, sobre todo en las principales capitales como son Londres, París y Ámsterdam. El mercado APAC (Asia-Pacífico) está creciendo rápidamente con cerca de 300 centros. 451 Research estima que, en la actualidad, menos de la mitad del espacio total destinado para colocation del mundo se encuentra en América del Norte, entorno a un 43%. EMEA y Asia-Pacífico componen una gran parte de la otra mitad, cada uno representa una cuarta parte del mercado. América Latina cuenta con alrededor de 5% del mercado.

Según Mordor Intelligence, se espera que el mercado de Centros de datos de colocation en **Europa** crecerá desde 6.000 millones de dólares en 2014 a 10.000 millones de dólares a finales

de 2020, a una tasa de crecimiento anual del 10,18%. El mercado de Centros de Datos europeo está creciendo rápidamente con nuevos operadores y Centros de Datos nuevos que se desarrollan sobre todo en Europa occidental.

El país que lidera el sector en **Europa** es Reino Unido con 224 centros. Francia (principalmente su capital, París) ocupa el segundo lugar con 48 seguido de Ámsterdam con 38. Se espera que las cifras aumenten a medida que aumenta el optimismo en el mercado y los proveedores respondan a la creciente demanda mediante la ampliación de sus instalaciones.

El mercado de colocation en **Latinoamérica** se consideró en 2014 con un volumen de 400 millones de dólares y se espera un crecimiento hasta los 800 millones en 2019 con una tasa de crecimiento anual del 14,87%. Sin duda es un mercado donde hay mucho recorrido y posibilidades de expansión. Se estima que existen 50 Centros de Datos de colocation repartidos en varios países, lo cual da lugar a que se considere un mercado con bastante potencial por desarrollar.

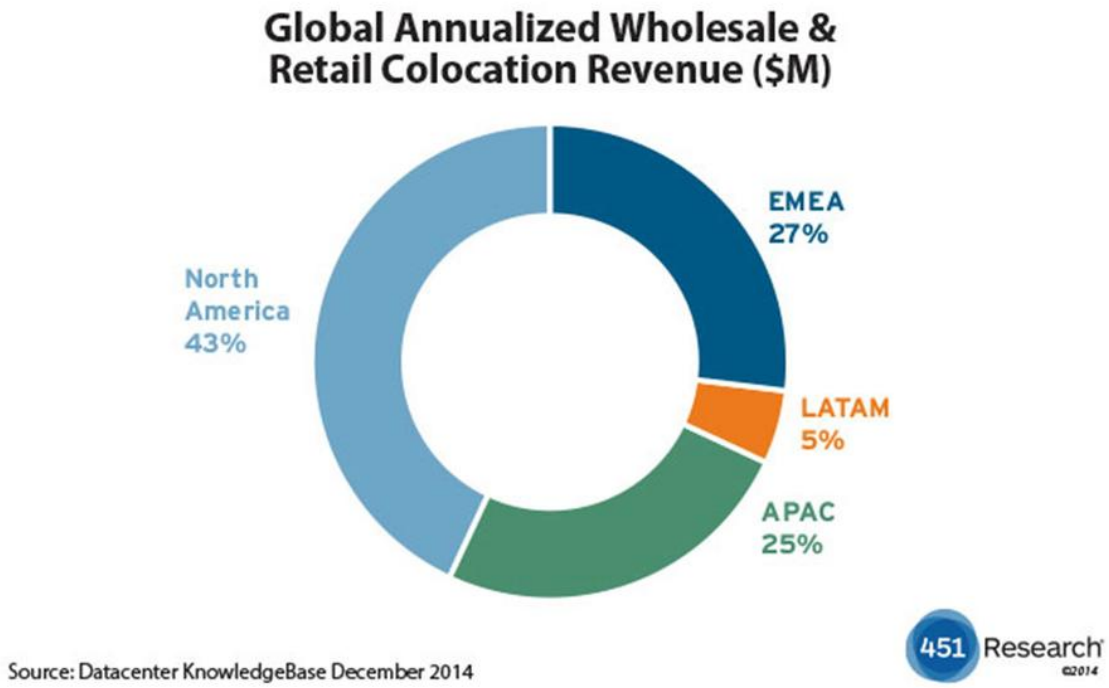


Figura 4 Distribución de ingresos anuales por servicio de colocation por regiones.

Fuente: 451 Research

3.3 Benchmark. Estándares para la compatibilidad de la tecnología de los centros de datos con la normativa ecológica

Es importante tener muy presente la relevancia de las cuestiones medioambientales por el impacto ecológico directo e indirecto que conllevan así como por la consecución de la mejor gestión posible que estará ligada a ahorros en el gasto de operación.

Las dos magnitudes más extendidas para medir la eficiencia energética del Centro de Datos son las siguientes:

- **Power Usage Effectiveness** (PUE). Fue creado por los miembros del Green Grid. Consiste en dividir la potencia total suministrada al Centro de Datos entre la potencia que consume el equipamiento IT. La máxima eficiencia es 1.

- **Data Center Infrastructure Efficiency** (DCIE) es el recíproco del PUE y se expresa como un porcentaje, que mejora a medida que se acerca al 100%.

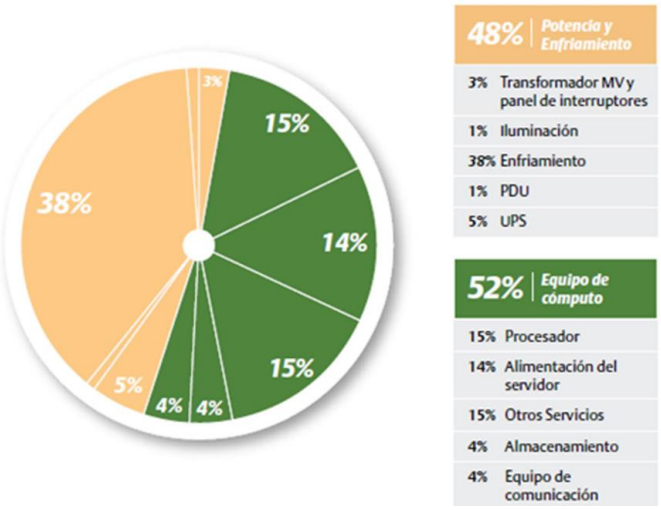


Figura 5 A grandes rasgos la mitad de la energía la consume el equipamiento TIC y la otra mitad los sistemas de soporte (alimentación y refrigeración).

Fuente: Epsilon DC

Asociada a la eficiencia energética está la huella de carbono. La huella de carbono es la cantidad de gases de efecto invernadero generada por el Centro de Datos. Al igual que en otros sectores, debido en parte al encarecimiento de la energía y también a la cada vez mayor conciencia ecológica, reportar la huella de carbono está siendo cada vez más habitual. En los Centros de Datos se consume mucha electricidad y se genera mucha energía térmica que se desperdicia.

El uso de Centros de Proceso de Datos supone un consumo del 1% de la energía a nivel mundial y las TIC suponen ya el 2% de las emisiones globales de gases de efecto invernadero a la atmósfera. En los últimos años, el costo de los servidores ha seguido una tendencia descendente y prácticamente se ha visto superado por el costo de la electricidad que consumen.

"Las organizaciones que apuesten por mover sus aplicaciones de negocio a la nube pueden reducir el consumo de energía y las emisiones de carbono en un 30 por ciento o más, frente a aquellas que tienen sus aplicaciones funcionando en infraestructura propia". Esta es la principal conclusión de un estudio encargado por Microsoft y llevado a cabo por Accenture y WSP Environment and Energy.

La Nube permite compartir recursos al más alto nivel, desde equipamiento TI, hasta equipos de infraestructuras de apoyo al centro de datos, esto permite reducir los consumos y el aprovechamiento máximo de la energía. De esta forma se optimiza la Huella de CO2.

Los grandes Centros de Datos, en los que se alojan las infraestructuras con modelo de Computación en la Nube, se benefician de economías de escala y eficiencias operativas que los departamentos de TI de las empresas que los tienen en sus propias instalaciones no pueden alcanzar. Estos beneficios son aún más evidentes para las pequeñas y medianas empresas.

La Computación en la Nube permite a las empresas trabajar de una manera más productiva y eficiente, erigiéndose como una alternativa económica y sostenible en la gestión de los recursos y ofreciendo significativas ventajas, a destacar:

- Un potencial de ahorro energético importante, ya que la computación en la nube ayuda a las empresas a reducir su consumo de energía, lo que, además de perjudicar al medio ambiente, les supone un gasto adicional y un impacto importante en su cuenta de resultados.
- La Computación en la Nube permite gestionar de forma remota y centralizada todas las oficinas o centros logísticos dispersos geográficamente. Del mismo modo, la nube permite su uso a través de ordenadores portátiles, dispositivos móviles, smartphones, etc., mediante el acceso a los servicios alojados en la nube desde cualquier lugar, minimizando con ello la necesidad de recursos.
- La Computación en la Nube permite diseñar e implantar políticas avanzadas de ahorro energético basadas en la reducción del consumo de maquinaria y/o equipos informáticos.

Además, los Centros de Datos para la Computación en la Nube disponen de infraestructuras cada vez más eficientes y ubicados en edificios inteligentes y/o automatizados que aportan un uso más eficaz y racional de las infraestructuras tecnológicas.

- Los Centros de datos actuales buscan trabajar en PUE : 1.3-1.8
- Los Centros de datos se diseñan empleando estrategias encaminadas a mejorar su rendimiento energético, prestando especial atención al ahorro de energía, la eficiencia en el uso de agua, la reducción de las emisiones de CO_2, el incremento de la calidad del ambiente interior, el empleo sostenible de los recursos y la sensibilización ante el impacto producido en el medioambiente.

Existe un concepto muy relacionado con la explotación de la computación en la Nube, que es conocido mediante el término inglés *Green IT*.

El *Green IT* es un conjunto de buenas prácticas con el objetivo de usar de manera eficiente los recursos energéticos y de capacidad IT para minimizar el impacto ambiental. Esto se consigue realizando una gestión eficiente de los recursos e infraestructuras para garantizar que se maximiza su uso y ocupación para aprovecharlos al máximo y evitar esos "ciclos ociosos" en los que consumimos energía y, sin embargo, no estamos usando los sistemas.

Mediante la consolidación de distintos Centros de Datos locales y sus sistemas de IT (ya sean servidores, almacenamiento, accesos a Internet, etc.) en Centros de datos como el que se proyecta para Asunción, se consigue no sólo los ahorros energéticos claros relativos a un diseño de los recursos propios del centro de datos más óptimo, sino que, gracias a que la computación en la nube se basa en la virtualización, los mismos elementos hardware físicos se pueden emplear en paralelo para diversos servicios, consiguiendo de este modo , además de ahorrar espacio físico en el Centro de datos también ahorraremos en costos de operación, lo que permitiría la eliminación de muchos Centros de datos ineficientes para apostar por soluciones en la nube mucho más eficientes.

Una métrica muy representativa para evaluar tanto la eficiencia de las infraestructuras técnicas del Centro de Datos como del propio equipamiento IT que está ubicado dentro del mismo se denomina CADE:

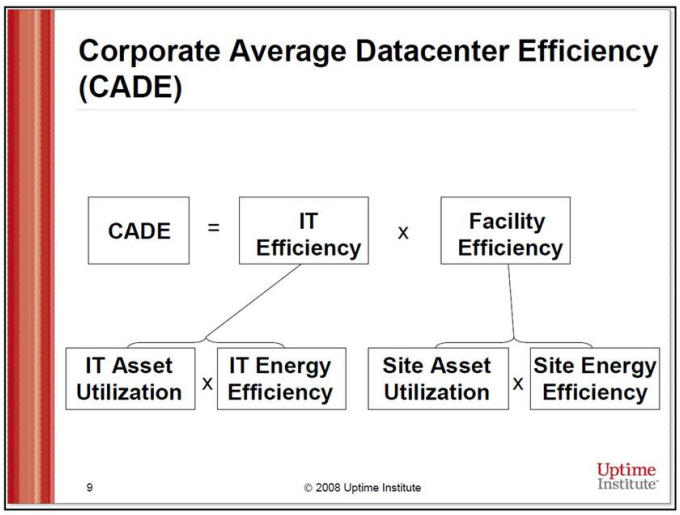


Figura 6 Este tipo de métricas nos van a permitir conocer cómo evoluciona a eficiencia de nuestro Centro de Datos en el tiempo.

Fuente: Uptime Institute

3.3.1 Tipos de Centros de Datos

Fundamentalmente, existen 2 tipos principales de Centros de datos **físicos**.

- Centro de Datos Empresarial (Enterprise DC).
- Centro de Datos No empresarial:
    - Centro de Datos de colocation.
    - Instalación de hosting y servicios gestionados.
    - Instalación de hosting al por mayor o mayorista (Wholesale DC).

Centro de Datos Empresarial

La aceptación general es que se trata de aquellos que son propiedad de la organización que los explota y exclusivamente para su propio uso.

Los Centros de datos empresariales suelen ser la opción por la que se decantan las empresas que precisan un elevado nivel de seguridad y fiabilidad en sus instalaciones de TI; en muchos casos se encuentran en los propios edificios de la sede principal y no suelen corresponder a la actividad principal de la organización.

Centro de Datos de Colocation

Los Centros de datos de Colocation son aquellos en los que los clientes pueden albergar sus propios equipos de misión crítica dentro de unas instalaciones propiedad de un tercero, que también las explota y presta toda la infraestructura de soporte necesaria como la alimentación eléctrica, el enfriamiento y la conectividad.

El uso de una infraestructura de centro de datos compartido puede generar ahorros permitiendo, al mismo tiempo, a los clientes conservar un elevado nivel de control sobre sus equipos y sistemas.

Las instalaciones de colocation tienen unos elevados niveles de seguridad física. La necesidad de los clientes de acceder físicamente solamente a sus propios equipos hace que el espacio en planta se presente generalmente con menor grado de densidad.

Instalación de hosting y servicios gestionados

Las instalaciones de hosting gestionado son aquellas en las que los clientes alquilan capacidad de servidor, en lugar de ser sus propietarios y quienes los operan.

El hosting puede ser dedicado (es decir, uso exclusivo de los servidores) o compartido, y puede ir desde un solo servidor hasta todo un Centro de Datos completo.

El nivel de servicio prestado varía de un cliente a otro en función de sus necesidades y requerimientos.

Instalación hosting mayorista

Las instalaciones hosting mayoristas son aquellas en las que los clientes alquilan espacio o capacidad de servidor de los propietarios de servicios de colocation y luego los utilizan para vender servicios a sus propios clientes. Es decir, se pide a un proveedor que ya da el servicio una cierta capacidad o disponibilidad sobre el equipamiento que dicha empresa tiene, y se ofrece a terceras empresas. Es por ello que se dice que es un concepto similar al de subarrendar espacio de oficinas, donde alguien que tiene una oficina grande alquilada subarrienda parte de la misma, que no usa, a terceras empresas.

Servicios en la nube

Los servicios en la nube pueden ser alojados como nubes privadas en Centros de Datos empresariales, como servicios en la nube pública como un negocio (por ejemplo: Yahoo! y Amazon) y como servicios de especialistas en la nube que suelen utilizar los mayoristas que operan entornos de colocation o de hosting gestionado.

Todos los tipos de Centros de datos pueden disponer de servicios en la nube.

3.4 Estándares de clasificación de los Centros de Datos

Las distintas clasificaciones disponibles (aunque hoy en día predomina la que referencia a los niveles Tier) son una estrategia de diseño de los Centros de datos para proporcionar cierto nivel de disponibilidad en función de la criticidad de una operativa de TI y de negocio.

Syska Hennessy
Clasificación de 1 a 10.

TIA 942
Tier 1 a Tier 4.

BICSI 002
Clase F0 a Clase F4.

Uptime Institute
Tier I a Tier IV.

Todas las clasificaciones reconocen cuatro categorías o clases principales de diseño para proporcionar un cierto nivel de disponibilidad:

1. Rutas únicas sin redundancia = N.
2. Rutas únicas con algunos componentes de redundancia = N+1.
3. Mantenibilidad simultánea = 2N.
4. Capacidad de mantenimiento simultáneo con plena tolerancia a los fallos = 2 (N+1).

3.4.1 El concepto TIER

El nivel de fiabilidad de un centro de datos viene indicado por uno de los cuatro niveles de fiabilidad llamados TIER, en función de su redundancia. A mayor número de TIER, mayor disponibilidad y, por tanto, ello supone mayores costos de construcción y mantenimiento.

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,671%	0,33%	28,82 horas
TIER II	99,741%	0,25%	22,68 horas
TIER III	99, 982 %	0,02%	1,57 horas
TIER IV	99,995%	0,01%	52,56 minutos

TIER I- Nivel 1 (Básico)

- Disponibilidad del 99,671 %.
- Sensible a las interrupciones, planificadas o no.
- Una sola ruta para el suministro eléctrico y distribución de aire acondicionado, sin componentes redundantes.
- Sin exigencias de piso elevado.
- Generador independiente.
- Tiempo de inactividad anual: 28,82 horas.
- Implica afecciones al servicio para realizar algún mantenimiento preventivo.

TIER II- Nivel II (Componentes redundantes)

- Disponibilidad del 99,741 %.
- Menor sensibilidad a las interrupciones.
- Una sola ruta para el suministro eléctrico y distribución de aire acondicionado, con un componente redundante.
- Incluye piso elevado, UPS y generador.
- Tiempo de inactividad anual: 22,68 horas.

- El mantenimiento de la alimentación y otras partes de la infraestructura requieren de alguna parada del servicio.

TIER III- Nivel III (Mantenimiento concurrente)

- Disponibilidad 99,982 %.
- Interrupciones planificadas sin interrupción de funcionamiento, pero posibilidad de problemas en las no previstas.
- Múltiples accesos de energía y refrigeración, con una sola línea de distribución activa. Incluye componentes redundantes (N+1).
- Tiempo de inactividad anual: 1,6 horas.

TIER IV- Nivel IV (Tolerante a errores)

- 99,995 % de disponibilidad.
- Interrupciones planificadas sin interrupción de funcionamiento de los datos críticos. Posibilidad de sostener un caso de improviso sin daños críticos.
- Múltiples pasos de corriente y rutas de enfriamiento. Dos líneas de distribución simultáneamente activas, típicamente en una configuración sistema + sistema. Incluye componentes redundantes (2(N+1)) – por ejemplo, teniendo 2 UPS cada uno con redundancia (N+1).
- Tiempo de inactividad anual: 0,88 horas.

Como referencia del sector debemos tener presente algunas de las Organizaciones Sectoriales más representativas:

The Green Grid

Consorcio global para reducir el consumo energético de los Centro de Datos.

Uptime Institute

Mejorar el tiempo de actividad del centro de datos y la productividad de TI mundial mediante el establecimiento de referencias y el aprendizaje colaborativo.

ASHRAE

American Society of Heating, Refrigeration and Air Conditioning Engineers (Sociedad Americana de Ingeniería de Calefacción, Refrigeración y Aire Acondicionado)

US EPA/DoE

El Energy Star es un programa conjunto de la EPA y el DOE estadounidenses para ayudar a identificar los productos y prácticas energéticamente eficientes.

SNIA

Consorcio global de líderes que ayuda a definir la eficiencia energética y la eficiencia en el espacio de almacenamiento.

Code of Conduct (Centro de Datos)

Código de Conducta de la UE (Unión Europea) para Centros de Datos

3.4.2 *Descripción de las instalaciones de apoyo*

Todo Centro de Proceso de Datos, deberá cumplir un conjunto de requisitos que garanticen su disponibilidad y continuidad:

ROBUSTEZ: por encima de todo, el Centro de Proceso de Datos será fiable. Independientemente de las catástrofes que pudieran ocurrir. El Centro de Proceso de Datos será el centro neurálgico donde se ubicarán los elementos de control y de comunicaciones requeridos por muchos centros de gran importancia para el correcto funcionamiento de las instituciones de la Republica del Paraguay, por lo que no deberán interrumpirse bajo ninguna circunstancia. Para garantizar esta situación, se implantará una infraestructura redundante.

Para dicha configuración el Centro de Proceso de Datos debería tener una topología, con las infraestructuras concurrentemente mantenibles. Se podrán hacer cualquier labor de mantenimiento a cualquier equipo y distribución sin que ello afecte a la continuidad del servicio crítico.

Como referencia se puede tomar la topología "TIER III" según Uptime Institute[1].

"La topología TIER III es *mantenimiento concurrente*, por lo que no son necesarios apagados para mantenimiento, lo cual permite un programa de mantenimiento más agresivo y mejora de esta forma el rendimiento total de los equipos. "

Según múltiples estadísticas y estudios, la mayoría de las causas de las afecciones al servicio del Centro de Datos fueron fallos en las infraestructuras de alimentación y refrigeración. Sin embargo, otro gran porcentaje se corresponde a los errores humanos, por lo que es imprescindible promover los buenos hábitos en el Centro de Datos y una formación continua.

[1] Uptime Institute: es una organización de asesoramiento imparcial centrado en mejorar el rendimiento, la eficiencia y la fiabilidad de las infraestructuras críticas de negocio a través de la innovación, la colaboración y certificaciones independientes. Es reconocido a nivel mundial para la creación y administración de las Normas y Certificaciones de Nivel para el diseño, Construcción y Sostenibilidad Operativa de los centros de datos.

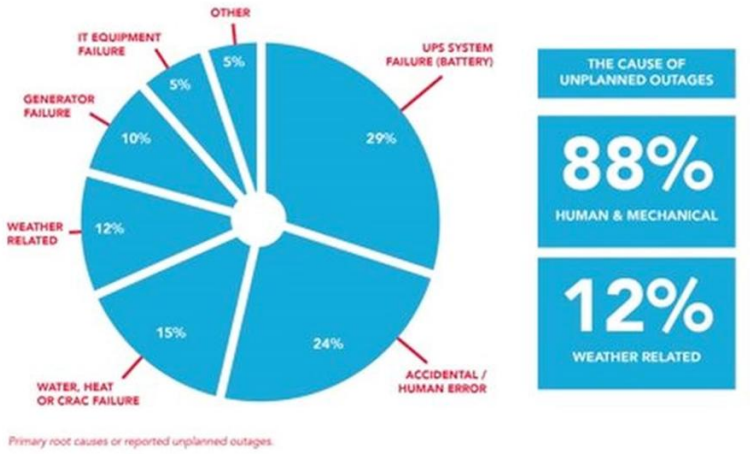


Figura 7 Causas de apagado no planeado en Centros de Datos.

Fuente: Emerson Network Power, Uptime Institute y Jason Weckworth

FLEXIBILIDAD: al igual que su infraestructura, un Centro de Datos no es estático. Por tanto, en su diseño y mantenimiento, se buscará la flexibilidad utilizando componentes que permitan una sencilla reposición o un desplazamiento rápido a otra posición.

El Centro de Datos deberá tener una vida útil mayor de 20 años. Durante este largo periodo se deberán abordar numerosas acciones de mantenimiento e incluso de sustitución o renovación completa de sus sistemas. Se deberán instalar salas de mantenimiento y almacén próximos al Centro de Datos.

El Centro debe disponer de una zona de gerencia y oficinas para poder operar el centro y ofrecer los servicios de Computación en la Nube.

Es importante que se disponga en el edifico de una sala de trabajo técnico donde se puedan realizar las tareas de configuración y mantenimiento de los diferentes equipos del Centro de Datos. Así mismo es recomendable disponer de un almacén para guardar de forma controlada equipos o piezas de recambio.

MODULARIDAD: El Centro de Datos debe ser modular y así mantener una infraestructura simple y escalable. El modularidad de un espacio permite que un usuario que conoce la configuración de un rack, entienda con rapidez el resto de armarios de la sala.

ESTANDARIZACIÓN: el Centro de Datos debe ser un entorno coherente, proporcionando estabilidad a los sistemas de información que alberga, así como aumentando su usabilidad. Cuantos más componentes distintos haya en el Centro de Datos, el entorno se vuelve más complejo y, por tanto, más difícil de manejar.

Solución eléctrica

Se acuerda planificar una solución eléctrica basada en un diseño Tier III.

Si empezamos desde fuera hacia dentro en nuestro centro de datos, el primer factor que debemos tener presente sería la **acometida eléctrica** por parte de compañía suministradora que debe ser dedicada y exclusiva para el Centro de Datos. Siendo recomendable, en base a la criticidad de los servicios y clientes, disponer de doble acometida eléctrica desde subestaciones distintas.

A continuación, pasaríamos, dentro de nuestro centro de datos, a la instalación asociada a nuestro **centro de transformación**, donde se dispondrá de, al menos, dos transformadores con las correspondientes celdas y protecciones asociadas. El tamaño de dichos transformadores vendrá definido por el tamaño del propio centro de datos (y por tanto por la capacidad física de albergar equipos y servicios de TI en las salas a tal efecto) y por el plan de crecimiento y expansión que se defina.

Grupo electrógeno, para arranque automático en caso de fallo de suministro de compañía. Tal y como se comentará en algún otro apartado, se debe estudiar la necesidad de tener redundancia, es decir más de un grupo electrógeno, en base a la tolerancia a fallo que estemos buscando, así como en base a la criticidad de las cargas y servicios a soportar. Hay que tener en cuenta que el grupo electrógeno siempre va a tener una capacidad inferior a su potencia nominal total en el momento del arranque y, por tanto, es un detalle a tener muy en cuenta a la hora de definir su capacidad.

Es importante que el grupo electrógeno que se seleccione cuente con regulador electrónico de velocidad con calidad de onda (frecuencia) de G3.

Asociado al grupo electrógeno de emergencia se debe disponer de **almacenamiento de combustible**, con capacidad suficiente para proporcionar al menos 72 horas de autonomía al grupo/s electrógeno/s a plena carga, siendo deseable llegar incluso a poder mantener la instalación durante 1 semana. Para ello se contempla disponer de depósitos principales de suficiente capacidad. Deberemos considerar un sistema automático de trasiego de combustible desde los depósitos nodrizas (principales) hasta los depósitos interiores de los grupos electrógenos, de manera que en caso de necesidad llegue el combustible sin precisar de intervención por parte de ningún operador o técnico del centro de datos.

Otro de los elementos que vamos a necesitar será un sistema para realizar la c**onmutación automática**, entre suministro de compañía y grupos electrógenos. Esto es posible realizarlo con múltiples soluciones (PLCs, ATS, etc.) que vendrán definidas por el tamaño y complejidad de nuestro centro de datos.

Durante el tiempo de transferencia desde el suministro de compañía al suministro por medio del grupo electrógeno, algo que suele durar unos segundos, y en el retorno una vez tengamos recuperado suministro, es necesario que la carga sea soportada por un **Sistema de Alimentación Ininterrumpida (SAI)**, con capacidad suficiente para soportar la carga que se defina en la fase de diseño. La redundancia mínima debe ser n+1, de manera que podamos soportar toda la carga con nuestro sistema, aunque uno de los elementos este fuera de servicio. Este sistema es de vital importancia ya que cortes de suministro eléctrico siempre van

a existir, bien porque haya fallado el suministro o por tareas propias de mantenimiento. Y asociadas a dichos equipos debemos tener sus baterías, que deben ser suministradas con autonomía de 10-15 minutos (a plena carga) y de una calidad mínima de 10/12 años de vida útil. Dados los múltiples y peligrosos incidentes que pueden ocasionarse durante los años que estén instaladas, habrá que seleccionar de manera meticulosa a los fabricantes que opten a su suministro. Las baterías deben siempre ubicarse repartidas en dos salas independientes, de cara a evitar que un incidente de cualquier índole en una sala nos deje sin ninguna batería disponible, y donde sólo tengamos instalados dichos elementos, para poder poner las medidas de seguridad y salud propias para dichas salas, así como para que podamos climatizar de la manera más adecuada para prolongar su vida útil al máximo, dado que son elementos de alto costo y si se deterioran antes de lo previsto nos van a incrementar sensiblemente nuestro costos de operación.

Con la adopción de arquitecturas de UPS escalables o modulares vamos a poder invertir en función del crecimiento del negocio. Así, el administrador del Centro de Datos simplemente puede agregar módulos a medida que crecen las necesidades del propio centro. En cualquier caso, siempre, y es algo que no podemos evitar, deberemos dejar la instalación (cables, protecciones, espacios para ampliaciones, etc.) dimensionada para soportar la máxima capacidad de dicho sistema en un futuro. Hoy en día existen bastantes fabricantes que nos ofrecen modelos de UPSs modulares en distintas potencias, por tanto, la clave para nuestra selección debe basarse en la presencia física y de soporte técnico que tengan dichos fabricantes de referencia internacional en Paraguay.

En muchos Centros de Datos y para poder cubrir cualquier necesidad o requerimiento de los distintos sistemas y plataformas de TI que se instalen a futuro, es posible considerar en su diseño la instalación de un **Sistema de Continua, Rectificadores (-48V)** y sus baterías asociadas. Especialmente si se va a soportar mucho equipamiento de comunicaciones, para dar servicios a través de la red de fibra óptica por ejemplo, de manera que sería necesario establecer un sistema de alimentación de garantía de suministro eléctrico para dicho equipamiento.

Existen infinidad de detalles a controlar y monitorizar, de manera que es muy importante seleccionar aquellos que por su importancia serán más críticos para la seguridad de la operación de nuestro Centro de Datos. Es por ello que se sugiere instalar algún sistema de monitorización avanzada de uno de los elementos más críticos, como son las baterías. En este tipo de sistema mediante corriente continua se visualiza el estado de cada celda individualmente y con ello maximizamos la detección precoz de deterioro interno permitiendo realizar las actuaciones que correspondan.

Todas las canalizaciones metálicas deberán estar puestas a tierra.

Solución de climatización

Para poner las bases de su alcance comenzaremos diciendo que la producción de frio es igual a la eliminación de calor. De hecho, la refrigeración podemos definirla como el proceso de extracción de calor de una sustancia o espacio por cualquier medio. Además, debemos

recordar que el calor es una forma de energía y desde el punto de vista de la termodinámica es la energía en tránsito de un cuerpo a otro como resultado de una diferencia de temperatura entre los dos cuerpos. Agregar o quitar energía implica un cambio en el estado físico del material (sólido, líquido, gas) y un cambio en su temperatura. Finalmente, y para dejar totalmente definidas las bases del ciclo frigorífico, debemos decir que se produce debido a que existen sustancias que a temperatura ambiente son capaces de evaporarse (los refrigerantes). En este cambio de líquido a gas absorben mucho calor (eliminamos calor de sala). El lugar donde realizan este proceso es el EVAPORADOR. Ese gas recalentado (con la energía de la sala) es llevado al exterior mediante el CONDENSADOR, elemento que forma parte del circuito cerrado. El intercambio térmico con el exterior provoca que este gas se transforme de nuevo en líquido. En medio de ambos existe una "bomba" que mueve el gas desde el evaporador al condensador, este elemento es el COMPRESOR, funcionamiento según ciclo de Carnot.

Límites de diseño ASHRAE TC9.9

Conforme a lo establecido en las guías diseño del Uptime Institute y la TIA-942, se deben considerar las condiciones máximas de operación establecidas por la ASHRAE TC9.9. Al ser equipos críticos se consideran sus más altos niveles de condiciones ambientales de nivel A1. Los valores recomendados son:

- Temperatura de bulbo seco: 18 - 27 ºC
- Humedad relativa: Entre -9 ºC de punto de rocío y 15 ºC de punto de rocío y 60 % de humedad relativa sin condensación

En las mismas recomendaciones se hacen referencia a límites máximos admisibles:

- Temperatura de bulbo seco: 15 - 32 ºC
- Humedad relativa: Entre -12ºC de punto rocío y 8 % de humedad relativa y 17 ºC de punto de rocío y 80 % de humedad relativa sin condensación

Estas condiciones de temperatura son idóneas para mantener niveles seguros de humedad relativa, así como también permite al sistema de refrigeración tener cierta inercia en caso de fallo del sistema.

Por su lado, los niveles recomendados de humedad relativa son adecuados para operaciones de procesamiento de datos. Bajo estas circunstancias, los equipos IT están protegidos contra problemas de corrosión asociados a altos niveles de humedad, y evitan fallos temporales y permanentes causados por interferencias intermitentes de las descargas electrostáticas asociados a valores bajos.

Las descargas electrostáticas se generan y se disipan en mayor medida en zonas donde la humedad relativa presenta valores por debajo del 20 %, y se convierte en valor crítico cuando el nivel baja del 8 %.

Dichas condiciones deben preservarse en las tomas de aspiración de los equipos IT, y no en su parte posterior, es decir, en los pasillos fríos. Mientras que la temperatura deberá ser controlada de una manera estable, la humedad podrá fluctuar arbitrariamente siempre y cuando se mantenga dentro de los límites establecidos.

Por último, los equipos serán diseñados de manera a poder asegurar la calidad del aire en su interior, según norma ISO 14644-1 clase 8.

Perfil psicrométrico

Los sistemas de climatización deben ser dimensionados respecto a las peores condiciones ambientales en los últimos 20 años conforme a lo estipulado en las guías de diseño del Uptime Institute y la TIA-942. Para ello, se ha considerado la estación meteorológica más cercana dentro de la base de datos de la ASHRAE de su edición 2015, la cual está ubicada en el aeropuerto internacional de Silvio Pettirossi en Asunción (Paraguay) a 18 km del centro de la ciudad. Sus datos son:

- WMO #: 862180
- Latitud: 25,240 Sur
- Longitud: 57,519 Oeste
- Elevación: 89 msnm
- Datos considerados: 1990 a 2014.

Los datos extremos a 20 años son:

- Temperatura máxima de bulbo seco: +41,3 ºC
- Temperatura mínima de bulbo seco: -1,1 ºC
- Temperatura máxima de bulbo húmedo: +29,9 ºC
- Temperatura mínima de bulbo húmedo: -1,6 ºC
- Temperatura máxima de punto de rocío: +29,9 ºC
- Temperatura mínima de punto de rocío: -8 ºC

Debido a que la ubicación del nuevo Centro de Datos permitirá una buena disipación de la energía, no se considera necesario acentuar demasiado los factores de seguridad. Así pues, se considerará las siguientes condiciones de diseño:

- Temperatura máxima de bulbo seco: +42,0 ºC
- Temperatura mínima de bulbo seco: -2,0 ºC
- Temperatura máxima de bulbo húmedo: +30,0 ºC
- Temperatura mínima de bulbo húmedo: -2,0 ºC
- Temperatura máxima de punto de rocío: +30,0 ºC
- Temperatura mínima de punto de rocío: -8,0 ºC

A continuación, se muestran la frecuencia en horas anuales de la temperatura de bulbo seco, punto de rocío y bulbo húmedo para dicha estación:

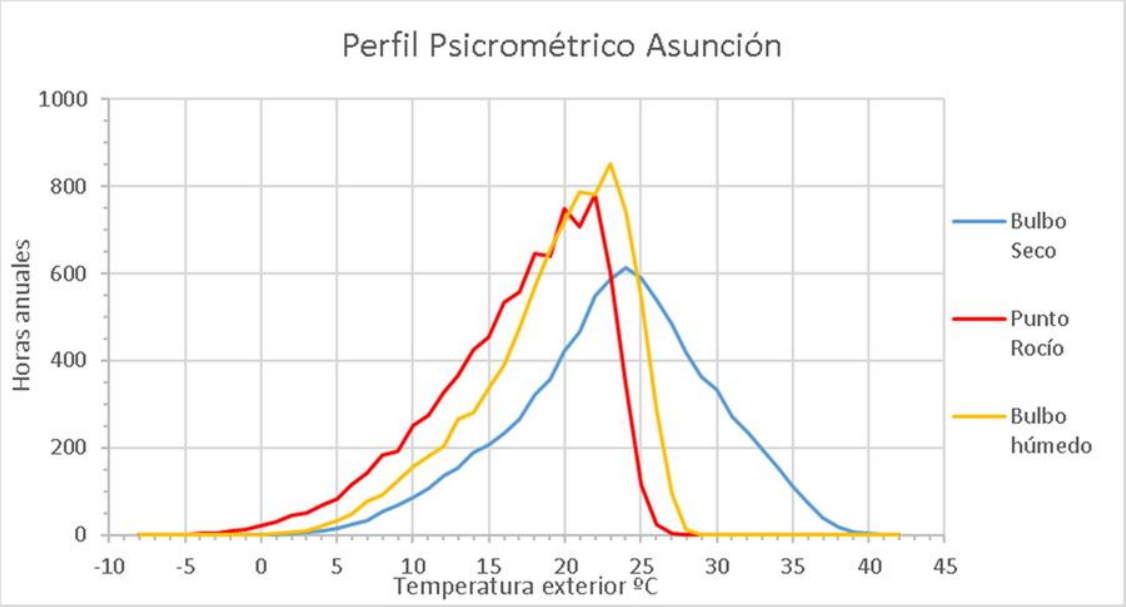


Figura 8 Perfil psicrométrico de Asunción

Fuente: Elaboración propia

Como se puede observar las condiciones son muy estables a lo largo del año siendo temperaturas muy habituales en bulbo seco entre 20 y 30 ºC. Así mismo, cabe destacar que los valores de humedades son bastante elevados a lo largo del año siendo durante buena parte del año por encima de 15 ºC.

Entre los distintos sistemas y multitud de soluciones que se pueden encontrar hoy en día en el mercado, dependiendo siempre de lo que estemos dispuestos a gastarnos, cabe destacar algunos grupos principales:

Sistemas de agua refrigerada: Utiliza agua refrigerada en lugar de refrigerante para mover el calor entre las unidades de aire, las enfriadoras (chillers) y el intercambiador de calor. La solución suele ser agua o un sistema de agua/glicol (de cara a evitar congelaciones en las tuberías en zonas donde se alcancen temperaturas que pueden ocasionar la congelación del agua). El calor de la sala de equipos se gestiona desde las unidades interiores. En la mayoría de las instalaciones actuales la temperatura del agua enfriada/refrigerada se entrega a 6ºC/7ºC con una temperatura de retorno de 12ºC/13ºC. Lo aconsejable para ser más eficientes sería diseñar para trabajar con una temperatura de impulsión en torno a 20ºC y la de retorno a 26ºC. De hecho, podríamos intentar ir a temperaturas incluso superiores para conseguir una mejor eficiencia y por tanto un mayor ahorro.

Sistema de expansión directa (DX): En estos sistemas un refrigerante es utilizado como parte de un sistema de enfriamiento de compresión/expansión directa. El evaporador está en contacto directo con el aire, de forma que el serpentín de enfriamiento del circuito de aire también es el evaporador del circuito de refrigeración. El aire pasa por la parte exterior del serpentín del evaporador para que se enfríe directamente por la expansión del refrigerante que pasa a través del serpentín.

Economizadores: Utilizados para complementar o sustituir a las enfriadoras (chillers) aprovechando la temperatura del aire exterior. Típicamente incluyen filtros para capturar partículas. Solemos clasificarlos en dos tipos: Lado del aire, cuando se introduce aire exterior más frío para reducir el calor. Lado del agua, cuando el aire frío enfría una torre exterior de agua enfriada/refrigerada.

Los Centros de Datos bien diseñados y operados pueden conseguir una óptima reducción de consumo.

Hay estudios que muestran que en algunas regiones del mundo es posible construir un centro de datos que funcione prácticamente sin refrigeración mecánica. Es importante tener presente que debemos definir con nuestros clientes, stakeholders e instituciones a las que vayamos a prestar servicio cuáles serán las condiciones de funcionamiento de nuestro centro de datos.

En cualquier caso, habrá que estudiar la mejor opción teniendo en cuenta las necesidades, tamaño y ubicación del centro de datos. Es importante tener siempre presente que uno de los costos más representativos del centro de datos es la climatización (tanto en la fase de construcción como en los costos operativos de su gestión diaria dado su impacto en la factura del consumo eléctrico), además de ser uno de los sistemas más importantes para el correcto funcionamiento de todos los servicios que se vayan a alojar dentro de nuestro centro de datos. Volvemos a insistir en que hay que considerar fabricantes e instaladores con presencia física en el país donde vayamos a comprar e instalar dichas soluciones de climatización.

Se recomienda una solución de climatización basada en expansión directa, evaluando el considerar la fórmula de freecooling directo o indirecto en función de las características de la ubicación final de los Centro de Datos, dada la flexibilidad que nos permitirá ante un crecimiento por fases y modular de nuestros futuros Centros de Datos. Además, este tipo de soluciones permiten una garantía adicional para evitar puntos únicos de fallo algo que en la parte de climatización se hace de vital importancia.

Todos los equipos especificados deben ser de alto rendimiento y quedarían configurados como una solución integrada bajo único sistema de control que permitirá que las unidades trabajen coordinadamente para asegurar el máximo rendimiento y menor PUE posible en cualquier situación de carga del Centro de Datos.

Indicar que como apoyo a la mejor eficiencia y aprovechamiento de la refrigeración se establecerán cerramientos de pasillo frio en las salas de equipos IT. Dichos pasillos fríos dispondrán de una distancia mínima de 120cm entre las filas de racks.

Los racks serán de 42 “U” con un tamaña de 80cm de ancho y 100cm de fondo. Disponiendo de blanking panels para tapar todas las “U” que no se utilicen con equipos de cara a facilitar el uso más adecuado del flujo de aire frio.

Independiente de la solución que se decida usar para la climatización es más que recomendable disponer de un sistema de **detección de fuga de líquidos,** el cual normalmente consta de un cableado que distribuiremos por el perímetro de las distintas salas técnicas y dentro de la sala de equipos TI (normalmente bajo el suelo técnico), para identificar cualquier posible fuga o escape que pudiera producirse.

Instalación de fontanería

Sistema de distribución de agua para los servicios de aseos y otros propios de oficinas.

Instalación de saneamiento

Red de saneamiento para la recogida de condensados de las unidades CRAC y su conexión al sistema general de saneamiento de la zona.

Exteriormente, el sistema comprende una red de bajantes pluviales que permite recoger el agua de lluvia desde la cubierta del edificio y llevarla hasta la cota 0 a nivel de calle para que el agua sea posteriormente recogida por el saneamiento de la zona.

Red de saneamiento exterior para la recogida de aguas fecales para que sea recogida por la red exterior de saneamiento de zona.

Sistema de Protección Contra Incendios

Los sistemas de seguridad juegan un papel fundamental, aunque solo nos acordamos de ellos en caso de incidentes en dicha materia. De ellos conviene destacar en primer lugar el sistema de protección contra incendios. Este sistema va a venir definido por una central principal que hace de gestor de todas las alarmas y acciones en dicho sistema. Es conveniente disponer de un sistema automático de extinción al menos en sala/nodo donde tengamos los equipos, plataformas y sistemas de TI. La central principal de detección recibe información de los distintos detectores (que deben ser analógicos direccionales) que tendremos que tener instalados por todo el centro de datos, y es la que debe dar orden a las sub-centrales de extinción para que actúen ante un conato de incendio. Siempre debe tratarse de protocolos abiertos y por tanto el lenguaje que se use para la comunicación entre la central principal y los detectores debe ser igual y estar disponible para las distintas empresas que pueden ofrecer su mantenimiento. Además, dicha central principal dará la señal de evacuación del centro en caso de producirse esa situación (algo que estará perfectamente recogido en el plan de evacuación como veremos más adelante). Todos los paneles/centrales tanto de detección como de extinción deben disponer de sus propias baterías con una autonomía mínima de 8 horas. El sistema debe dotarse de los avisadores acústicos y luminosos necesarios para que nos permita manejar cualquier incidencia que se produzca para notificar, llegado el caso, a los usuarios que evacuen la instalación.

Las salas de equipamiento IT deberán estar protegidas frente a incendios externos a la misma, para ello deberán estar compartimentas y sectorizadas con respecto a otros usos.

Las salas eléctricas, por el riesgo que entrañan dichas instalaciones deberán estar compartimentas y sectorizadas con respecto a otros usos, para que en caso de incendio en una sala no se propague al resto del edifico.

Sistema de extinción automática

Las salas IT y salas eléctricas deberán disponer de un sistema de extinción automática mediante Gas. El sistema se basará en una batería de cilindros, con un cilindro maestro equipado con válvula activada eléctricamente por solenoide o manualmente por medio de disparo manual. La descarga del gas se realizará en el falso suelo y en el ambiente. Para la descarga del gas uniformemente en la sala, se dispondrá de una red de tuberías y difusores distribuidos tanto en ambiente como por el suelo técnico.

Esta instalación está formada en un sistema de detección conectado a una central de control que activa una sirena de alarma y activa automáticamente una electroválvula que contienen el agente extintor presurizado el cual se descarga en el recinto mediante una red de difusores.

Para que el sistema sea eficaz y garantice la máxima protección de los bienes del recinto, la descarga tiene que efectuarse en pocos segundos y se tiene que mantener confinado para garantizar que el incendio se extingue y no vuelve a reavivar.

El sistema será comandado por una central de extinción ubicada en el exterior de sala, dicha central incorporará baterías para autonomía y una placa/modulo con relés auxiliares.

El sistema tendrá pulsadores de bloqueo/paro y de disparo en caso de emergencia a la entrada de la sala IT del Centro de Datos, de manera que en caso de aviso de disparo intempestivo sea posible la interrupción del aviso de disparo al panel de control del sistema de extinción, o en caso de fallo del sistema automático de disparo el pulsador de emergencia para disparo permita su activación por simple actuación de una persona. Habrá letreros luminosos que podrán activarse en caso de aviso de disparo; dichos letreros están ubicados junto a dintel de puerta de acceso.

La actuación del sistema de extinción está programada para una detección cruzada. Es decir, el comienzo de la extinción se realizará cuando entren en alarma dos detectores.

Hoy en día es conveniente disponer de un sistema precoz de detección de humos (el más común es el del fabricante VESDA, pero hay más en el mercado) que son sistemas muy sensibles y nos ponen en alerta ante cualquier pequeño indicio de posible incendio y por tanto permiten actuar en la fase más incipiente permitiendo reaccionar rápido y garantizar el éxito de sofocarlo a tiempo. Indicar que la central principal de detección tiene que tener comunicación con sistemas que tengan que reaccionar de algún modo ante una evacuación, por ejemplo, mandando señal al sistema de control de accesos para que libere todas las puertas, de la ruta de evacuación, que se gestionen bajo dicho sistema y haciendo que los ascensores (en caso de disponer de ellos) dejen de funcionar y vayan directamente a la planta principal quedándose abiertos.

Con respecto a las posibles soluciones para el sistema automático de extinción debemos indicar que son muy variadas (Novec 1230 (FK 5-1-12), FM200 (HFC 227ea), ProInert (IG55), Inergen (IG541), Argonite (IG55) …), y por tanto hay que analizar las disponibles en cada país, para evitar costos futuros en su mantenimiento. El sistema automático debemos contemplarlo en la sala de equipamiento IT principalmente, y podemos evaluar teniendo en cuenta los recursos económicos disponibles si fuese recomendable en alguna sala técnica, como la que ocupen las UPS y la de las baterías asociadas a ellas.

Aspectos a tener en cuenta en la elección del gas extintor para un Centro de Datos:

- No debe ser dañino para el medio ambiente.
- No debe tóxico ni peligroso para las personas.
- Debe proteger los bienes que contiene el local.

*Catalogado como Agente limpio**.*

**Agente limpio: Sustancia extintora que tiene como características las siguientes:
No es conductora de la electricidad
No daña equipo electrónico/Eléctrico
No deja residuos
Permite que una vez aplicada y controlado el incendio se pueda restaurar el funcionamiento del área protegida rápidamente (no se requiere limpieza)
No corrosivo

CONDICIÓN	INERGEN			NOVEC			FM-200			ARGONITE			ECARO 25		
	NO RECOMENDADO	SE PUEDE USAR	RECOMENDADO	NO RECOMENDADO	SE PUEDE USAR	RECOMENDADO	NO RECOMENDADO	SE PUEDE USAR	RECOMENDADO	NO RECOMENDADO	SE PUEDE USAR	RECOMENDADO	NO RECOMENDADO	SE PUEDE USAR	RECOMENDADO
AMBIENTE OCUPADO			■		■			■		■				■	
AMBIENTE OCUPABLE			■		■			■		■				■	
AREA NO HERMETICA			■		■			■				■		■	
AREA HERMETICA		■				■		■							
POCO ESPACIO PARA CILINDROS	■					■		■		■				■	
SE DESEA EVITAR DAÑO AMBIENTAL			■			■	■				■		■		
ALTO RENDIMIENTO TERMICO		■				■		■			■			■	
SISTEMAS DE DETECCION EXISTENTES			■			■		■			■			■	
PROBADO EN HUMANOS			■	■	■	■	■	■	■	■	■	■	■	■	■
FACIL RECARGA			■			■		■		■				■	
GARANTIA AMBIENTAL DE 20 AÑOS			■			■	■			■			■		

	HFC 227 ea (FM 200)	FK 5-1-12 (NOVEC 1230)	IG-541 (INERGEN)
PROBADO EN HUMANOS @ CONCENTRACION DE DISEÑO SIN EFECTOS ADVERSOS	NO	NO	SI
CONCENTRACIÓN MAXIMA DE DISEÑO	7,40%	4% - 6%	37,80%
NOAEL	9,00%	10%	43,00%
LOAEL	10,50%	>10%	52,00%
MARGEN DE SEGURIDAD	**3 - 20%**	**67 - 150%**	**14,00%**

Figura 9 Comparación de agentes limpios en cuanto a Seguridad en humanos.

Fuente: Prodeseg

El factor de seguridad del Novec sobre el FM200 es de hasta el 150% versus apenas 20 de este último. Este factor de seguridad tan alto del NOVEC garantizar la supervivencia de personas en los recintos en caso de descarga accidental.

Igualmente, el Inergen, al ser el único agente probado en humanos, se constituye en un gas inocuo para los seres vivos si están en un recinto con Inergen como atmosfera.

Es importante realizar una prueba de estanqueidad de la sala donde tengamos la instalación de extinción automática para evaluar su efectividad en caso de disparo. Dicha prueba (DFT—Door Fan Test) debemos realizarla antes de poner la instalación en fase de producción y cada vez que realicemos algún cambio sustancial (relacionado con aberturas y paso de cables principalmente) en la sala de equipos IT.

Hay que tener muy alineado y concienciado a todo el personal que entre y trabaje dentro de nuestro centro de datos para evitar que se introduzcan materiales combustibles (papel, cartón, etc.). En función del tamaño del centro de datos se debe o no considerar la disponibilidad de un grupo de presión de incendios para garantizar la presión en las distintas Bocas de Incendio Equipadas (BIEs) que pudiéramos considerar instalar, así como un aljibe de agua que nos permita tener garantizada la autonomía de dicho recurso en caso de falta de abastecimiento de la red de distribución justo el día que se pudiese producir la necesidad de usarla.

Sistema manual de extinción de incendios

Se dispondrán de extintores portátiles.

- General: extintores portátiles de eficiencia 21-113B
- Salas de equipamiento eléctrico: extintores portátiles de 5 Kg. de CO_2.

Sistemas de seguridad física

Asegurar físicamente las instalaciones, equipamiento y bienes reviste una gran importancia a la hora de ayudar a reducir posibles intrusiones en los lugares donde se encuentran los Centros de datos. Por tanto, es de vital importancia que el personal de seguridad restrinja el acceso, permitiendo únicamente el del personal y vehículos autorizados, por ejemplo, mediante el despliegue de soluciones de reconocimiento automático de número de matrícula (ANPR, Automatic Number Plate Recognition) en cada zona de acceso de vehículos.

La tecnología ANPR, cuando se combina con un **CCTV** (Circuito Cerrado de TV) de alta definición en cada punto de acceso, se convierte en un método efectivo para controlar el flujo de vehículos y personal desde y hacia la zona en donde se encuentra el centro de datos. Las cámaras de CCTV HD son capaces de hacer barridos y zoom sobre eventos específicos en cada punto de acceso proporcionando una imagen más clara de cualquier actividad sospechosa. La tecnología CCTV HD ofrece una mayor calidad de detalle en comparación con tecnologías CCTV antiguas, mejorando notablemente la calidad de las imágenes y haciéndolas aptas para fines como el reconocimiento facial. Este nivel de detalle significa también que los análisis post-evento se puedan realizar más rápido; permitiendo a los investigadores analizar y procesar la información de manera más eficiente y precisa en caso de problemas. Los registros electrónicos de fecha y hora permiten una búsqueda más rápida y precisa de la información archivada para la policía o personal de seguridad en caso de llevarse a cabo investigaciones criminales.

Los grabadores que soporten el sistema de CCTV deben estar alojados en el centro de seguridad donde se encuentra el puesto del vigilante de seguridad (zona que debe tener una alta restricción de acceso). El grabador debe disponer de mínimo 16 canales y las imágenes de las cámaras deberán grabarse con una ratio de 6fps. Asimismo, la unidad debe tener una capacidad para poder almacenar imágenes con una resolución de tipo D1, durante por lo menos un mes completo (31 días).

Todos los elementos asociados, como por ejemplo las cámaras interiores y exteriores, deben ser seleccionadas en base al tamaño del centro de datos y considerando fabricantes de primeras marcas que tengan presencia propia en el país.

El sistema deberá estar basado en tecnología IP-POE con al menos un videograbador de red de 6TB y sistema de almacenamiento adicional de 8TB. La gestión en tiempo real y del material almacenado se realizaría desde un ordenador central a través del software de gestión específico.

En cuanto al sistema de **control de accesos**, debemos tener presente que será preciso utilizar un sistema que nos permita generar distintos perfiles de cara a facilitar el acceso a las distintas zonas del edificio. Respecto a las salas técnicas donde se alojarán los sistemas de infraestructuras técnicas (transformadores, cuadros de conmutación, UPS, baterías, producción de climatización, etc.) suelen mantenerse siempre cerradas con llaves específicas de seguridad gestionándose mediante un procedimiento de solicitud de dichas llaves en caso de necesitar su acceso. Es un método fiable para controlar quién accede a la vez que cumplimos y velamos por tomar las máximas medidas en materia de Seguridad y Salud.

Como ya se ha comentado en algún otro apartado, este sistema debe permitir liberar todas las puertas que gestiona y pertenezcan a una ruta de evacuación de la instalación, ante una situación de emergencia que genere una evacuación.

El control de accesos al Centro de Datos, debido a la criticidad de los procesos de negocio ejecutados en su interior, así como a la información que se mantiene en el mismo, se prestará especial importancia a los controles establecidos para gestionar y monitorizar el flujo de personas y materiales. Para ello se desarrollarán e implantarán procedimientos y tecnologías que permitan a modo de ejemplo:

- Gestión de accesos y habilitaciones, que permita administración delegada y definición de perfiles.
- Eliminar o limitar al mínimo la intervención humana sobre los controles.
- Asegurar la identificación y autenticación del personal impidiendo entradas no autorizadas e intentos de acceso fraudulento.
- Posibilidad de gestión completa (horarios, rutas, …)
- Asegurar la información en tiempo real de todos los eventos.
- Posibilidad de determinar de un modo automático las personas presentes ante una necesidad de evacuación por emergencia (cuantos y donde).
- Posibilidad de ampliar las opciones de gestión
- Control de presencia / horario.

- Control de visitas.
- Control de acreditaciones.
- Gestión de rondas.
- Mantenimiento de niveles de seguridad ante pérdida de tarjetas.
- Posibilidad de generación de informes, listados, estadísticas…

Se debería disponer de un sistema de control de accesos en los accesos principales al edificio y a las salas críticas. No sería necesario en salas no criticas como la cocina/office, los aseos/baños, salas de reuniones, etc.

El sistema de control de accesos debe permitirnos disponer de un servidor central desde el cual gestionar y operar otros sub-sistemas que tengamos en distintas ubicaciones, para poder ir creciendo en el tiempo y poder apoyar desde el puesto de seguridad de uno de los Centros de Datos a otro que tengamos en otra localidad (existe software específico a tal efecto como por ejemplo el Borer Fusion).

Intercomunicadores de audio y video es recomendable disponer en las puertas de acceso al perímetro de nuestro centro de datos, tanto de personal como de vehículos, para que el vigilante de seguridad pueda gestionar el acceso de visitas, clientes y proveedores de una manera ágil y segura.

Como complemento a todo lo expuesto la recomendación sería instalar un **sistema de detección de intrusión** mediante volumétricos, sensores en puertas y detectores ubicados en distintos puntos estratégicos de la instalación. El panel central de este sistema debe disponer de sus propias baterías con una autonomía mínima de 12 horas.

Adicionalmente se recomienda una serie de medidas que son una buena práctica en la mayoría de los Centros de datos de todo el mundo y que facilitan no solo la seguridad del centro sino también el correcto acceso de colaboradores y clientes a la instalación. Estos aspectos pasan por disponer de una **doble valla perimetral de seguridad,** así como **puertas giratorias** vinculadas al sistema de control de accesos para el paso de las personas dentro del edificio. Todo ello apoyado en un servicio de **vigilantes de seguridad** con presencia 24x7.

Tengamos presente que la altura por planta de suelo a techo debe ser de 5m o mayor. Y que se debe considerar que exista espacio en el exterior o en la terraza del edificio para los equipamientos y sistemas que allí tenemos que alojar (un tamaño razonable para un centro de datos medio puede ser 800m2).

Todos los sistemas de seguridad tienen que estar procedimentados con el propósito de que el vigilante de seguridad actúe según las pautas establecidas. Deben ser documentos claros y concisos para que las indicaciones sean concretas evitando con ello interpretaciones.

GMAO

Para poder gestionar el día a día en la operación de todos los sistemas y las infraestructuras técnicas, y que además tengamos un punto donde quede recogido todo el plan de

mantenimiento cuando hay que hacerlo, tanto en caso de revisiones obligatorias por la legislación que corresponda, como por recomendaciones y procesos propios, y poder facilitar que todo fluya, es muy recomendable implementar alguna herramienta GMAO (Gestión del Mantenimiento Asistido por Ordenador). Nuevamente debemos mencionar que hay multitud de opciones en el mercado y el principal criterio de selección debe ser usar una que tenga soporte local en Paraguay.

BMS

Otro sistema que va a ser fundamental durante toda la operación del centro de datos es el sistema BMS o sistema de gestión de nuestro edificio. La principal función que nos va a permitir es recoger los estados y alarmas de todas nuestras infraestructuras técnicas de cara a que siempre conozcamos el estado de nuestra instalación. La mayoría de estos sistemas nos pueden enviar correos electrónicos o SMS cuando se produzca un evento/alarma, además de permitirnos una conexión Web a nuestro sistema para que podamos ver en cualquier momento qué está ocurriendo en la instalación desde otra ubicación. Existen bastantes soluciones y fabricantes en el mercado de manera que lo principal es evaluar a aquellos que tienen presencia física en Paraguay (de cara a que los costos futuros de mantenimiento o incluso a posibles actuaciones de reparación o mejora del sistema, sean lo más económicas posibles). Importante también es que se basen en Protocolo abierto.

El sistema no deberá realizará tareas de control sobre ningún elemento de la instalación.

El sistema estará basado en cuadros de control distribuidos con lógica residente en controlador local, de forma que se permita la realización de tareas de mantenimiento concurrente al sistema sin afección a los procesos críticos.

Los cuadros de control deberán contener todos los controladores, pasarelas, módulos Entradas/Salidas necesarios para la recepción de señales digitales y analógicas, integraciones de los principales equipos mediante Modbus o pasarela similar.

El sistema incluirá todos los elementos de campo como sondas de presión, sondas de temperatura, sondas de humedad, etc.

Control de salas eléctricas:

Permite la integración de los estados y disparos de celdas de media tensión, los interruptores automáticos críticos del sistema de protección y distribución en baja tensión del bloque eléctrico. Integra mediante protocolo Modbus el sistema de transferencia, generadores, sistema SAI, medidores de energía, así como las unidades CRAC de refrigeración de la sala eléctrica.

Control de la sala IT:

Permite la integración de las sondas de temperatura/humedad de pasillos fríos y calientes, integración mediante Modbus de los PDUs y unidades de climatización CRAC.

El sistema incorporará un software que facilitará, al menos, 7 informes fundamentales referidos al comportamiento energético del edificio, a saber:

Visión general

Este informe mostrará los datos en formato tabla, diagrama de barras y/o gráfico de queso/tarta, dando una visión global de los consumos para cada tipo de energía (eléctrica, gas, etc.) por edificio o zona. Los consumos de cada tipo de energía serán normalizados para tener una unidad de comparación única.

Consumo

Será un informe similar al descrito anteriormente, pero referido a periodos de tiempo concretos y definidos por el usuario, efectuando asimismo gráficos comparativos inter-periodos.

Energía eléctrica

Estos informes se centrarán en la energía eléctrica pero no sólo focalizándose en el consumo sino también en otros parámetros, picos de demanda, potencia reactiva, factor de potencia del sistema, etc., utilizando asimismo gráficos amigables.

Producción

En estos informes se facilitará información sobre los puntos identificados como de producción de energía frente al consumo energético, facilitando, asimismo, factores de eficiencia en cada periodo.

Costos energéticos

En estos informes se calcularán los costes energéticos, de acuerdo a un formato definido por la propiedad, en la que habrá que actualizar costos de la energía. Asimismo, se facilitarán los datos en formato gráfico para poder efectuar comparativas de manera rápida y sencilla

Perfil de carga

Informes enfocados al perfil de demanda diaria de energía, proporcionando una información clave para definir estrategias que permitan minimizar y/o eliminar los picos de demanda.

Funcionamiento de equipos

Estos informes estarán enfocados a conocer las horas de funcionamiento de los equipos, así como conocer el número de arranques de los mismos y se podrán efectuar para periodos determinados de tiempo. Estos informes serán muy útiles para el mantenimiento preventivo de los mismos.

La pérdida de un componente de la red no interrumpirá el funcionamiento del control de otros dispositivos, conforme a un control totalmente distribuido.

Visualización de datos:

La finalidad del sistema de control y gestión del edificio es facilitar la tarea de operar y mantener el edificio y las instalaciones que componen la infraestructura de producción y distribución.

Para ello se hace necesario crear una serie de pantallas de visualización de datos que permitan interactuar de forma fácil y cómoda con el sistema.

Se presentan en este apartado algunas de las pantallas que deberían formar parte del puesto de control, aunque los detalles y peticiones asociados a estas pantallas deberán efectuarse en fase de licitación y ejecución junto con la SENATICs.

PUE

La métrica PUE (Power Usage Effectiveness) mide la eficiencia de la instalación en términos de kW TOTALES por cada Kw TI consumido.

Por lo tanto, es interesante desde el punto de vista de eficiencia energética, disponer de un gráfico histórico de la evolución del PUE para poder evaluar el impacto de acciones de mantenimiento o mejoras realizadas a lo largo de la vida del Centro de Datos.

Desglose de consumos

Es interesante poder evaluar los distintos consumos de los sistemas instalados frente al total de consumo del edificio, y frente al consumo de TI.

Ya que se dispone de analizadores de redes integrados al sistema de control en todos los cuadros eléctricos secundarios, es una tarea fácil elaborar un gráfico donde se muestre la evolución de los consumos parciales de cada instalación o parte de la instalación (Producción, Bombeo, Tratamiento de aire, etc.).

Infraestructura eléctrica

A través de los correspondientes esquemas sinópticos señalizar el estado de funcionamiento de cada uno de los bloques eléctricos (Red / Grupo), estado de las conexiones de potencia principales, consumos de los distintos elementos, etc. De una forma intuitiva y gráfica, debiéndose señalizar en colores verde y rojo los cierres y aperturas de interruptores.

Infraestructura de climatización

De forma similar a la infraestructura eléctrica, los distintos esquemas sinópticos deberían señalizar el estado de funcionamiento del sistema de producción, distribución y trasiego de aire de forma intuitiva y gráfica.

Infraestructura de fuel

De forma similar al resto de infraestructuras críticas, los distintos esquemas sinópticos deberían señalizar el estado de funcionamiento del trasiego de fuel, capacidades de depósitos, etc. de forma intuitiva y gráfica.

Condiciones eléctricas y de climatización en sala

A través de las integraciones en interruptores automáticos y de las sondas de control de temperatura y humedad, deberá ser posible visualizar de forma fácil las condiciones en las que se encuentra la sala de servidores.

Solución DCIM

Hoy en día una de las tendencias principales en cualquier Centro de Datos y especialmente en todos los de nueva construcción es la implantación de una solución DCIM para el Manejo de

las Infraestructuras del Centro de Datos (de sus siglas en inglés Data Center Infrastructure Management), que se trata de una plataforma que permite:

1. Mitigar el riesgo de IT

* Minimizar el riesgo de cambio al reconocer fácilmente las dependencias.

* Aumentar la precisión con un inventario de activos en tiempo real.

* Controlar automáticamente y responder a los eventos para asegurar la disponibilidad

* Aumentar la seguridad con control completo sobre el acceso a todos los activos del centro de datos

2. Optimizar la eficiencia

* Consolidar la gestión de Centros de datos con una única fuente de datos para instalaciones y TI.

* Obtener una profunda perspectiva de la capacidad para maximizar el uso y posponer gastos de capital.

* Modelar el efecto de cambio para mejorar la disponibilidad y el rendimiento.

* Mejorar los márgenes operativos con una gran precisión en la planificación y la ejecución

3. Respaldar iniciativas futuras

* Respaldar crecimiento y cambios en el modelo de funcionamiento con una perspectiva precisa del uso actual y la capacidad de modelar el impacto del cambio.

* Aumentar la flexibilidad y la resiliencia de la infraestructura con seguimiento en tiempo real de tendencias y cambios históricos.

* Optimizar la gestión de la carga de trabajo y los procesos con una vista unificada de los activos de las instalaciones y de IT.

Con este sistema el equipo gestor del Centro de Datos tendrá una capacidad de gestión integral del mismo que:

1. Gestión de Tecnologías de la Información (TI)

* Garantice que se tengan en cuenta las interdependencias en un único punto para la evaluación de infraestructuras.

* Realice el inventario automático de todos sus activos con un esfuerzo manual mínimo o inexistente.

* Controle los cambios con análisis de tendencias y datos de carga en tiempo real de "antes y después".

2. Gestión de instalaciones informáticas

* Realice un diagrama de su centro de datos de extremo a extremo para identificar oportunidades de aumento de la eficiencia y el uso.

* Analice las cargas actuales en tiempo real y modele los cambios propuestos para asegurar la disponibilidad y reducir costos.

* Realice el seguimiento de dónde va exactamente la alimentación y por qué, para poder optimizar la alimentación y la refrigeración.

* Aproveche eficiencias ocultas con procesos automatizados para ajustar el equipo de alimentación y refrigeración.

3. Gestión ejecutiva de Centros de datos

* Otorgue poder a su equipo con datos completos en tiempo real, esquemas y modelados de capacidades para una planificación más inteligente y control de cambios.

* Comprenda dónde se implantan sus recursos y cómo se usan para recuperar capacidad sin explotar y planificar con precisión necesidades de capacidad.

* Mejore de forma continua la colaboración y la comunicación con conocimientos compartidos sobre la interrelación entre los activos de TI y de las instalaciones.

* Planifique sus necesidades futuras mientras respalda las iniciativas actuales.

4 Recomendación de ubicaciones de los Centros de Datos

A la hora de seleccionar una ubicación de un nuevo Centro de Datos se tendrán en cuenta los siguientes requisitos:

- Protección de la zona elegida frente a amenazas exteriores.
- Facilidad de acceso a la zona.
- Disponibilidad de acceso a múltiples operadores de telecomunicaciones
- Facilidad de crecimiento.

A continuación, se enumeran las amenazas cuya materialización impactaría negativamente en la operativa de los sistemas ubicados en un Centro de Datos, y que, por tanto, deberán considerarse en la evaluación de la zona:

- Proximidad de materiales inflamables
- Polución
- Interferencias Electromagnéticas
- Naturales: Vibraciones, Inundación, Terremotos, etc.

Empezaremos por indicar que debemos evaluar la proximidad a subestaciones eléctricas desde las cuales se obtendrá el suministro eléctrico. Siempre que sea posible que estén a una distancia razonable para que los costos de la acometida de la compañía eléctrica (en caso de necesitar realizarse nueva) no sean muy elevados.

Por la importancia de facilitar la interconexión con redes existentes y futuras se recomienda, como uno de los principales requisitos, que el futuro Centro de datos se encuentre ubicado en las principales ciudades, y lo más próximo posible a infraestructuras existentes de fibra óptica, tanto propias como de otros operadores para facilitar la interconexión de redes. Indicar que en caso de que no estén aún desarrolladas, una buena referencia son las previsiones o proyectos de centros tecnológicos o de concentración de empresas multinacionales dado que, tarde o temprano, llegarán las redes de fibra óptica hasta los mismos.

No debe estar cerca de ningún almacenamiento de productos peligrosos, inflamables o combustibles; tampoco donde existan empresas productoras de elementos contaminantes, ni en las inmediaciones de estaciones de servicio (gasolineras), centrales nucleares, líneas de alta tensión, antiguos cauces de ríos y arroyos, volcanes activos, etc.

Siguiendo con las restricciones, no debe situarse dentro de un radio de 4,8 km/ 3 millas de la ruta de despegue o aterrizaje de vuelos. Esto evitará dos cuestiones principales: el riesgo de posibles colisiones, así como evitar los efectos de las emisiones de la aviación sobre las instalaciones exteriores de nuestro centro de datos.

En el mismo sentido la ubicación no debe estar a menos de 250m de una vía de ferrocarril ni de una vía principal de carreteras (dos carriles o más por sentido). Tampoco debe colocarse en

zonas donde debajo pasen rutas de transporte subterráneo (tipo metro o suburbano). Y finalmente el sitio no debe estar situado en la vecindad inmediata de un edificio o área que pueda ser un probable objetivo militar o de ataque terrorista.

Por otro lado, es preferible que el centro de datos no esté demasiado lejos de los aeropuertos para facilitar la comunicación y visitas de empresas y técnicos colaboradores. Por tanto, se sugiere que no esté más lejos de 20km de un aeropuerto.

Se debe mirar que la construcción del centro de datos no genere ningún tipo de impacto ambiental en la zona de ubicación, ni por nivel sonoro de los equipos que se instalen dentro o fuera del edificio (terraza o perímetro) ni por el impacto visual de dichos equipos allá donde puedan verse desde el exterior.

En la ubicación que se decida, debe poder construirse un vallado de seguridad en todo el perímetro exterior, de manera que debemos contar con el mismo, y en caso de que pensemos que van a tener que acceder vehículos de cierto tamaño (como camiones para entrega de equipamiento, futuros reemplazos de equipos, etc.) habrá que considerar los radios de giro necesarios para que se pueda facilitar dichos accesos. Los caminos, puentes y carreteras desde las vías principales hasta la ubicación definitiva del centro de datos deben también tenerse en cuenta, dado que pueden suponer gastos muy elevados si hay que superar dificultades adicionales con el transporte de material.

4.1 Amenazas exteriores

Como indicábamos anteriormente un paso fundamental para evaluar de la idoneidad de una zona consiste en obtener toda la información en cuanto a posibles amenazas exteriores.

El mayor riesgo natural en muchos países son los terremotos.

En un escenario ideal, se deberá ubicar el Centro de Datos en una zona con riesgo cero. Como siempre pueden surgir amenazas naturales no controlables, lo ideal es disponer de un centro de datos de respaldo ubicado en una localidad diferente a Asunción.

Principales causas sismogenéticas en el Paraguay son:

1. Subducción de la Placa de Nazca por debajo de la Placa Sudamericana, generando eventos de moderadas magnitudes (Región del Chaco Paraguayo)

2. Eventos intraplacas, asociados a fallas geológicas que presentan actividad (Región Oriental)

Figura 10 Epicentros de los últimos eventos sísmicos sentidos en Paraguay

Fuente: Geología del Paraguay

Como ya se ha mencionado anteriormente la propuesta se basa en un Centro de Datos en Asunción, en las antiguas caballerías del Ejército.

Es fácil que algunos de los servicios que se vayan a prestar precisen de la necesidad de colocar equipamiento de respaldo en otro centro de datos (idealmente en otra zona del país). Lo aconsejable es que exista una distancia significativa entre las dos ciudades para asegurar que cualquier desastre en una zona no tenga la misma magnitud en la otra.

Un centro de datos destinado a la computación en la nube puede ser un elemento principal para la continuidad de negocio de los organismos y empresas que utilicen dicho servicio.

En la actualidad los sistemas que maneja un Centro de Datos están diferenciados de la siguiente forma, desde el punto de vista de las empresas que contraten dichos servicios:

- Sistemas críticos para el negocio:
  Cualquier fallo en el sistema, ya sea provocado por fallos, desastres y errores humanos, influye en la operativa de la empresa, y en la continuidad del negocio de la misma. Por ello el Centro de Datos debería tener un mínimo de robustez que garantice una continuidad en labores de mantenimiento y una continuidad contra incidentes de gran magnitud. Disponibilidad de un DRP (Disaster Recovery Plan -- Plan de Recuperación ante Desastres) por parte de la empresa para asegurar la operación de forma continua. En caso de desastre la operación de la empresa se realizaría desde un DRC (Disarter Recovery Center -- Centro de Recuperación de Desastres), y solo se habría perdido la información que estaba siendo trasmitida en el momento del fallo.

- Sistemas importantes para la operativa:
  En situaciones críticas dichos sistemas pueden dar una espera mayor para su recuperación, es decir son necesarios para la operativa, pero no para la continuidad inmediata del negocio de la empresa.
  Cualquier fallo en el sistema, ya se provocado por fallos, desastres y errores humanos, influyen en la operativa del grupo, pero no en la continuidad del negocio. En caso de prolongación temporal en la restitución del sistema, este puede llegar a ser crítico en la continuidad del negocio. Por ello el Centro de Datos debería tener un mínimo de robustez que garantice una continuidad en labores de mantenimiento y una continuidad contra incidentes de gran magnitud.

- Sistemas no críticos para la operación:
  Cualquier fallo en el sistema, ya se provocado por fallos, desastres y errores humanos, NO influyen en la operativa de la empresa. En caso de prolongación temporal en la restitución del sistema, este puede llegar a ser crítico en la operativa pero no en la continuidad del negocio.

Los sistemas y la criticidad de ellos, será según la definición de dichos servicios por parte de las empresas que los requieran.

Para sistemas críticos en las continuidades de negocio, según la tipología, los sistemas entre el Centro de Datos principal y el Centro de Datos de respaldo debe ser Copias Síncronas de los sistemas críticos, de esta forma se asegura que todo dato escrito en el Centro de Datos principal también se escribe en el DRC (Centro de Recuperación de Desastres) antes de continuar con cualquier otra operación.

El Centro de datos debe tener un mínimo de robustez que garantice una continuidad en labores de mantenimiento y una continuidad contra incidentes de gran magnitud.

Aunque la ubicación no es un elemento que actualmente pueda considerarse como determinante, para la futura certificación del Centro de Datos como Tier III, tanto en materia de **Diseño** como de **Construcción**, sí que hay que tener presente que la parcela que se está considerando para la ubicación del nuevo Centro de Datos (una superficie de 63.173,40 m² en las antiguas caballerías del Ejército), la proximidad a la estación de servicio (gasolinera) y al aeropuerto quedan recogidos como elementos no aconsejables por *Uptime Institute*[2] para la ubicación de un Centro de Datos y podrían requerir justificar medidas específicas sobre dichos riesgos si en algún momento se considerase el llegar a certificar el Centro de Datos en la parte de **Sostenibilidad Operativa**.

[2] Organización imparcial de asesoramiento centrada en mejorar el rendimiento y aumentar la eficiencia y la fiabilidad de la infraestructura crítica de las empresas mediante la innovación, la colaboración y las certificaciones independientes.

Se adjuntan detalles de las tablas de la organización *Uptime Institute* que definen los requisitos de la certificación TIER en Sostenibilidad Operativa de Uptime donde se ven reflejadas estas consideraciones:

Uptime Institute®

Categoría Riesgo de desastres naturales	Nivel de riesgo [1]	
Componente	**Más alto**	**Más bajo**
Inundaciones (río, lago, embalse, canal, estanque, etc.) y tsunami [2]	Llanura de inundación de < 100 años	Llanura de inundación de > 100 años
Huracanes, tornados y tifones	Alto	Medio
Actividad sísmica [3]	> 0,8 m/s²	< 0,8 m/s²
Volcanes activos	Alto	Medio

Tabla 3.1 Ubicación del sitio: categoría Riesgo de desastres naturales

Categoría Riesgo de desastres causados por el hombre	Nivel de riesgo [1]	
Componente	**Más alto**	**Más bajo**
Aeropuerto/aeródromo militar	A < 3 millas de cualquier pista de aterrizaje activa; dentro de una extensión de pista de 1 x 5 millas	A > 3 millas de cualquier pista de aterrizaje activa; fuera de una extensión de pista de 1 x 5 millas
Exposiciones a propiedades colindantes	Planta química, fábrica de fuegos artificiales, etc.	Edificio de oficinas, área no desarrollada, etc.
Corredores de transporte	< 1 milla	> 1 milla

Tabla 3.2 Ubicación del sitio: categoría Riesgo de desastres causados por el hombre

[1] El nivel de mitigación implementado reducirá el posible impacto en las operaciones.

[2] Evaluación de riesgos a partir del mapa de llanuras de inundación local o regional o el equivalente internacional.

[3] Aceleración máxima del suelo (metros por segundo al cuadrado [m/s²]) que se puede esperar en los próximos 50 años con una probabilidad del 10 %.

Categoría Elementos de construcción		Aplicable al Tier			
Componente	**Comportamiento**	**I**	**II**	**III**	**IV**
Construcción dedicada	1. Centro de datos de construcción dedicada			✓	✓
	2. Instalación con finalidad exclusiva para respaldar operaciones del equipo de TI			✓	✓
	3. Edificio independiente separado físicamente de otras instalaciones corporativas del sitio			✓	✓
	4. Centro de datos construido según los estándares superando los códigos de construcción de jurisdicciones locales para garantizar la continuidad de las operaciones tras un desastre natural			✓	✓
Espacios de soporte y especializados	1. Espacio adecuado separado de la sala de cómputo para la recepción, el almacenamiento, el almacenamiento temporal, la construcción y la realización de pruebas de hardware de TI		✓	✓	✓
	2. Espacio adecuado separado de la sala de cómputo para las siguientes funciones: • Centro de control de BMS/sistema de automatización de edificios (BAS) • Centro de comando/recuperación ante desastres • Almacenamiento de piezas y herramientas • Actividades del taller de ingeniería e instalaciones • Reuniones y formación			✓	✓
Seguridad y acceso	1. Acceso controlado a todas las salas de cómputo y los espacios de soporte		✓	✓	✓
	2. Acceso controlado a los edificios			✓	✓
	3. Revisión periódica de los accesos			✓	✓
	4. Acceso controlado al sitio				✓
Distancias mínimas	1. Espacio adecuado alrededor del centro de datos para minimizar impactos en instalaciones adyacentes			✓	✓

Tabla 2.2 Características de la construcción: categoría Elementos de construcción

Figura 11 Requisitos de la certificación TIER en Sostenibilidad Operativa

Fuente: Uptime Institute

5 Propuesta del Centro de Datos

A la hora de plantear la construcción del nuevo Centro de Datos previsto por la SENATICs debemos tener muy presente algunos aspectos fundamentales.

El primero es que el nuevo Centro de Datos será dedicado para soportar servicios a órganos y estamentos gubernamentales.

Hoy en día existen múltiples posibilidades para desarrollar la construcción de un nuevo Centro de Datos.

Quizá la primera de las cuestiones a considerar es si debemos construir un Centro de Datos in situ (o de manera tradicional) en la ubicación que se acuerde por la SENATICs o si por el contrario elegimos la opción de desarrollar una solución modular.

Desde Networld Consulting se recomiendo la **propuesta modular** basándonos en los siguientes beneficios:

- El tiempo de construcción se reduce respecto a una construcción tradicional realizada in situ, con el consiguiente ahorro de costos. Si además comparamos con utilizar un espacio dentro de un edificio existente, ello genera muchas más indefiniciones y detalles a solventar sobre la marcha, según van surgiendo durante el desarrollo de los trabajos.
- Se puede diseñar para cumplir la clasificación TIER III solicitada por la SENATICs para el Centro de Datos. Pudiendo obtener certificados sobre el diseño y la construcción del mismos. Algo que siempre le va a dar valor y reconocimiento internacional.
- Se pueden simular situaciones y condiciones extremas para garantizar el funcionamiento y operatividad del Centro de Datos antes de ponerlo en operación. Evitando con ellos riesgos para el servicio y ganando en reputación sobre las garantías de funcionamiento para los clientes que estén interesados en usar los servicios que se prestaran desde los mismos.
- La solución puede ser totalmente probada, y garantizar con ello el cumplimiento de los mejores y más exigentes estándares del mercado.
- Al ser un mercado aun por madurar y por tanto con no tantas empresas especializadas, se garantizará que expertos en las distintas materias y sistemas hagan la mejor instalación posible.
- Debemos tener presente que las instalaciones se diseñaran para trabajar de manera bastante automática y cuantas más pruebas se puedan hacer antes de ponerla en marcha nos ofrecerá mayores garantías sobre la forma en la cual se comportará ante imprevistos.
- Todos los cableados y elementos auxiliares pueden ser probados de antemano, evitando los múltiples problemas que suelen aparecer durante las instalaciones in situ,

y los consiguientes retrasos, que luego generan prisas para entregar las obras, lo que trae consigo que algunas cosas se hagan con menos calidad, etc.

Además, es importante tener presente:

- Se deben considerar de manera **preferente** a los fabricantes de los distintos sistemas y equipamientos a emplear, que tengan **presencia (con servicio técnico propio) en Paraguay**. Esto permitirá, además de apoyar a las empresas que invierten en Paraguay y que generan puestos de trabajo y riqueza en el país, garantizar que durante la vida útil de dichos equipos podamos recibir el soporte adecuado, así como un costo razonable de componentes y repuestos.

Teniendo en cuenta la localización del futuro Centro de Datos, así como los requisitos solicitados por SENATICs se ha decidido utilizar los siguientes parámetros de diseño:

* Intentar disponer de doble suministro en Media Tensión. Y a ser posible desde Subestaciones Eléctricas distintas. Una de las líneas debe ser dedicada y exclusiva para el Centro de Datos. Para lo cual debemos analizar la disponibilidad de dicha opción en las ubicaciones finales para el nuevo Centro de Datos

* Sistema de respaldo mediante Grupo Electrógeno y SAI (Sistema de Alimentación Ininterrumpida)

* Distribución en doble rama

* Temperatura exterior máxima 41ºC (ASHRAE)

* Tier III. Se acuerda con la SENATICs que es un diseño suficientemente robusto, siempre que se gestione con el personal y la formación adecuada a tal fin

Se propone la creación del Centro de Datos de forma modular, de esta forma se asegura una inversión inicial menor y posibilidad de crecimiento futuro sin interrupción del servicio.

El Centro de datos propuesto se puede desarrollar en dos fases, en dependencia del crecimiento y necesidades.

El hecho de optar por la solución modular reduce significativamente los aspectos constructivos a realizar en el propio emplazamiento, en cualquier caso, siempre se va a necesitar acondicionar el terreno y preparar la cimentación donde se asentará el futuro centro de datos, tal y como queda recogido en el desglose por partidas del presupuesto de inversión.

A continuación se exponen las diferentes partes de las que se compone la solución propuesta, ordenadas de la siguiente manera:

5.1 Exteriores

5.1.1 Losa de cimentación
5.1.2 Vallado perimetral
5.1.3 Estacionamiento de autos

5.2 Obra civil- Solución estructural

5.2.1 Distribución del centro de datos
5.2.2 Estructura exterior
5.2.3 Sala proveedores servicios (carriers)
5.2.4 Sala de telecomunicaciones
5.2.5 Sala IT
5.2.6 Salas UPS Y baterías
5.2.7 Almacén
5.2.8 Sala NOC
5.2.9 Sala CERT-PY
5.2.10 Sala de crisis
5.2.11 Sala de reuniones
5.2.12 Sala de capacitación y mantenimiento
5.2.13 Sala de guardia o seguridad
5.2.14 Muelle de carga/descarga
5.2.15 Sala coffee-cocineta
5.2.16 Baños

5.3 Solución potencia

5.3.1 Estructura del esquema unifilar
5.3.2 Equipos eléctricos principales
5.3.3 Distribución y organización de cableado
5.3.4 Protecciones eléctricas
5.3.5 Iluminación

5.4 Solución refrigeración

5.4.1 Estudio de la solución técnica
5.4.2 Equipos mecánicos para sala IT
5.4.3 Equipos mecánicos para sala UPS
5.4.4 Equipos mecánicos para sala baterías
5.4.5 Equipos mecánicos para sala NOC, sala CERT-PY, sala reuniones, sala crisis, puesto seguridad, mantenimiento y almacén

5.5 Sistemas adicionales

5.5.1 Sistema de control y supervisión
5.5.2 Control de acceso y vigilancia
5.5.3 Protección y extinción de incendios
5.5.4 Racks
5.5.5 Cableado de datos
5.5.6 Emergency Power Off (EPO)

5.6 Descripción de las fases de la solución propuesta

5.7 Gestión del proyecto

5.7.1 Ingeniería de apoyo
5.7.2 Project management
5.7.3 Controles de calidad
5.7.4 Planificación del proyecto

5.8 Certificación del proyecto

5.1 Exteriores

5.1.1 *Losa de cimentación*

Para garantizar la integridad del Centro de Datos en caso de seísmos se ha previsto realizar una cimentación por losa aligerada.

Las características y la preparación de la misma son:

- Excavación de rasa para losa de cimentación de suelo compacto mediante retroexcavadora hasta 2 metros de profundidad y transporte de tierras con camión.
- Relleno de material granular de piedra granítica (gravas), de 50 a 70 mm de grosor, en tongadas de 25 cm como máximo (debajo de losa de cimentación), colocación y compactación del mismo.
- Hormigón para losa de cimentación de 25 cm de canto (aligeramiento) HA-25/B/20/IIa de consistencia blanda y tamaño máximo del árido de 20 mm, desde camión, con una cuantía media de 25 kg/m^2.
- Hormigón para losa de cimentación de 40 cm de canto (aligeramiento) HA-25/B/20/IIa de consistencia blanda y tamaño máximo del árido de 20 mm, desde camión, con una cuantía media de 30 kg/m^2.
- Hormigón de limpieza para losa de cimentación, de espesor 10 cm HM-20/B/20/IIa de consistencia blanda y tamaño máximo del árido de 20 mm, desde camión.
- La tensión admisible media del terreno considerada de 1,5 kg/cm^2.
- La resistencia máxima a carga considerada es de 2.500 kg/m^2.
- Pendiente acorde para poder evacuar las aguas de lluvia hacia zonas seguras fuera del terreno y no se produzca acumulación.

Así mismo la zona que recoge el centro de datos y las instalaciones de apoyo debe disponer de una **valla perimetral de seguridad,** y también se dispondrá de **puertas giratorias** vinculadas al sistema de control de accesos para el paso de las personas dentro del edificio por los accesos principales.

5.1.2 *Vallado perimetral*

Para asegurar la protección contra intrusión del recinto se ha considerado la siguiente solución:

- Valla de alta seguridad especialmente diseñadas de un modo que no se puedan trepar ni cortar. La separación entre los centros de los alambres comprende 12,7 mm (vertical) x 76,2 mm (horizontal), impidiendo así el paso de los dedos y el empleo de cizallas, garantizando una seguridad plena.
- Estará constituida por paneles de **mallazo plano electrosoldado** constituido a partir de alambre de acero Tipo 5T22 (Norma UNE 36 089) de 4 mm de diámetro (AWG 8).
- La valla va sujeta a unos postes que son vigas tipo IPE 120 embutidas en dados de hormigón de 0,4 m x 0,4 m x 1 m. Pueden utilizarse además otros perfiles, como por ejemplo de W, dependiendo siempre de la altura de la valla y otros parámetros de

resistencia. Los paneles estándar de alambre de acero electrosoldado tendrán una altura de 4 m y una anchura máxima de 2,5 m.

- Puerta giratoria mecanizada formada por tres hojas de 2,20 cm de altura, de diámetro 2.000 mm. Puertas y cilindro de protección formadas por perfiles tubulares de acero. Acceso biométrico incluido.
- Puerta automática metálica corredera de una hoja o movimiento horizontal deslizante. Compuesta por una hoja de bastidor rectangular de barrotes. Costará de todas las medidas de seguridad fundamentales, sensor de detección de vehículos, indicador luminoso de funcionamiento, protecciones contra atrapamientos, etc. Con sistema de control de acceso incluido.

Figura 12 Puerta metálica corredera para acceso de vehículos

- Para la correcta gestión de las visitas, tanto el acceso peatonal como el de vehículos contaran con videoportero que comunicará con el puesto de guardia (seguridad.

Se contempla utilizar una solución terminada en color verde que genera un menor impacto visual en la zona.

5.1.3 *Estacionamiento de autos*

Se ha contemplado el acondicionamiento del recinto interior dentro del vallado de manera que se pueda transitar por el mismo con autos.

Así mismo además de los viales para el tránsito de vehículos o camiones con mercancías tanto durante la construcción como durante la operación del centro de Datos, se construirán varias

zonas de estacionamiento, con identificación de su uso: personal Centro de Datos, colaboradores y visitas.

Todos los vehículos deberán disponer en lugar visible de identificación de vehículo autorizado para su estacionamiento dentro del recinto.

El acceso al recinto está previsto realizarse mediante dos formas:

- Acceso peatonal: será el acceso habitual el cual dispondrá de una puerta giratoria que asegurará el acceso individual a la instalación y regulado mediante control de acceso biométrico.
- Acceso de vehículos: será utilizado únicamente para el acceso de vehículos y será una puerta corredera de al menos 3 m de ancho.

5.2 Obra civil- Solución estructural

El diseño del nuevo centro de datos ha sido definido desde adentro hacia afuera con los siguientes objetivos:

- Utilizar el eficientemente el espacio para reducir costes de estructura, y posibilitar la futura réplica y ampliaciones.
- Cumplir con las exigencias de seguridad y disponibilidad estipulados por la TIA-942.
- Cumplir con todas las exigencias del Uptime Institute a nivel de Tier III.
- Facilitar la operación y mantenimiento de la instalación.

5.2.1 *Distribución del centro de datos*

La estructura del Centro de datos ha sido concebida en dos partes:

- estructura interior.
- estructura exterior, envolvente de las salas interiores, que las protege de las inclemencias medioambientales (radiación solar, lluvia, viento…).

Adicionalmente en el exterior se encuentran algunos equipos que por su tipología y tamaño se prevén puedan estar situados en compartimentos separados en el exterior.

Así pues, la disposición de los diferentes equipos y salas en el Centro de Datos se ha realizado de la siguiente manera:

- Salas de proveedores de Telecomunicaciones: Serán dos salas independientes a las cuales llegarán los cableados de fibra óptica por rutas totalmente independientes.

- Sala el establecimiento del IXP: para la interconexión de los distintos proveedores de Internet, popularmente conocida en el sector del Centro de Datos como “Meet me Room”. Sala para interconectar todas las instituciones públicas
- Salas para equipos IT (Convencional y Cofre): espacio donde están ubicados todos los equipos IT y networking
- Salas UPS y de Baterías: espacio donde están ubicados todos los equipos de suministro y distribución energético a excepción de los grupos electrógenos y equipos de Media Tensión.
- Sala NOC: espacio dedicado para la operación y seguimiento del data center.
- Sala para CERT-PY.
- Sala de Crisis
- Sala de Capacitación y de Mantenimiento.
- Baños para uso interno, y otros cercanos a la entrada para visitas y terceras empresas.
- Office o pequeña cocina para almorzar
- Almacén: espacio dedicado al almacenamiento de equipos, reparación y desempaque.
- Muelle de carga/descarga: espacio de acceso al Centro de Datos para mercancías y equipamiento
- Espacios exteriores: todo el espacio situado al exterior del edificio y donde están ubicados los grupos electrógenos y los tanques de combustible, sistema de transformación media tensión y climatizadoras.
- Estacionamiento de autos.

A continuación, se describe punto por punto las diferentes soluciones técnicas previstas para cada espacio. Así mismo se describen las soluciones previstas para la obra civil y estructura exterior del complejo.

5.2.2 *Estructura exterior*

Se parte de la idea de trabajar con un volumen exterior común y homogéneo que transmita una imagen urbana del complejo tecnológico.

El acceso se sitúa en la esquina noreste donde los vehículos entran a un muelle de descarga cubierto, generando un espacio de transición entre el espacio interior y el exterior.

Para la fachada se sugiere resolver con un material único, los Panel Acero Lacado fijados por medios mecánicos, que dotan de estanqueidad del recinto y así proteger las salas interiores de las inclemencias medioambientales.

La estructura será de resistencia al fuego RF120, para evitar el colapso de la misma sobre las salas interiores y muy especialmente sobre la sala cofre en caso de incendio exterior. La envolvente es de resistencia al fuego RF120, de acorde a la estructura.

Estructura de suportación

La estructura de suportación cumplirá con los requisitos descritos en materia de:

- Resistencia antisísmica
- Resistencia al viento
- Resistencia al fuego RF120

Las características constructivas de la misma son:

- Pilares cada 5 metros y cerchas en la dirección larga.
- Pilares metálicos tubulares de acero S275JR de diámetro 323mm y espesor 6 mm de hasta 6 metros de altura.
- Perfiles metálicos tubulares rectangulares de acero S275JR para cordones de cercha de cubierta de dimensiones 300x250 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras en taller incluidas.
- Perfiles metálicos tubulares rectangulares de acero S275JR para montantes y diagonales de cercha de cubierta de dimensiones 180x120 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras a taller incluidas.
- Perfiles metálicos tubulares rectangulares de acero S275JR para bigas riostra de cubierta de dimensiones 300x200 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras a taller incluidas.
- Perfiles metálicos IPN400 de acero S275JR para bigas secundarias cubierta de hasta 6 metros de longitud. Soldaduras a taller incluidas.
- Hormigón HA-25/B/20/IIa de relleno de los pilares tubulares, con una cuantía media de 25kg/m3.
- Acero en pletinas S275JR para soporte de pilares en cimentación. Pernos de anclaje incluidos. Soldaduras a taller incluidas.
- Montaje de cubierta de paneles sándwich de placas de poliéster reforzado grecadas, de 2 a 2,5 metros.
- Pintura intumescente de protección antincendios para una protección R120 de la estructura (pilares y perfilería) (Grosor de hasta 3000 µm)

5.2.3 *Sala proveedores servicios (carriers)*

Se requiere que exista separación física entre los caminos de acceso desde el exterior del propio recinto de manera que un incidente no pueda afectar la disponibilidad de ambas conexiones.

Cada sala de acceso de los proveedores de servicios de comunicaciones está definida para albergar 3 racks, así como ODFs para finalización de los cableados de fibra óptica.

Physical Layout

Para aprovechar y hacer un uso eficiente de la refrigeración se propone una distribución en salas separadas con intermediación de la sala de interconexión o IXP entre ambas salas de proveedores, separadas todas entre si mediante reja de seguridad que permitirá el paso del aire, pero no el acceso de personas entre las salas.

Cerramiento y accesorios

Estas salas estarán diseñadas bajo los mismos requerimientos y requisitos de la sala IT, a fin de garantizar la continuidad en el servicio, utilizando la misma calidad de accesorios.

El falso suelo de idénticas características que la sala IT.

5.2.4 *Sala de telecomunicaciones*

El cuarto de telecomunicaciones está contemplado para albergar 2 Racks tipo MDA (Main Distribution Area – Core para comunicaciones) y 6 Racks tipo GC (rack de comunicaciones).

Physical Layout

Para aprovechar y hacer un uso eficiente de la refrigeración se propone una distribución con refrigeración compartida con las salas adyacentes de acceso de servicios de comunicaciones, separadas todas entre si mediante reja de seguridad que permitirá el paso del aire, pero no el acceso de personas entre las salas.

Cerramiento y accesorios

Estas salas estarán diseñadas bajo los mismos requerimientos y requisitos de la sala IT, a fin de garantizar la continuidad en el servicio, utilizando la misma calidad de accesorios.

El falso suelo de idénticas características que la sala IT.

5.2.5 *Sala IT*

Sala IT es el espacio donde van situados todos los equipos informáticos (IT) y de comunicación (networking). Es el núcleo del Centro de Datos y es por ello que debe ser la parte mejor protegida, de manera a garantizar:

- Disponibilidad de los servicios
- Seguridad operacional
- Protección de los equipos y datos almacenados en caso de catástrofe

Physical layout

La distribución física de la instalación está definida según recomendaciones de la TIA-942 y BICSI-002. Así, se propone una sala IT con cuatro filas de racks dispuestas en configuración pasillo frío-caliente de la siguiente forma:

Sala Convencional

- 1ª fila: 8 racks densidad 6 kW/rack, numerados del Rack1 al Rack08
- 2ª fila: 8 racks densidad 6 kW/rack, numerados del Rack09 al Rack16
- 3ª fila: 7 racks alta densidad 10 kW/rack, numerados del Rack17 al Rack23
- 4ª fila: 7 racks alta densidad 10 kW/rack, numerados del Rack24 al Rack30

Sala Cofre

- 5ª fila: 5 racks densidad entre 6 y 10 kW/rack, numerados del Rack31 al Rack35
- 6ª fila: 5 racks densidad entre 6 y 10 kW/rack, numerados del Rack36 al Rack40

La distancia entre filas en pasillo frío es de 1,2 m, dejando un mínimo de 1,2 m de pasillo en todo el espacio deambulatorio de la sala, según estipulado en TIA-942 y BICSI-002.

Se garantiza un espacio en pasillo frío y pasillo perimetral de 1,2 m, tal y como es exigido en la TIA-942 y BICSI-002. En pasillo caliente, se establece un ancho de al menos 1 m, de acuerdo a BICSI-002.

Requisitos de la estructura

La estructura cumpliría con los requisitos necesarios estipulados por la TIA-942 y BICSI-002 que una estructura convencional de hormigón no podría cumplir.

Además, la sala cofre cumple con las exigencias de la EN1047-2, que con vigencia desde 2002 y armonizada en la UE, especifica las prestaciones que deben cumplir las salas técnicas (Salas de Procesos de Datos (CPDs)) para dotarlas de la máxima seguridad y garantía de supervivencia, incluso ante casos de fuego.

Principales especificaciones a cumplir:

- Protección contra el fuego.
- Límite máximo de temperatura interior en sala (en condiciones de ensayo durante 60 minutos) de 75ºC.
- Límite máximo de humedad relativa interior en sala (en condiciones de ensayo durante 60 minutos) del 85%.

Un Centro de Datos tiene una probabilidad media de ser dañado por fuego (interior o exterior) del 4% (fuente: HP). Asimismo, el 95% de empresas cuyos Centros de Datos se incendian sin back-up actualizados, cesan su actividad (quiebran) en menos de 12 meses (fuente: HP). De ahí la criticidad de una protección adecuada, no sólo contra los daños producidos por el fuego, sino también contra los efectos de temperaturas elevadas (ya que dañan cintas, máquinas, discos,…) y de humedades relativas que puedan condensar agua y cortocircuitar cuadros eléctricos y máquinas.

Además, si bien la norma no especifica protección hidrófuga, aun siendo la probabilidad de daños por inundación de alrededor del 3% (fuente: Swiss RE), es recomendable obtener una protección IPX5 en el Centro de Datos (protección frente a la exposición directa de agua por la parte superior a 45º de inclinación y lateral con caudales importantes de exposición), o incluso IP67 (protección contra inundación completa, sólo disponible por requerimiento específico del cliente).

La altura libre mínima en la sala entre racks y techo será al menos de 460 mm tal y como establece la TIA-942.

Características cerramiento

El cerramiento escogido para la Sala Cofre correspondería a una solución del tipo Rittal LSR 18.6E o similar.

El cerramiento estará realizado 100% con paneles y estructura autoportantes. A fin de garantizar la continuidad de la protección, las uniones entre los paneles se efectuarán a través del machihembrado especial de los propios paneles, junto con la aplicación de juntas intumescentes protectoras y embellecedor de recubrimiento especial, que además proporciona un alto grado de protección a la intrusión en la sala.

El cerramiento escogido mantiene la temperatura interna de la sala por debajo de 75 ºC durante todo el ensayo al fuego.

Los paneles de pared y techo de protección contra el fuego estarán compuestos por un sándwich de materiales ignífugos y materiales termo aislantes para soportar altas temperaturas y aislar de forma estanca el recinto. El sándwich será revestido por chapa de acero galvanizado con un acabado lacado blanco en ambos lados.

Uno de los puntos más críticos en el diseño de un Centro de Datos conforme con normativa EN 1047 es el diseño de las puertas de acceso al mismo, las cuales deben soportar esfuerzos y tensiones muy importantes. Es por este motivo que la puerta de acceso será especial con un marco completo y un perfil especial. Dispondrá en el interior de una barra antipánico, mientras

que en el exterior existirá una maneta de apertura de la puerta con llave de cerramiento. La apertura se controlará mediante un sistema de control de accesos.

La resistencia a la efracción para la sala cofre será clase RC 3 (WKIII) de acuerdo a EN1627/EN1630. Las puertas en cambio cumplirán con una resistencia clase RC 4 (WKIV).

Las características de la sala comparadas con una construcción convencional son:

Criterion	Standard	Conventional construction[2]	LSR 18.6 E
System test	Test as a complete system or construction according to the following standards	X	✔
Fire protection Test at temperatures of up to over 1000° C	ECB-S certification according to EN 1047-2, 50K temperature rise and 85% rel. humidity **over 24 hours** (soak-out period), heating time 60 minutes	X	✔
	50K temperature rise and 85% rel. humidity over 30 minutes, without soak-out period	X	✔
	F120 as system test according to EN 1363 (DIN 4102), for the design of the room units and their installation modules.	X	✔
	F90 as system test according to EN 1363 (DIN 4102), for the design of the room units and their installation modules.	X	✔
	F180 as component test only according to EN 1363 (DIN 4102), wall system only	X	✔
	F120 as component test only according to EN 1363 (DIN 4102), wall system only	(✔)	✔
	F90 as component test only according to EN 1363 (DIN 4102), wall system only	✔	✔
Explosion	Detonation test as system test of 200 kg TNT from 40 m distance	X	✔
Water	Standing water, 72 hours, 40 cm, 20 droplets maximum	X	✔
	Fire-fighting water, IP x6 as system test according to EN 605 29, for the design of the room units and their installation modules.	X	✔
	relative humidity, 85 %, over 24 hours (soak-out period), 60 minute heating time, in accordance with EN 1047-2	X	✔
	relative humidity, 85 %, over 30 minutes	X	✔
Dust tightness	IP 5x as system test according to EN 605 29, for the design of the room units and their installation modules	X	✔ +
Corrosive fire gases	Fume/smoke (corrosive gas) tightness based on EN 1634-3 (DIN 18095)	X	✔
Unauthorised access	WK 3 as system test in accordance with EN 1627 / 1630, for the design of the room units and their installation modules, e.g. doors	X	✔
	WK 2 as system test in accordance with EN 1627 / 1630, for the design of the room units and their installation modules, e.g. doors	X	✔
	WK 4 as component test only in accordance with EN 1627 / 1630, door system only	X	✔
Debris loads	Impact test as system test, 3 lateral impacts of 200 kg from 1.5 m height	X	✔
EMC protection	Verified in accordance with tests on comparable components by Aachen Technical University	X	✔

Figura 13 Características cerramiento LSR 18.6E

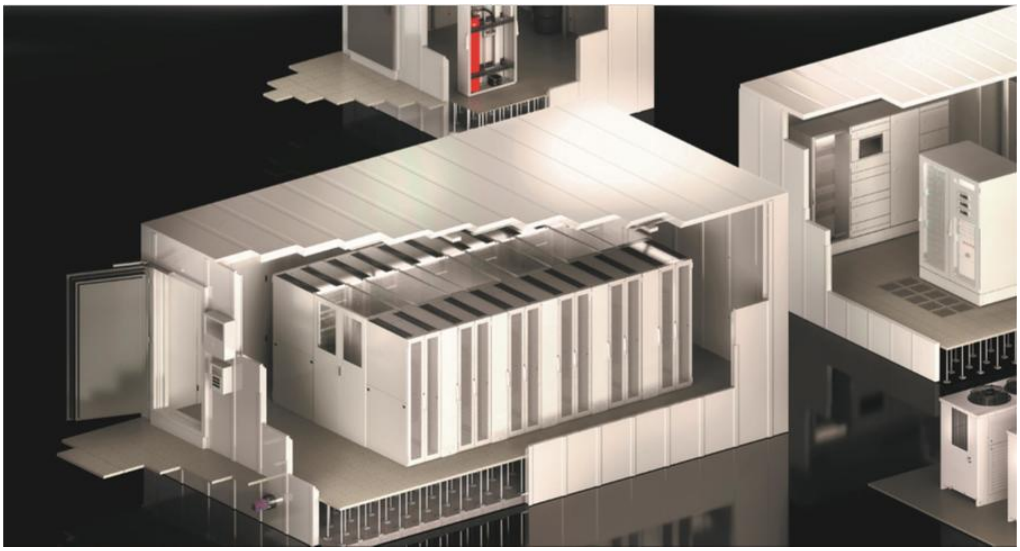


Figura 14 Ejemplo estructura de cerramiento

La estructura vendrá completamente certificada en su totalidad para resistencia al fuego de 120 minutos tanto de material como de la propia sala y estabilidad térmica en caso de incendio según normativa EN1047-2.

Pasamuros

El Centro de Datos requiere de un sistema aislante resistente al fuego y al agua con sellado de paso de cables. Consistirá en módulos con diámetro practicable en función del grosor de cables de energía y datos, con marco de acero. Se encajará en la estructura de la pared del cerramiento a través de un marco y un contramarco específico de acero galvanizado. El sellado total se realizará mediante los módulos de dimensión de cableado adaptables y unidad de compresión.

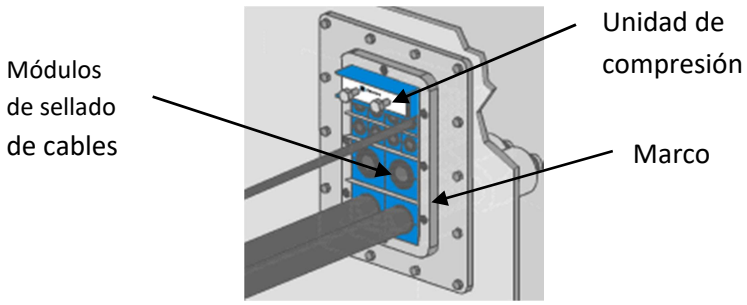


Figura 15 Componentes del pasamuros

El cerramiento también contempla la posibilidad de implantación de otros tipos de sellados en función de las necesidades específicas de cada caso, como pueden ser altas densidades de cableado de datos, tuberías de aire acondicionado, etc.

Figura 16 Otras posibilidades de pasamuros

Normativas obligatorias y condiciones para pasamuros

- El pasamuros, conjuntamente con la estructura completa (compuesta de paredes, juntas, esquinas, uniones, puertas y pasa cables) deberá proveer estabilidad térmica en caso de fuego externo a la sala. Deberá cumplir los valores medios de temperatura y humedad interna de sala establecidos para caso de incendio según la norma de protección al fuego de salas de alta seguridad EN1047-2 durante el tiempo establecido de calentamiento (máxima temperatura de 70ºC y humedad del 85%). Se requerirá una certificación emitida por una entidad certificadora independiente reconocida internacionalmente que pruebe la consecución de los requerimientos de la norma y en este sentido que se ha cumplido el requerimiento de temperatura y humedad interna de la sala y estabilidad térmica pertinente.
- El pasa muros conjuntamente con el cierre de la estructura deberá proporcionar una protección mínima de 20 dB a los efectos de campo electromagnético exteriores o medioambientales en concordancia con la norma europea EN 61000-4-3.
- El pasamuros conjuntamente con el cerramiento estructural debe proporcionar un aislamiento acústico mínimo de 31 dB en un rango de frecuencias de 100 Hz a 4 kHz.
- Emisión de gases y estanqueidad térmica: bajo condiciones de ensayo según curvas de fuego de la norma EN-1047, el pasa muros y en su conjunto la sala deberá permanecer estanca durante 60 minutos y por tanto no se deberán de registrar gases en su interior. Se requerirá una certificación emitida por una entidad certificadora independiente reconocida internacionalmente que pruebe la consecución de los resultados.
- Estabilidad mecánica: el pasamuros y en su conjunto la sala deberá permanecer en condiciones óptimas de estabilidad mecánica durante los 60 minutos requeridos bajo las condiciones de ensayo según curva de fuego de la norma EN-1047. Se requerirá una certificación emitida por una entidad certificadora independiente reconocida internacionalmente que pruebe la consecución de los resultados.
- Los pasamuros deberán proporcionar protección a la sala, ofreciendo una alta protección contra el agua según nivel de protección IP67 de la norma europea EN

60529. La estructura deberá estar certificada por una empresa certificadora acreditada y reconocida a nivel internacional.

- Todos los materiales instalados deberán ser materiales no combustibles establecidos por la norma ISO 1182.
- La sala debe de estar diseñada y construida en concordancia con lo estipulado en la norma TIA-942.

Compuerta cortafuegos

La compuerta cortafuegos es utilizada en caso de comunicación de conductos de aire entre el exterior y el interior de un Centro de Datos. La compuerta se instalará en el cerramiento para conservar las características de protección del mismo. Algunas de las características de la compuerta son:

- Fabricadas en acero galvanizado.
- Se pueden instalar en paredes y techos.
- Incorporación accionamiento por relé o automatizado mediante motor.
- Incorporación de elementos para el acabado e integración con acabados.

Figura 17 Compuerta cortafuegos

Normativas obligatorias y condiciones para compuerta cortafuegos:

- Las compuertas cortafuegos estarán certificadas en concordancia con la norma DIN-4102, con resistencia al fuego de 120 minutos.
- Todos los materiales instalados serán no combustibles establecidos por la norma ISO 1182.
- Todas las compuertas cortafuegos serán diseñadas en concordancia con la norma TIA 942.

Falso Suelo

El falso suelo o piso técnico es un sistema de pavimentación que facilita un espacio bajo toda su superficie para la conducción de servicios, permitiendo fácilmente el acceso a este espacio en cualquier punto del mismo. El falso suelo facilita la reubicación de las máquinas de la sala, cubre los cables de interconexión y comunicaciones, y los cables y cajas de conexión eléctrica de las distintas máquinas y facilita el reparto de cargas sobre el suelo real.

Los principales equipos irán anclados directamente al suelo mediante bancadas específicamente dimensionadas a fin de mitigar los efectos de seísmos y vibraciones.

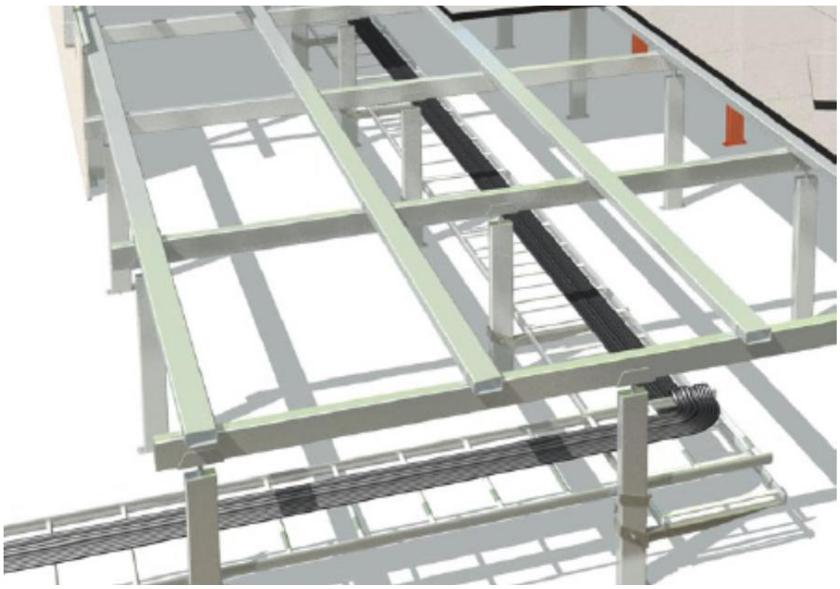


Figura 18 Ejemplo de estructura falso suelo

Las especificaciones técnicas son las siguientes:

- Dimensiones de placa 600x600 mm.
- Panel modular en aglomerado de madera y resinas de alta densidad (720 kg/m3), con un espesor de 35 mm. Acabado Inferior en hoja de aluminio de 150 micras y acabado superior en PVC universe de gerflor con 2 mm de espesor y canteado con un junquillo de 1 mm.
- Se intentará conseguir una altura de 500mm (por encima de las exigencia de VDI-2054)
- Acabado de placa mediante capa anti-estática de material PVC HPL (High Pressure Laminate), con una resistencia eléctrica de acuerdo a EN1815 > 2 kV.
- Reacción al fuego clasificado en M1 según NFP 92-507 y Euroclase BFL S1
- Pedestal TUBULAR fijado mecánicamente al forjado, compuesto por cabeza de 110 x 110 con mecanismo para fijación del travesaño tubular, varilla roscada M16. Base con platillo de 2 mm de espesor y soldado tubo de diámetro de 20 mm y 2 mm de espesor.

Los travesaños están compuestos por un tubo de acero zincado de 1 mm de espesor con una sección rectangular de 50 x 25 mm, su longitud es de 550 y 1800mm,

- Peso soportado 1.250 kg/m^2.
- Máxima permeabilidad al aire de 3 $m^3/h \cdot m^2$ a 50 Pa.
- Rejillas de refrigeración:
    - Dimensiones de 600 x 600 mm
    - Paso de aire permitido del 56% (estudio térmico de cada sala es recomendable llevarlo a cabo, para determinar el paso de aire más adecuado)
- La estructura soportará zona sísmica 3 (0,3 g) y para ello todos los pedestales irán anclados a suelo final y utilizando suportación adicional entre pedestales para arrastramiento integral del suelo.
- Las rampas en entradas no superaran un máximo del 15% de pendiente.

Cerramiento de pasillo frío

Es necesario cerrar el pasillo con los materiales adecuados para un Centro de Datos, de manera que aseguremos las condiciones en el pasillo frío.

El cerramiento de pasillo frío propuesto consiste en un sistema prefabricado diseñado para ajustarse a diversos tamaños de racks y equipos no estándar, con el objetivo de separar dos zonas climáticas dentro de la sala técnica de servidores, una fría, acondicionada por los climatizadores a la temperatura adecuada para los servidores, y otra caliente, donde descargan térmicamente estos servidores.

Las principales funciones de esta separación de pasillos son:

- Mejora de la eficiencia energética, ya que el salto térmico entre entrada y salida de aire al climatizador es mayor (mayor EER de los climatizadores), además de permitir que ellos modulen la capacidad y velocidad de los ventiladores para ajustarse estrictamente a las necesidades de los servidores.
- Disminuye las necesidades de capacidad de los climatizadores, ya que al aumentar el salto térmico aumenta la capacidad de cada unidad.

Las principales características de estos cerramientos son:

- Sistema prefabricado adaptable a cualquier tamaño de racks o equipos. Contemplando en inicio que la altura de la estructura es para armarios de 42U.
- Puertas de entrada deslizantes con posibilidad de equiparlas con cerraduras mecánicas o eléctricas (control de accesos), de chapa de acero con ventanas de cristal de seguridad y cepillos para mejorar el sellado. La puerta corredera nos va a permitir optimizar el espacio.
- Sistema mecánico de cierre automático de las puertas (para mejorar la eficiencia energética), con función de retención de puerta abierta.

- Paneles de techo transparentes de baja carga de incendios y baja generación de humos.
- Fabricado en chapa de acero lacado.
- El espacio del pasillo interno será de 1200 mm.

Figura 19 Ejemplo de cerramiento de pasillo

5.2.6 *Salas UPS Y baterías*

Se tomarán los mismos objetivos que la sala IT para diseñar las salas de UPS y Baterías.

La TIA-942 y BICSI-002 requieren que a partir de 100 kW de potencia IT, los equipos UPS estén físicamente separados de los equipos IT. Así mismo, se requiere que exista separación física entre los caminos de distribución de manera que un solo evento no afecte la disponibilidad de ambos caminos.

Physical Layout (Salas UPS y baterías)

Los estándares TIA-942 y BICSI-002 recomiendan que los grupos de baterías estén físicamente separados de los equipos UPS y los cuadros eléctricos.

Asimismo, los equipos UPS y las baterías requieren diferentes condiciones de temperatura por lo que separándolas físicamente y utilizando dos sistemas diferentes de refrigeración se pueden obtener importantes ahorros energéticos.

La distribución en la UPS se han mantenido las distancias recomendadas por el estándar TIA-942 y BICSI-002 de 1,2 m de espacio en pasillos.

Cerramiento y accesorios (Salas UPS y baterías)

Estas salas estarán diseñadas bajo los mismos requerimientos y requisitos de la sala IT, a fin de garantizar la continuidad en el servicio, utilizando la misma calidad de accesorios.

El falso suelo de idénticas características que la sala IT.

5.2.7 *Almacén*

El almacén es un espacio destinado a almacenamiento de equipos y piezas de repuesto para los equipos del Centro de Datos, así como también es un espacio destinado al montaje y desmantelamiento de equipos.

Si bien, los equipos que se guardan en su interior son de importante valor económico, no es considerada una sala crítica, y es por ello que los requerimientos a cumplir serán inferiores.

Physical layout

La distribución exacta en la sala quedará por definir según la operatividad del Centro de datos, pero sí que se considerarán tres espacios bien diferenciados:

- un espacio destinado al almacenaje, con estanterías de un mínimo de 500 mm de fondo,
- otro espacio reservado al montaje y reparación de equipos, con una mesa de trabajo y un espacio para guardar las herramientas,
- y finalmente un espacio destinado al reciclaje de los deshechos.

Cerramiento

Esta sala al no ser considerada crítica no es necesario cumplir con los requisitos de las sala IT. Ahora bien, ésta debe albergar componentes equipos IT y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.8 *Sala NOC*

La sala NOC estará destinada a efectuar el control de redes de computación y parámetros de funcionamiento del Centro de Datos.

La sala es considerada crítica en términos de control y operación, y es por ello que debe estar protegida. Ahora bien, en ella no se ubicarán equipos críticos y en caso de incendio deberá ser desalojada.

Physical Layout

La distribución exacta en la sala quedará por definir según la operatividad del Centro de Datos, pero sí que se considerarán dos espacios bien diferenciados:

- Puestos de control y supervisión del Centro de Datos, con suficiente espacio al menos para seis puestos de trabajo con estaciones de trabajo y pantallas panorámicas de control, y estanterías para almacenar documentación de mantenimiento y operación
- Mesa de reuniones donde poder hacer reuniones de seguimiento del Centro de datos, reuniones de gestión de incidencias y formación personalizada del personal.

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de las sala IT, pues debería ser desalojada en caso de incidente grave en el Centro de datos. Sin embargo, ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

Los criterios a cumplir serán los mismos de cerramiento de la sala IT, pero sin certificación de la sala.

5.2.9 *Sala CERT-PY*

La sala para el equipo CERT-PY estará destinada a efectuar el control de las incidencias, así como de todas las gestiones en materia de ciberseguridad, habiéndose solicitado por parte de la SENATICs que se considere su ubicación dentro del nuevo Centro de Datos.

La sala es considerada crítica en términos de control y operación, y es por ello que debe estar protegida. Ahora bien, en ella no se ubicarán equipos críticos y en caso de incendio deberá ser desalojada.

Physical Layout

La distribución exacta en la sala quedará por definir según la operatividad del Centro de Datos, pero sí que se considerarán dos espacios bien diferenciados:

- Puestos de control y supervisión del Centro de Datos, con suficiente espacio al menos para seis puestos de trabajo con estaciones de trabajo y pantallas panorámicas de control, y armarios cerrados para poder almacenar documentación bajo llave.
- Mesa de reuniones donde poder hacer reuniones de seguimiento.

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de las sala IT, pues debería ser desalojada en caso de incidente grave en el Centro de datos. Sin embargo,

ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

Los criterios a cumplir serán los mismos de cerramiento de la sala IT, pero sin certificación de la sala.

5.2.10 *Sala de crisis*

Se contempla una sala de reuniones con características específicas para ser utilizada como sala de crisis, donde se puedan desarrollar reuniones por los gestores del Centro de Datos para tomar decisiones frente a pantallas que puedan monitorizar, según se precise, los distintos sistemas de control.

El espacio permitirá reunirse hasta 16 personas en torno a una misma mesa y contará con Video Wall para mostrar los principales sistemas a analizar (replica de los que se visualizan en la sala NOC).

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de la sala IT, pues debería ser desalojada en caso de incidente grave en el Centro de datos. Sin embargo, ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.11 *Sala de reuniones*

Es preciso disponer de una sala para uso específico de las reuniones con terceras empresas, ya sean colaboradores proveedores o cualquier institución que requiera mantener un encuentro dentro del centro de Datos.

La ubicación física estará lo más próxima posible al punto de entrada al edificio, desde el acceso de visitas, de cara a limitar el tránsito de personal por las zonas estrictamente necesarias (ello facilitará el mejor grado de seguridad posible, así como una mejor mantenibilidad y limpieza de las zonas menos transitadas).

El espacio permitirá reunirse hasta 10 personas en torno a una misma mesa.

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de las salas IT, pues debería ser desalojada en caso de incidente grave en el Centro de datos. Sin embargo, ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.12 *Sala de capacitación y mantenimiento*

El personal técnico que operará el centro de datos en materia electro-mecánica especialmente, contará con una sala específica donde guardará las herramientas para el desarrollo de su labor diaria, así como el material de repuesto imprescindible para la correcta gestión del mantenimiento.

Esta misma sala contará con un espacio donde se podrá desarrollar la capacitación del personal que trabaje en estas laborales.

Para otro tipo de capacitaciones con terceras empresas (como los fabricantes de equipamiento) se podrá utilizar la sala de reuniones anteriormente mencionada.

Se contará con dos puestos de trabajo completos (mesa, silla, ordenador y pantalla). Además, se dispondrá de un tercer puesto donde se dispondrá de una continua monitorización del BMS, mientras los técnicos se encuentren en dicha sala.

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de las salas IT, pues debería ser desalojada en caso de incidente grave en el Centro de datos. Sin embargo, ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.13 *Sala de guardia o seguridad*

En la entrada a las instalaciones estará ubicada la sala desde la cual se realizará el control de acceso físico.

En dicha sala se contará con al menos los siguientes medios:

- PC y monitor asociado, para gestión de operaciones habituales del puesto de seguridad
- PC y monitor asociado, para BMS
- PC y conjunto de dos monitores asociados, para gestión de sistemas de seguridad (Control de accesos y CCTV).
- PC y monitor asociado, para sistema gráfico del sistema contra incendios
- Consola para visualizar las llamadas de los videoporteros e intercomunicadores.

La comunicación con los visitantes se realizará a través de panel acristalado con refuerzo de seguridad, y dispondrá de paso/orificio para el intercambio de documentación y acreditaciones.

Cerramiento

Si bien esta sala es considerada crítica, no es necesario cumplir con los requisitos de las salas IT, pues podría ser desalojada de manera rápida en caso de incidente grave en el Centro de

datos. Sin embargo, ésta debe albergar personal trabajando y mantenerse en condiciones óptimas en caso de incidente sobre la instalación. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.14 *Muelle de carga/descarga*

El muelle de carga y descarga es necesario en un centro de datos para poder asegurar la integridad de los equipos IT durante la descarga, gestionar la logística y almacenar momentáneamente los bultos.

Así mismo, realizará funciones de acceso al Centro de Datos tanto principal como de mantenimiento.

Physical layout

La distribución queda definida según la operativa del Centro de Datos, y considerará los siguientes espacios:

- Acceso principal al Centro de Datos, con una puerta gestionada por control de acceso
- Acceso de mantenimiento, por el cual poder introducir grandes bultos.
- Espacio de almacén temporal, dónde poder almacenar momentáneamente bultos durante la carga y descarga.
- Zona protegida para la descarga de camiones, de manera que las inclemencias climáticas no tengan impacto sobre los bultos que se descargan.

Cerramiento

El cerramiento de esta zona es considerado no crítico, y es por ello que se utilizará la misma estructura exterior del edificio como cerramiento.

5.2.15 *Sala coffee-cocineta*

Se dispondrá de sala para poder almorzar o tomar un café por parte del personal que trabaja dentro del centro de datos (facilitando de este modo la gestión de los equipos que trabajaran 24x7) y para las visitas a las cuales se acuerde facilitar su uso.

Esta sala se encontrará alojada lo más cercana posible al acceso principal de la instalación.

Cerramiento

Esta sala no es considerada crítica, pues podría ser desalojada de manera rápida en caso de incidente grave en el Centro de datos. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.2.16 *Baños*

Se contemplan dos zonas de baños independientes.

La que se situará más próxima al punto de acceso principal del edificio se dedicará principalmente al uso por parte de los visitantes y terceras empresas, que accedan al centro de datos. Dispondrá de dimensiones adecuadas para personas de movilidad reducida.

Los baños contemplados para el personal operativo del centro de datos dispondrán de una ducha para cada género.

Cerramiento

Esta sala no es considerada crítica, pues podría ser desalojada de manera rápida en caso de incidente grave en el Centro de datos. Así pues, se propone una solución de certificación de material, pero no de sala, lo cual garantiza las funciones que deben cumplir.

5.3 Solución potencia

En el siguiente apartado ser describirá el suministro de potencia a los equipos IT, así se describirá:

- Estructuración de esquemas unifilares.
- Equipos eléctricos principales.
- Distribución y organización del cableado.
- Protecciones eléctricas.
- Iluminación e Iluminación de emergencia.

5.3.1 *Estructura del esquema unifilar*

Como se ha descrito anteriormente, el sistema ha sido diseñado para cumplir con las exigencias de nivel Tier III. Así pues, se ha optado por utilizar un diseño simple de Tier III con las siguientes características:

- Régimen de neutro TNS en toda la instalación
- Doble alimentación de compañía al centro de datos (al menos una dedicada)
- N grupos electrógenos de suministro primario para cada línea, total 2N
- N UPS por línea para equipos IT, total 2N
- Suministro mediante busbar a equipos IT.
- ATS entre las dos líneas para suministro eléctrico a componentes no críticos

- Protecciones contra sobretensiones en cuadros de distribución

Figura 20 Descripción estructura del esquema unifilar

FASE I

La instalación eléctrica se basa en una redundancia 2N por lo que se distinguen dos ramas de infraestructura (A y B). Cada rama eléctrica está compuesta por los siguientes elementos:

- Suministro MT de compañía. Centro de seccionamiento y medida de compañía eléctrica.
- Centros de transformación MT/BT de tipo abonado para cada rama eléctrica. Para dos transformadores. En dicha fase se instalará un transformador de tipo seco con una potencia de 1600 kVA. Cuadros de distribución de Baja Tensión.

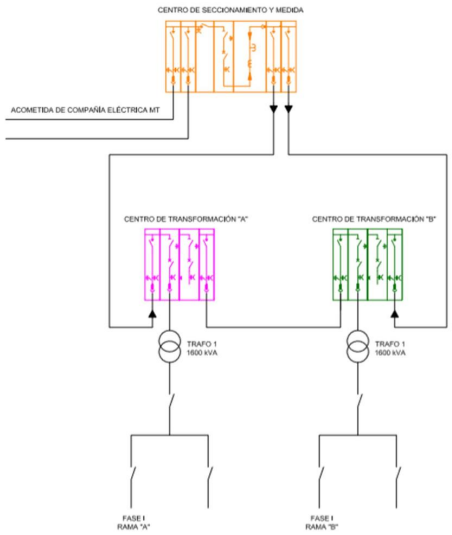


Figura 21 Detalle del esquema unifilar de la fase I

- Generador en ejecución automática de potencia 750kVA/600KW Emergencia, para cada rama eléctrica. Un total de 2 unidades.
- Conmutación Red- GRUPO mediante ATS de transición cerrada, por cada rama eléctrica. Un total de 2 unidades.
- Sistema de alimentación ininterrumpida modular para respaldo de servicios esenciales de 300kVA/kW con respaldo de baterías para 10 minutos a plena carga. El sistema de baterías tendrá 10-12 años de vida útil. Por cada rama eléctrica, un total de 2 unidades.
- Distribución primaria y secundaria por busbar, por cada rama eléctrica.

El funcionamiento de cada una de las ramas es completamente independiente de forma que cualquier defecto quede completamente aislado y se garantice la continuidad del servicio. No se prevé el acoplamiento de una rama sobre la otra ni de forma automática ni manual.

Las protecciones serán tripolares realizadas mediante interruptor automático con relé electrónico y cableado dimensionado en acorde a las intensidades demandadas.

FASE II

Ampliación de acometidas en BT a las dos nuevas salas eléctricas, una por rama.

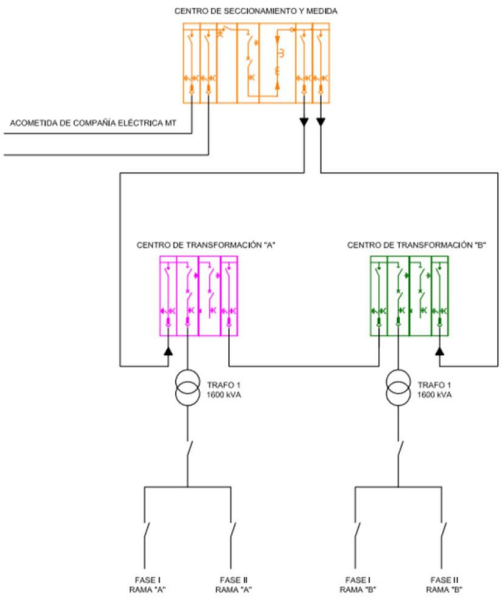


Figura 22 Detalle del esquema unifilar de la fase II

Ampliación de dos salas eléctricas:

- Generador en ejecución automática de potencia 750kVA/600KW Emergencia, para cada rama eléctrica. Un total de 2 unidades.

- Conmutación Red- GRUPO mediante ATS de transición cerrada, por cada rama eléctrica. Un total de 2 unidades.
- Sistema de alimentación ininterrumpida modular para respaldo de servicios esenciales de 300kVA/kW con respaldo de baterías para 10 minutos a plena carga. El sistema de baterías tendrá 10-12 años de vida útil. Por cada rama eléctrica, un total de 2 unidades.
- Distribución primaria y secundaria por busbar, por cada rama eléctrica.

El funcionamiento de cada una de las ramas es completamente independiente de forma que cualquier defecto quedará completamente aislado y se garantizará la continuidad del servicio. No se prevé el acoplamiento de una rama sobre la otra ni de forma automática ni manual.

Las protecciones serán tripolares realizadas mediante interruptor automático con relé electrónico y cableado dimensionado en acorde a las intensidades demandadas.

La topología del sistema para alimentación a servicios IT y servicios mecánicos queda reflejada en el correspondiente esquema unifilar.

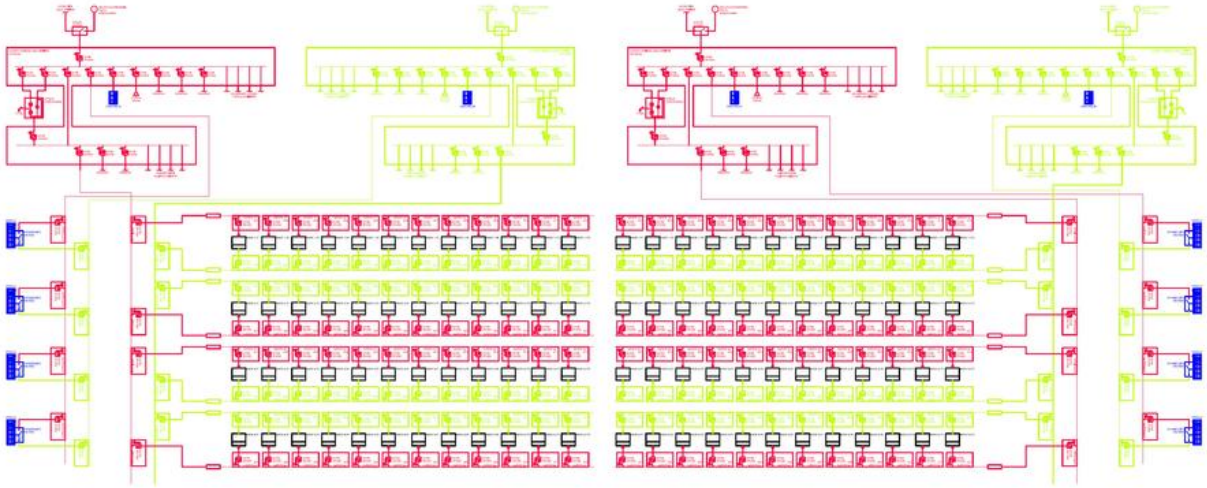


Figura 23 Esquema unifilar para ambas fases (I y II)

Se prevé una conexión a red eléctrica de media tensión (dedicada y exclusiva para el Centro de Datos). Siendo recomendable solicitar a ANDE la posibilidad de una segunda línea como respaldo o socorro. Las líneas eléctricas serán independientes la una de la otra, proviniendo de diferentes subestaciones y diferentes anillos de distribución.

En cada una de las líneas de distribución se situará un transformador de media a baja tensión de 1600kVA para dar respuesta a las demandas totales de la instalación.

Aguas abajo de los transformadores se situará los grupos electrógenos cada uno con su ATS el cual dispondrá de solapamiento de neutro a fin de evitar la pérdida de referencia durante una conmutación y tener régimen de neutro flotante.

De cada uno de los ATS se conectarán los cuadros de distribución de baja tensión, que repartirán la energía a cada uno de los componentes del sistema. El mismo cuadro tendrá su propia protección contra sobretensiones.

En cada cuadro de distribución de baja tensión estará separado en tres partes. Por un lado el suministro a equipos IT, por otro suministro a equipos mecánicos y por último para servicios no críticos.

Ambos cuadros de distribución de baja tensión. Se dotarán de aparamenta de primeras marcas ABB, Schneider (o calidad similar), y dispondrán de un 20% de espacio libre sin equipar para permitir futuras ampliaciones. Todos los interruptores y elementos internos serán monitorizados a distancia por el BMS a través de contactos auxiliares.

La línea de suministro a equipos IT estará respaldada con UPS (o SAI) de 300kVA por cada rama, los cuales asegurarán la calidad energética de suministro a los equipos IT, filtrando toda clase de fluctuaciones, sobretensiones, huecos de tensión, harmónicos, etc. A parte de los propios circuitos de rodeo de los equipos UPS (bypass), el cuadro eléctrico contará con su propio circuito de rodeo para mantenimiento de los equipos. La autonomía de respaldo será de 10 min, por encima de lo mínimo estipulado por la TIA-942 y BICSI-002.

La distribución de energía a los equipos IT se realizará mediante busbar para cada una de las filas de racks, reduciendo así la cantidad de cableado y mejorando su operación. Cada rack contará con su propia PDU de acuerdo a la potencia máxima estipulada. A todos los equipos IT se les debe asegurar doble suministro eléctrico.

En los cuadros de servicios, a cada uno de los equipos de refrigeración de la sala IT se le suministrará doble alimentación que será gestionada por el propio equipo. Los equipos de refrigeración de las salas UPS y baterías tendrán un único suministro pues no serán redundantes.

El sistema de control - BMS del Centro de Datos también estará alimentado desde alimentación segura de UPS.

5.3.2 *Equipos eléctricos principales*

Los equipos eléctricos principales corresponden a:

- Equipos de transformación de media a baja tensión.
- Grupos electrógenos.
- UPS.

Transformación media-baja tensión

Los equipos de transformación son completamente redundantes, independientes e instalados cada uno en su propia caseta de hormigón prefabricada y conforme a las regulaciones locales.

Cada transformador va acompañado por sus correspondientes celdas de conexión a compañía eléctrica y medición de consumo de energía activa y reactiva, para así ofrecer un proyecto llave en mano. Serán montados en casetas prefabricadas que albergarán la aparamenta de protección, medición y seccionamiento correspondiente.

Se plantean dos subestaciones transformadoras de 23 kV a 400 V, una para cada lado del sistema eléctrico.

El transformador seleccionado es un equipo seco encapsulado de 1600 kVA, con las principales características:

- Clase H: para uso intensivo.
- Con pantalla electrostática para reducir los harmónicos del Centro de Datos.
- Bajas pérdidas para aumentar su eficiencia energética.
- Transformador seco con envolvente metálica y refrigeración natural por aire.

Las características del equipo bajo norma IEC 60076-11 son:

- Potencia nominal: 1600 kVA.
- Tensión primaria: 23 kV.
- Tensión secundaria en vacío: 400 V.
- Frecuencia: 50 Hz.
- Número de fases: 3.
- Pérdidas debidas a cara a 120 ºC: 9 kW.
- Potencia acústica: 65 dB.

Figura 24 Ejemplo de Transformador

Se mantendrá un cierto margen de movimiento en el cableado para satisfacer las necesidades de zona anti-sísmica. El anclaje de los equipos será especialmente indicado de manera a amortiguar el efecto de un seísmo.

Grupo electrógeno

Los grupos electrógenos son completamente redundantes, independientes e instalados cada uno en su propia cabina de contenedor ISO standard de 20 pies.

El equipo seleccionado cumplirá con las siguientes características:

- Modelo motor: diesel 4 tiempos, 12 V, 1500 rpm
- Potencia total: 750 kVA
- Tensión de salida: 400 V
- Factor de potencia: 0,8
- Grado de protección aislamiento alternador: Clase H
- Tanque de combustible integrado en el propio chasis, con indicador de nivel.
- Con regulador electrónico de velocidad con calidad de onda (frecuencia) de G3.
- Alternador trifásico, tensión 400/230 V, frecuencia 50 Hz, sin escobillas, con regulación electrónica de tensión tipo AREP R-450, con capacidad de cortocircuito de 3 veces la intensidad nominal durante 10 segundos.
- Cargador electrónico de baterías además del alternador de carga de baterías propio del motor diesel.
- Interruptor automático tetrapolar de protección, con bobina de desconexión automática al actuar cualquier protección.
- Dos baterías de arranque con cables, terminales y protección.
- Resistencia calefactora con termostato del líquido refrigerante para asegurar el arranque del motor diesel en cualquier momento y permitir la conexión rápida de la carga.
- Todos estos elementos montados sobre bancada metálica con antivibratorios de soporte de las máquinas y debidamente conectados entre sí.
- El grupo se suministrará con líquido refrigerante y con el cárter lleno de aceite.
- Incluye protecciones de los elementos móviles (correas, ventilador, etc.) y elementos muy calientes (colector de escape, etc.).
- FLEXIBLE metálico de salida de escape de motor.

- Silenciador básico de escape de 25 dB(A) de atenuación, con bridas, contrabridas, juntas y tornillos.
- Juego de silenblocks para amortiguar las vibraciones entre la bancada del grupo y el suelo.
- Cubierta metálica insonorizada apta para instalar en el exterior, y adecuada para obtener un nivel de potencia acústica LWA de 97 dB(A), equivalente a un nivel medio de presión acústica de 69 dB(A) a 10 m. Dispondrá de puertas practicables para acceso a las diferentes partes del grupo.
- Silenciador con flexible y tubo de escape montado en el grupo.

Cada equipo vendría equipado con su propio sistema ATS de conmutación con solapamiento de neutro y sin aislamiento de bypass.

Figura 25 Ejemplo de solución para Grupo electrógeno

Se mantendrá un cierto margen de movimiento en el cableado para satisfacer las necesidades de zona anti-sísmica. El anclaje de los equipos será especialmente indicado de manera a amortiguar el efecto de un seísmo.

Depósito nodriza de combustible:

Depósito de combustible de capacidad suficiente para garantizar suministro al Centro de Datos durante 72 horas, de acero, de doble pared, con pies de apoyo, que responde a los siguientes requisitos y accesorios:

- Se suministra con certificado de fabricación y prueba.
- Por ser de doble pared se considera depósito con cubeto incorporado.
- Incluye detector de fugas mediante vacuómetro.
- Se incluye una tapa de boca de hombre con bocas para el llenado, aspiración, sobrante de motor, ventilación, montaje de detectores de nivel y rebosadero.
- La boca de llenado es de 3" con acoplamiento rápido para llenado mediante unión hermética y tubo de carga al interior del depósito hasta 15 cm del fondo.
- La salida para aspiración de combustible incluye un tubo en el interior del depósito con válvula de retención para evitar que se desencebe el circuito (si la salida es por parte superior)
- Detector de nivel mínimo para señal de alarma.
- Latiguillos flexibles para conexión al grupo.

Sistema de trasiego:

Equipo de llenado automático del depósito interior, montado sobre el propio grupo, desde el depósito nodriza, comprendiendo:

- Doble bomba eléctrica de tipo engranajes de 1.000 l/h, para llenar el depósito de combustible del grupo.
- Detector de nivel máximo y mínimo montado en el depósito incorporado en el grupo.
- Electroválvula de seguridad a la entrada de combustible del depósito de grupo.
- Cuadro de maniobra de bombas de combustible, conteniendo aparamenta para la maniobra de cada bomba, con selector de funcionamiento Automático-Manual. Este cuadro mantiene el combustible entre los niveles máximo y mínimo, poniendo en marcha y parando las bombas al recibir la señal del detector de nivel. Dará también señal de apertura y cierre para la electroválvula de la entrada del depósito de grupo.
- Tendrá una entrada para recibir señal de nivel mínimo en el depósito nodriza que provocaría el paro de las bombas para que no trabajen en vacío.

UPS

La UPS mantendrá automáticamente la alimentación de CA de la carga crítica dentro de tolerancias específicas, sin interrupción durante el fallo o el deterioro del suministro de alimentación de la red eléctrica (por un período específico según el tiempo de funcionamiento de las baterías). La UPS puede expandirse mediante módulos adicionales en paralelo de la misma potencia con el fin de suministrar los requisitos del crecimiento de la carga o de la redundancia del módulo.

La solución más adecuada técnicamente pasaría por utilizar un sistema de UPS modular por módulos de 30, 40 o 50 kW.

Una solución alternativa pasa por el uso de UPS modulares de mayor tamaño. Ambas soluciones son energéticamente eficientes y fiables.

Se utilizarán los mismos equipos tanto para respaldo de equipos IT como la parte de control de los equipos mecánicos. De esta manera:

- UPS IT A: 300 kW
- UPS IT B: 300 kW

Así la solución propuesta puede considerarse para 2 UPS modulares de 150kVA por rama, con las siguientes características:

- Sincronización entre las UPS
- Sistema de gestión de la potencia para ahorro energético
- Disponibilidad de eco-mode para funcionar off-line y reducir aún más el consumo
- Bajo coste de mantenimiento
- 10 minutos de autonomía con batería de duración de vida útil 10-12 años.

La sincronización entre los mismos módulos de un mismo grupo es necesaria y un requisito indispensable.

Se mantendrá un cierto margen de movimiento en el cableado para satisfacer las necesidades de zona anti-sísmica. El anclaje de los equipos será especialmente indicado de manera a amortiguar el efecto de un seísmo.

El sistema dispondrá de un algoritmo mediante el cual, analizando el estado de carga real de la UPS, conecta y desconecta módulos para mantener al sistema en un estado de carga elevado para mejorar su rendimiento energético (siempre manteniendo activos los módulos redundantes deseados). Esto es especialmente interesante cuando la carga es estacional, o cuando se configuran sistemas de doble bus de alimentación.

Otra de las características importantes es la posibilidad de trabajo a temperaturas de hasta 55ºC, con lo que prácticamente no se verá afectado su funcionamiento si la sala donde estarán ubicadas tuviera algún problema con la climatización.

Las principales características técnicas para las UPSs a instalar en este proyecto son:

General:

- Potencia nominal: 300 kVA
- Topología: Posibilidad de trabajar en VFI, VI y VFD, con algoritmo que conmute automáticamente de un modo a otro en función de las necesidades de la red y de la carga.
- Módulos de 30kVA conectables e intercambiables en caliente.
- Algoritmo de control de módulos que active/desactive módulos en función del estado real de carga del SAI.
- Clase 1 según IEC62040-3.
- Capacidad de conexión de hasta 6 equipos en paralelo.
- Rendimiento AC/AC (en modo VFI): 96,8%.
- Rendimiento AC/AC (en modo VI): hasta 98,5%
- Rendimiento AC/AC (en modo VFD): hasta 99%
- Temperatura de funcionamiento: hasta 55ºC.
- Protección contra retorno de tensión por la línea de by-pass (back feed protection).
- Control por procesador DSP
- Posibilidad de conexión de baterías centralizadas (bus común de CC) o distribuidas (cada módulo con sus baterías).
- Sistema de gestión inteligente de baterías.
- EMC (emisiones electromagnéticas): clase C3 según IEC/EN 62040-2.
- Resistencia a sobretensiones: nivel 3 según IEC/EN 61000-4-5

Caja de entradas/salidas:

- Interruptor de entrada a rectificadores.
- Interruptor de entrada a sistema de by-pass.
- Interruptor de salida.
- Interruptor de baterías.
- Interruptor manual de by-pass con señal a los inversores para su protección ante un cierre accidental.

Bypass estático:

- By-pass centralizado con puente de tiristores en la línea de reserva, con impedancia de choque en cada fase.
- Sobrecarga: 125% durante 10 min; 150 % durante 1 min.
- Tiempo de transferencia con by-pass centralizado: <2 ms para fallos de baja impedancia.

Descripción de los módulos:

Rectificador:

- Tensión de entrada: 400 V, 3F+N+T; 50Hz, 60 Hz ±10%.
- Tensión de entrada admisible por el rectificador sin descargar baterías: 320 V – 460 V
- Tecnología: rectificador a IGBT de tres niveles controlado mediante PWM con control vectorial.
- THDi de entrada < 3%.
- FP de entrada > 0,99
- Corriente de inserción < I máxima
- Arranque suave en rampa con pendiente programable (1 a 90 s); tiempo de retardo de arranque programable (1 a 180 s).

Inversor:

- Potencia nominal de salida: 300 kVA / 300 kW
- Tensión de salida: Trifásica 400 V (380 V / 415 V ajustable)
- Estabilidad de la tensión de salida: ±1%
- Frecuencia: 50/60 Hz ±0,1%
- THDu: <3% / <5% (carga lineal/ no lineal).
- Sin desclasificación de potencia activa ni aparente de salida para cargas capacitivas.
- Tecnología: Inversor a IGBT de tres niveles controlado mediante PWM con control vectorial, sin transformador en el ondulador.

Conectividad y comunicaciones:

- Display táctil de cristal líquido con mímico de bloques, medidas de todos los parámetros eléctricos de entrada y salida, registros de eventos, estado de las baterías, etc.
- Puerto de comunicaciones RS-232.
- Tarjeta de entradas/salidas de contactos libres de potencial con asignación de eventos internos de la UPS programables.
- Posibilidad de equiparlo con tarjeta ethernet, IEC 485, etc.
- Software para el cierre de sistemas operativos ante un final de la autonomía tras un corte prolongado de alimentación.
- Sistema de supervisión y telemantenimiento gestionado y vigilado por el fabricante desde sus oficinas, de forma tal que, ante situaciones de alarma de la UPS o su entorno eléctrico, de arranque al plan de contingencia contemplado en el contrato de mantenimiento, que genere llamadas y correos electrónicos de aviso al personal de mantenimiento, que elabore informes automáticos mensuales con, como mínimo, la siguiente información: registros de eventos; gráficos de tendencias de temperatura de baterías e interna de la UPS, carga por fase (activa y aparente) y mínimos y máximos de tensión y corriente; resultados de los test de baterías.

Baterías:

Se dotará a cada UPS de dos ramas de baterías (para conseguir redundancia de baterías en cada módulo) que puedan soportar la carga máxima admisible por cada equipo durante 10 minutos. Las baterías serán de plomo-ácido estancas (libres de mantenimiento), de tecnología VRLA (de válvula regulada), de 10-12 años de vida útil según clasificación Eurobat.

Sistema de monitorización de baterías

Uno de los principales causantes de cortes imprevistos en una instalación son los fallos en los sistemas de baterías de las UPSs. Por esto, incluimos un sistema de monitorización de baterías (tipo Alber), que consiste básicamente en un hardware al que se realiza una conexión con cada batería con la finalidad de poder registrar, en tiempo real, los distintos parámetros que rigen su comportamiento. Las principales características del sistema son:

Medidas:

- Medida y registro de la corriente de carga y descarga de cada rama de baterías.
- Medida y registro de la tensión de flotación y de descarga de cada batería dentro del sistema.

- Medida y registro de la temperatura de la sala de baterías.
- Medida y registro de la temperatura de cada batería (opcional).
- Medida del rizado de corriente de la rama de baterías.
- Medida de embalamiento térmico con contacto de salida libre de potencial para orden de desconexión del cargador.

Medidas automáticas programadas para:

- Medida y registro de la resistencia (no impedancia) interna de cada batería y de la resistencia de contacto entre baterías.
- Medida y registro de la resistencia de contacto de las protecciones eléctricas de las ramas de baterías.

Precisión de las medidas:

- Medida de tensión de batería: 0-4 V, 0,1% ±1 mV.
- Medida de tensión de batería: 0-8,5 V, 0,1% ±2 mV.
- Medida de tensión de batería: 0-20 V, 0,1% ±10 mV.
- Medida de tensión de rama: 0-80 V, 0,2% ±20 mV
- Medida de tensión de rama: 0-400 V, 0,2% ±10 mV
- Medida de tensión de rama: 0-600 V, 0,2% ±20 mV
- Medida de resistencia de contactos de interruptores: 0-5 mΩ, 5% ±5 μΩ
- Medida de resistencia de conexiones entre baterías: 0-500 μΩ, 0,25% ±5 μΩ
- Medida de resistencia interna de batería: 0-32 mΩ, 5% ±1μΩ
- Medida de temperatura de batería: 0-80 ºC, ±1%.
- Medida de temperatura de sala/armario de baterías: 0-80 ºC, ±1%.
- Medida de corriente de descarga: ±4.000 A, ±1% a fondo de escala.
- Medida de corriente de flotación: 0-5 A, ±50 mA.

Informes generados:

- Informe periódico de la resistencia interna de cada batería.
- Gráfica de descarga de cada batería

- Alarma de alta temperatura de la sala de baterías.
- Alarmas al exceder los umbrales definidos por el usuario.

Conectividad y prestaciones:

- Posibilidad de integración con sistemas SCADA o BMS mediante los siguientes protocolos de comunicaciones: TCP/IP, Modbus o SNMP, bajo Ethernet o IEC485.
- Servidor web incorporado
- Conexión USB para acceso local mediante PC portátil.
- Base de datos conteniendo toda la información registrada incorporada localmente en el registrador.
- Posibilidad de definir umbrales de los parámetros de las baterías por parte del usuario para avisos tempranos de alarmas.
- Generación de alertas vía correo electrónico.
- Contactos libres de tensión para alarmas y estados del sistema.
- Conexión entre módulos del sistema mediante fibra óptica para garantizar completo aislamiento.

5.3.3 *Distribución y organización de cableado*

Cableado principal

Uno de los requisitos es compartimentalización de todos los caminos de distribución y componentes de capacidad.

Desde los cuadros distribución de baja tensión se distribuirá el cableado eléctrico por todo el Centro de Datos garantizando los requisitos del nivel Tier III y las recomendaciones de la TIA-942 en relación a distancias de seguridad.

Se asegurará la estanqueidad de la compartimentalización mediante pasacables estancos.

El cableado siempre será conducido mediante bandejas portacables metálicas para cables de energía, con conexión a directa a tierra.

Busbars

La distribución de potencia en sala se realizará mediante busbars. Estos elementos son embarrados que mejoran sustancialmente las características de las salas IT, ofreciendo:

- Flexibilidad: permiten la conexión-desconexión de circuitos rápidamente

- Trabajo en caliente: permiten la conexión-desconexión de circuitos en caliente sin tener que abrir ninguna línea.
- Eficiencia energética: eliminando el cableado en el falso suelo se evitan los taponamientos para la circulación de aire
- Escalabilidad: las conexiones pueden ser añadidas tanto como se necesiten
- Modularidad: todas las densidades de potencia pueden ser alimentadas con la misma infraestructura de busbar
- Simple configuración: cargas trifásicas y monofásicas pueden ser conectadas al mismo busbar.
- Bajo coste: Menos material necesario y menor coste de instalación que los sistemas tradicionales
- Ampliable: densidades más elevadas pueden ser fácilmente acomodadas en un futuro
- Reinstalable: Todos los elementos pueden ser fácilmente reinstalados en nuevas instalaciones.
- Reducción de riesgos por fallo humano: todos los circuitos son mucho más visibles y gestionables
- Reducción de riesgo de sobrecarga por fase: el conductor nunca cambia físicamente de lugar

En la figura siguiente se muestra la diferencia entra la distribución de cableado a través de un sistema tradicional de PDU's y un sistema con Busbar.

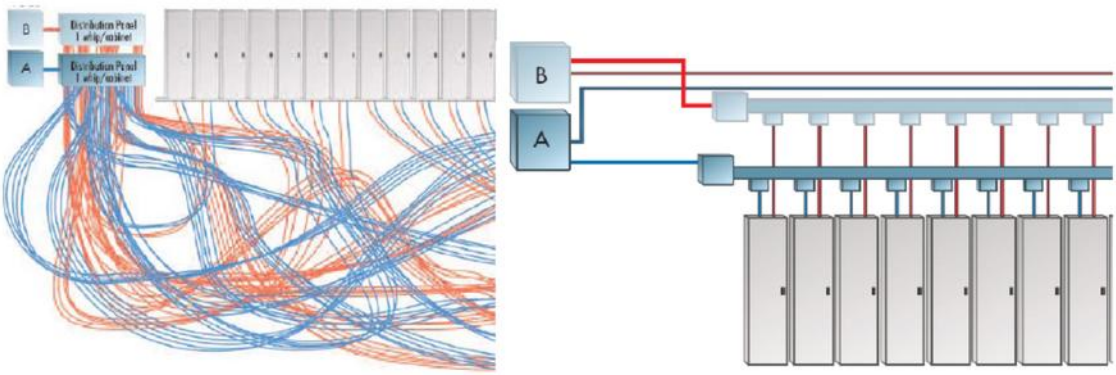


Figura 26 Diferencia entre distribución por PDU tradicional y Busbar

PDUs intelligentes

La distribución de potencia dentro de cada rack activo requerirá la utilización de PDUs inteligentes para garantizar la alimentación redundante a cada equipo IT que lo precise. Se recomienda utilizar unidades de distinto color para el lado A y el lado B de manera que sea muy visual reconocer si un equipo IT está conectado a ambas fuentes.

Las PDU (Power Distribution System) deben ser gestionables y controlables a nivel de tomacorrientes, esto es, puede conocerse a distancia todos los parámetros eléctricos de cada tomacorriente, así como activarlos y desactivarlos a distancia. Sus principales características son:

- Monitorizable a nivel de tomacorriente.
- Precisión de la medida: ± 1% en corriente y tensión.
- Encendido/apagado por tomacorrientes a distancia, mediante interruptores biestables (telerruptores).
- Múltiples alarmas por caída de carga, superación de umbral de corriente, etc.
- Display local (en la PDU) y remoto opcional (para instalar frente al rack)
- Diversas configuraciones de tomas de salida (IEC C13 y C19, Nema)
- Medida de V, I, kW, kVA, kWh, factor de potencia, factor de cresta, frecuencia.
- Posibilidad de conexión de sensores externos de temperatura, humedad, puertas abiertas, contactos de estado.

Figura 27 Ejemplo de PDU inteligente

5.3.4 *Protecciones eléctricas*

Protecciones para equipos, líneas y personas

En el diseño de Centros de Datos se recomienda la no duplicación de interruptores. Por ello, no se instalarán aquellos interruptores que realicen una función homóloga a otro interruptor aguas arriba o aguas abajo del mismo. Con esto se evita que exista el mínimo riesgo de fallo de las protecciones. En caso necesario, se podrán instalar seccionadores de circuito eléctrico, los cuales no tienen ningún tipo de actuación automática.

No habrá protecciones diferenciales previstas puesto que el régimen de neutro es TNS.

Se prevé la vigilancia diferencial con visualización de fugas y contacto de alarma de umbral programable, que solo dé información del nivel de fugas y dé una alarma, pero sin necesidad de disparar ninguna protección.

Para el resto de equipos se utilizará curva C y dimensionados según sus consumos máximos.

Todos los ATS y STS, a excepción de los principales dispondrán de circuito de aislamiento.

Los ATS principales, situados aguas abajo de los grupos electrógenos dispondrán de solapamiento de neutro a fin de evitar la un sistema de referencia flotante y transitorios de

tensión entre el neutro y tierra en los equipos IT lo que provocaría disparos intempestivos de protecciones.

Todo el cableado será libre de halógenos.

Protección contra sobretensiones

Los cuadros eléctricos de distribución estarán equipados con una protección para sobretensiones de clase I y II. Éstos serán dispositivos de protección contra sobretensión de red de 4 polos. El estado de estas protecciones, junto con sus protecciones eléctricas, serán monitorizadas a distancia por el BMS mediante contactos libres de tensión

Analizadores de redes

Los cuadros eléctricos estarán equipados de analizadores de redes para realizar medidas y registros de consumos en los distintos puntos de la instalación. Sus principales características son:

- Medidas de tensiones, corrientes, potencias y energías (activa, reactiva y aparente), frecuencia, armónicos de corriente y tensión.
- Dispondrán de tarjetas de comunicaciones Ethernet con protocolo Modbus.
- Transformadores de corriente con bornas de verificación.
- Protección mediante seccionador fusible R8 para señales de tensión.

Mallados de tierra

La función del mallado de tierras es elevar la seguridad de personas y equipos ante posibles fugas de corriente y garantizar la equipotencialidad de toda la instalación. Asimismo una buena malla equipotencial evita bucles de corriente que podrían provocar fallos de comunicación, ruido eléctrico y descargas electroestáticas. También conseguiremos una protección contra perturbaciones eléctricas externas.

El estudio de la malla será realizado de acuerdo a las recomendaciones de la TIA-942 y BICSI-002, y según la normativa vigente.

El mallado asegurará conexionado directo a tierra de:

- Todos los equipos capacitivos (UPS, climatizadoras, grupos electrógenos, cuadros eléctricos…)
- Cada uno de los racks de equipos IT
- Todas las bandejas portacables
- Estructura y falso suelo de todas las salas
- Resto de equipos o sistemas que necesiten de puesta a tierra.
- Esquema de neutros: TNS.

Protecciones contra rayos

La caída de un rayo en el terreno tiene dos tipos de consecuencias: directas e indirectas.

Los sistemas pararrayos tradicionales aseguran la protección directa, derivando toda la energía a tierra. Ahora bien, los efectos secundarios pueden ser muy importantes, pudiendo llegar a afectar a la seguridad de equipos y personas.

Los pararrayos desionizantes basan su principio en la desionización del aire. El objetivo es evitar la saturación de carga electroestática entre la instalación de tierra y la atmósfera que rodea a la instalación, concretamente compensar pacíficamente la diferencia de potencial eléctrico de la zona durante el primer proceso de la formación del rayo.

Así, pues se instalará un pararrayos desionizante de carga electroestática. Éste está constituido por dos armaduras de geometría diferente elaboradas preferentemente en aluminio, separadas eléctricamente por tres aisladores, soportado todo ello por un mástil con adecuado aislamiento eléctrico, presentando además internamente en cada uno de los aisladores un dieléctrico variable tipo gas noble, en función del campo electroestático atmosférico, de manera que cada aislador, al compensar la energía en su interior, anula la saturación de cargas electroestáticas en la atmósfera de la zona de protección que son las responsables de las formaciones de los rayos, siendo su campo de acción suficiente para proteger toda la parcela del Centro de Datos.

Estudio de Selectividad

Se presentará un estudio de regulación de protecciones respetando criterios de selectividad y seguridad para proteger cargas, equipos y personas. Todas las protecciones serán reguladas de acuerdo a este estudio durante la fase de integración final.

5.3.5 *Iluminación*

La iluminación es necesaria para que los operadores puedan ver, leer y trabajar dentro del Centro de Datos. El sistema corresponde a sistema de fluorescente, modificable a tipo led una vez se establezca la operación del Centro de Datos y por lo tanto su uso diario. Las características del sistema de iluminación son:

- 500 lux en plano horizontal y 200 lux en plano vertical, según TIA-942 y BICSI-002.
- Baja emisión electromagnética.
- Resistencia al impacto 20 J y aislamiento IP65, para evitar propagación de gases en caso de rotura de tubo.

En el caso de la iluminación de emergencia, se establecen los siguientes requisitos:

- En la misma línea eléctrica y protección que la iluminación.
- 1 hora de autonomía.
- 50 lux en plano horizontal y vertical, según NFPA-101.

- Situadas en todo los marcos de puertas en su parte superior.
- Encima de los cuadros eléctricos.

5.4 Solución refrigeración

Para conseguir el máximo nivel de eficiencia y reducir el PUE del Centro de Datos al máximo desde bajas potencias, pasa por utilizar el sistema de climatización más eficiente del mercado disponible.

Para conseguir el máximo nivel de eficiencia y reducir el PUE del Centro de Datos al máximo desde bajas potencias, pasa por utilizar el sistema de climatización más eficiente disponible en cada mercado local.

5.4.1 *Estudio de la solución técnica*

A fin de determinar las soluciones técnicas se deben establecer las condiciones de trabajo:

- Temperatura de entrada de equipos IT: +25 ºC bulbo seco
- Diferencial de temperatura de equipos IT: +12 K
- Temperatura de entrada de UPS: + 25 ºC bulbo seco
- Diferencial de temperatura de UPS: + 10 K
- Temperatura ambiente sala de baterías UPS: +22 ºC
- Rango de humedades de trabajo: según lo establecido en las recomendaciones de ASHRAE TC9.9 para equipos clase A1 sin hacer control exhaustivo de los puntos de consigna: - 9 ºC a +15 ºC punto rocío y 60 % humedad relativa.

Para elegir la tecnología más adecuada es necesario estudiar con atención las condiciones climáticas equivalentes anuales. Comparándolas contra los límites recomendados por ASHRAE se obtiene:

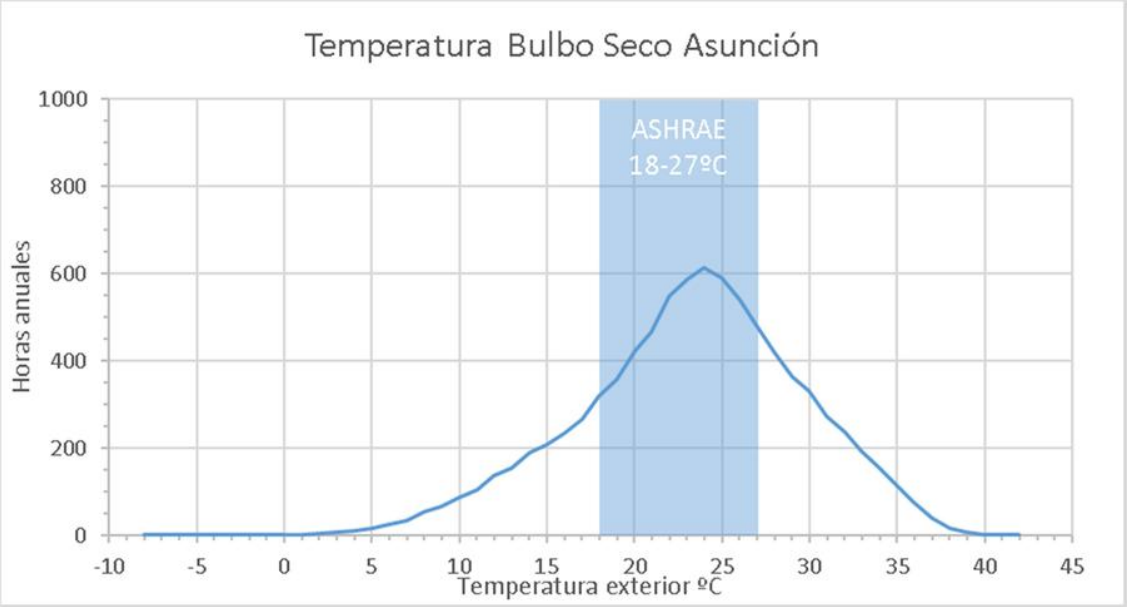


Figura 28 Temperatura bulbo seco Asunción

Fuente Elaboración propia

Temperatura bulbo seco:

- Temperaturas < 18 ºC hay 1.601 horas anuales
- Temperaturas > 27 ºC hay 2.710 horas anuales

En cuanto al punto de rocío:

Figura 29 Temperatura punto de rocío Asunción

Fuente Elaboración propia

- Temperaturas < 9ºC no existen
- Temperaturas > 15ºC hay 6152 horas anuales

Así pues, los valores altos de humedades a lo largo del año de 6152 horas anuales (70% del tiempo) demuestran que será indispensable deshumidificar la sala durante todo el año a fin de mantener ciertas condiciones correctas. Esto limita el uso de sistemas de expansión directa o de agua fría a 7/12 ºC.

La posibilidad de utilizar economizadores para el uso de free-cooling directo se descarta pues si bien se podrían llegar a utilizar casi 2610 horas, los cerramientos de las compuertas no serían totalmente estancos, lo cual incrementaría la humedad y el consumo energético.

El uso de sistemas de agua enfriada no es eficiente sino se realizan a altas temperaturas (agua fría >15 ºC). Son mucho más eficientes los sistemas de expansión directa condensados al aire, con compresores de última generación tipo invertir o digital y válvulas de expansión electrónica.

Queda la posibilidad de utilizar un sistema condensado al agua con baterías de free-cooling indirecto. Ahora bien, el análisis preliminar si bien permite realizar free-cooling completo hasta temperatura de 17-18 ºC y modo mixto hasta temperatura de 27 ºC, no existe ningún ahorro energético asociado. Es más, el aumento de consumo aumenta en un 17 %.

Para realizar los cálculos energéticos se recomienda considerar:

- Una potencia de UPS del 60% estable a lo largo del año,
- Temperatura de suministro de 22 ºC
- Temperatura de retorno de 30 ºC
- Todos los equipos de clima trabajando, con sus ventiladores funcionando a la mínima velocidad para mantener las condiciones.

Así pues, se recomienda el uso de sistema de climatización basado en expansión directa condensada al aire.

Estos tipos de sistemas están basados únicamente en circuito refrigerante, el cual circula entre el evaporador, situado dentro de la sala, y el condensador, situado en el exterior. El compresor hace circular el gas refrigerante entre ambas baterías de manera a transferir el calor de adentro hacia fuera. Para realizar el intercambio, una válvula de expansión, baja bruscamente la presión del refrigerante, disminuyendo a su vez la temperatura. El gas refrigerante al estar expuesto al aire caliente interno, se caliente, enfriando a su vez el aire de la sala. El compresor absorbe el refrigerante, comprimiéndolo, y aumentando su presión y temperatura para llevarlo posteriormente al condensador. El refrigerante al estar en contacto con el aire exterior que está a menor temperatura, disipa todo el calor interno. Posteriormente el refrigerante vuelve a llegar a la válvula de expansión iniciando una vez más el ciclo.

Figura 30 Ejemplo de unidad de climatización basado en expansión directa

5.4.2 *Equipos mecánicos para sala IT*

Climatizadoras

A partir de la carga IT a soportar se plantea la instalación de:

- Fase 1: 5 equipos en configuración n+1 en cada sala (convencional y cofre)
- Fase 2: 5 equipos adicionales en configuración n+1 en cada sala (convencional y cofre)

Cada equipo estará constituido de una unidad interna (CRAC) y dos unidades externas (condensadoras), las características de las cuales deben ser las siguientes:

Unidades internas – CRAC:

- Potencia frigorífica neta sensible: 105 kW/unidad
- Caudal de aire: 26.000 m3/h a 20 Pa de presión estática disponible
- Compresores scroll en tandem de regulación variable tipo inverter o digital emparejados 2 a 2 con compresores scroll convencionales.
- Doble circuito por equipo.
- Válvulas de expansión electrónica por circuito.
- Ventiladores EC-fan montados bajo falso suelo.
- Selección de opcionales para eficiencia energética

- Sistema integrado de control de trabajo en equipo mediante control de temperatura en pasillo frío.
- Pantalla de interfaz completa de visualización de los parámetros de funcionamiento del equipo y del conjunto
- Sin baterías de resistencias, sin humectador.
- Bandeja de condensados en acero inoxidable o similar.
- Tubería de refrigerante líquido totalmente aislada hasta condensadora con protección contra UV
- Filtro de partículas mínima EU4
- Supervisión mediante Modbus IP o Bacnet IP.
- Alarmas de contacto seco
- ATS con doble alimentación
- Protección de fases.

Unidades externas – Condensadoras:

- Ventiladores EC
- Control mediante señal de equipo CRAC
- Tratamiento epoxy en baterías de condensación a fin de alargar la vida de los equipos.
- Dimensiones lo más grandes posible a fin de reducir el consumo del compresor.
- Instaladas lo más cerca posible de las unidades interiores. A poder ser, inferior a 15 metros y con un diferencial de altura inferior a 5 metros.

Humectadores

Después del análisis preliminar, se concluye que no es necesario un sistema de humidificación.

Renovación de aire

El sistema de renovación de aire se realizará según normativa local intentando reducir al máximo el número de renovaciones a lo estrictamente necesario pues de lo contrario se estaría continuamente introduciendo aire húmedo a la sala IT.

Tendrán las características siguientes:

- Ventiladores EC
- Filtros EU4+EU8
- Compuertas estancas cuando el sistema esté apagado.
- Todas las entradas y salidas de aire de renovación estarán provistas de sus pertinentes compuertas cortafuegos para evitar la propagación de fuego a través del edificio.

Extracción de humos

Se deberá suministrar un sistema de extracción de humos a fin de renovar el aire en la sala después de disparo de agente extintor. El sistema deberá ser diseñado conforme a la normativa local, y poder renovar el aire completo de la sala en menos de 30 minutos.

Cerramiento de pasillo

Es necesario cerrar el pasillo con los materiales adecuados para Centros de Datos, de manera a asegurar las condiciones en el pasillo frío.

La puerta será especialmente diseñada para Centro de Datos que garantiza un ahorro de energía importante. Esto permite aumentar la eficiencia energética de los equipos instalados en su interior debido a la optimización de temperatura, consiguiendo así una refrigeración más directa.

La solución contempla las siguientes características:

- Fabricado en chapa de acero lacado.
- El acceso al sistema se realiza mediante puerta corredera para optimizar el espacio.
- La altura de la estructura es para armarios de 42U.

Figura 31 Ejemplo de cerramiento de pasillo caliente

5.4.3 *Equipos mecánicos para sala UPS*

Climatizadoras

Los equipos de refrigeración de la sala UPS serán de características idénticas a la sala IT, pero con el siguiente dimensionamiento:

- Cantidad de equipos: 2, manteniendo redundancia 1+1
- Potencia frigorífica neta sensible: 30 kW/Unidad
- Caudal de aire: 9.000 m3/h a 20 Pa de presión estática disponible
- Control por temperatura de aspiración de UPS.

Humectadores

Sin sistema de humectación.

Sistema de renovación de aire

De igual manera que la sala IT.

5.4.4 *Equipos mecánicos para sala baterías*

Climatizadoras

Los equipos de refrigeración de la sala baterías serán de características idénticas a la sala IT, pero con el siguiente dimensionamiento:

- Cantidad de equipos: 2, manteniendo redundancia 1+1
- Potencia frigorífica neta sensible: 5 kW/Unidad
- Caudal de aire: 1.500 m3/h a 20 Pa de presión estática disponible
- Control por temperatura en ambiente.

Humectadores

Sin sistema de humectación.

Sistema de renovación de aire

De igual manera que la sala IT,

5.4.5 *Equipos mecánicos para sala NOC, sala CERT-PY, sala reuniones, sala crisis, puesto seguridad, mantenimiento y almacén*

Climatizadoras

El resto de salas que no corresponden a equipamiento IT ni a infraestructuras de soporte electro-mecánicas, serán refrigeradas mediante equipos estándar de confort de alta eficiencia asegurando las adecuadas condiciones interiores:

- Meses de verano:
    - Temperatura de bulbo seco: 23-25 ºC
    - Humedad relativa: 45-60 %
- Meses de invierno:
    - Temperatura de bulbo seco: 21-23 ºC
    - Humedad relativa: 40-50 %

Renovación de aire

Para la renovación de aire se considerará calidades IDA 2, por lo que se requerirá al menos de 60 m^3/h para dichas estancias.

La renovación de aire se realizará mediante filtro EU9.

5.5 Sistemas adicionales

5.5.1 *Sistema de control y supervisión*

El sistema de control y supervisión es un sistema vital para gestionar, comprender y automatizar los procesos que ocurren dentro del Centro de Datos. Éste estará en basado en un BMS de protocolo abierto.

El sistema monitorización y control ofrece:

- Solución abierta, sin depender de ningún sistema privativo de fabricante
- Completamente personalizable a las necesidades del cliente
- Acceso universal a la información, desde cualquier lugar y cualquier momento
- Gestión de alarmas y acciones
- Histórico de datos, con gráficos y panales de control personalizados
- Accesible y fácil de usar
- Mantenimiento preventivo, previendo posibles problemas
- Operación pro-activa de la instalación
- Optimización energética y agua

El sistema va a permitir controlar y supervisar:

- Sensores de temperatura
- Sensores de humedad
- Sensores de presión
- Sensores de presencia de agua
- Medidores de potencia
- Alarmas de equipos
- Señales analógicas y digitales

- Señales mediante Modbus y otros protocolos industriales
- Interruptores, mecanismos…

La supervisión se realizará mediante:

- Software de monitorización instalado por duplicado en un PC de la sala NOC y en otro del puesto de seguridad.
- Modem GSM
- Envío de alarmas mediante SMS y correo electrónico.

El sistema será diseñado para ser completamente redundante en 2N, y asegurando la rápida respuesta en caso de incidente.

La definición de los parámetros a supervisar y a controlar serán definidos durante la ingeniería del proyecto.

5.5.2 *Control de acceso y vigilancia*

Se instalará un sistema de control de acceso global basado en tecnología biométrica para todo el Centro de Datos que regule el acceso a sólo personal autorizado a cada uno de los espacios.

Así pues, en cada una de las puertas de acceso habrá un dispositivo mediante sensor biométrico que autoriza únicamente el paso a las personas autorizadas sin que estas puedan prestar temporalmente a terceras.

El sistema contará con un histórico de datos que permitirá saber quién ha entrado en cada momento en las distintas salas.

El control de acceso se realizará también a nivel de pasillo de sala IT y racks, evitando que personal no autorizado pueda acceder a equipos IT de cualquier institución.

Así mismo, todo el perímetro del Centro de Datos, así como su interior será supervisado mediante un circuito cerrado de televisión (CCTV) completamente independiente al resto de sistemas. El sistema permitirá la grabación de imágenes durante al menos un mes para hacer un seguimiento de las operaciones y acciones que se llevan a cabo.

El sistema contará con una capacidad de hasta 32 cámaras en toda la instalación y podrá ser supervisado desde la sala NOC del Centro de Datos y desde el puesto de seguridad.

Con respecto a las características físicas de los sistemas electrónicos de seguridad y protección pasiva se contempla:

- Puertas de seguridad. El marco deberá estar fijado al muro con espárragos de sujeción y dispondrá de 3 bisagras de seguridad.

- Para el acceso a sala IT, se debería disponer de un sistema de doble control, como ejemplo de modelo de control: acceso formado por lector de tarjeta y biométrico (lector de huella). Dicho sistema se definirá junto con el resto de modelos de control de accesos, puede ser doble chequeo con huella o con teclado (PIN). Para el resto de salas se dispondrá de un sistema simple, por medio de lectores de tarjetas.
- Contacto magnético para montaje empotrado en puertas separación máxima 9 mm.
- APO (alarma por omisión) asociada al contacto magnético de la puertas con control de acceso para que de alarma en caso de permanecer abierta un determinado tiempo.
- Detectores doble tecnología infrarrojos y microondas en banda k mínima penetración en paredes, supervisado, tamper, led de prueba, detección con adaptación de patrón y compensación de temperatura para reducir las falsas alarmas, desplegados por el Centro de Datos.
- Pulsador de apertura de emergencia, debidamente protegido y conectado a la Central de supervisión de Alarmas.

5.5.3 *Protección y extinción de incendios*

La protección contra incendios se realizará a diferentes niveles:

- Detección precoz
- Detección convencional
- Extinción automática
- Extinción manual

Según la criticidad del espacio serán utilizados mayor o menor nivel de protección.

Detección precoz

El sistema precoz altamente sensible supervisa continuamente la presencia de partículas de precombustión o combustión en al menos 4 niveles de alarma. Desde el primer nivel, se envían alarmas de aviso de incendio. En caso de llegada al cuarto nivel, el sistema enviaría una señal de disparo de extinción.

El sistema más extensamente utilizado es VESDA, especialmente indicado para aplicaciones de alta sensibilidad como son los espacios IT. La sensibilidad es completamente programable evitando falsas alarmas.

Las características que deben tener estos sistemas son:

- Amplio rango de sensibilidad
- Detección de humo por medio de láser
- Al menos 4 niveles de alarma configurables
- Aspiradores de alta eficiencia

- Inmunidad al polvo, humedad y cambios de temperatura
- Relees programables
- Registro de eventos

Este sistema será instalado en las siguientes salas:

- Salas IT (Convencional y Cofre)
- Sala UPS y Baterías A, supervisado por un único sistema
- Sala UPS y Baterías B, supervisado por un único sistema

El resto de salas serán supervisadas mediante un sistema convencional de detección de incendios.

Detección convencional

El sistema convencional de incendios está compuesto por sensores ópticos fotoeléctricos distribuidos en el espacio a supervisar. En caso de detección de humo en una zona el sistema activa la alarma de incendio, y en caso de detección en dos zonas, el sistema autoriza la extinción automática (si estuviera conectada).

Los elementos principales del sistema de detección de incendios son:

- Central de detección convencional de incendios para detección y/o extinción automática
- Detectores ópticos fotoeléctricos de humo cruzados con base de montaje, led indicador y base para tubo visto
- Pulsador de disparo de extinción con tapa de protección
- Pulsador de parada de extinción con tapa de protección
- Letrero de señalización de extinción disparada
- Alarmas acústica-luminosas mediante sirenas

Este sistema será instalado en todas las salas y espacios del Centro de Datos.

Extinción automática

El agente extintor es un elemento esencial pues en un Centro de Datos debe cumplir dos funciones básicas:

- Extinguir cualquier incendio que pudiera afectar a la integridad y operación
- Asegurar la integridad y el funcionamiento de los equipos IT y los datos que contienen tanto en caso de incendio como en caso de falsa alarma.

Los agentes que cumplen estos requisitos según la NFPA son:

- Gas inerte de mezcla nitrógeno y argón, el cual es almacenado a elevadas presiones y requiere una sobrepresión de manera a desplazar el comburente del espacio físico
- FM-200, el cual es almacenado a media presión y está en desuso por su impacto medioambiental, el cual realiza una reacción química con el oxígeno eliminando el comburente del espacio físico
- Novec 1230, el cual es almacenado a media presión y aun siendo la solución más cara, actualmente es el agente que ofrece las características más ideales en materia de protección contra incendios. Sus principales características:
    - Absorción de calor al actuar en la reacción en cadena
    - Vida atmosférica: 0,014 años
    - Potencial de calentamiento global: 1 GWP
    - Concentración de diseño 4-6%
    - Conductividad eléctrica: dieléctrico (es utilizado como refrigerante en sistemas de refrigeración líquida directa para sistemas de supercomputación).

Los agentes extintores basados en agua u otro tipo de espuma o líquido pueden afectar seriamente la integridad de los equipos IT.

Así pues el agente elegido será mediante gas Novec 1230.

El sistema se diseñará mediante la utilización de software de cálculo provisto por el fabricante de equipos, con el objetivo de poder garantizar los caudales de descarga exacta de las toberas y asegurar una concentración óptima de gas en todos los puntos del área protegida.

Para la descarga del gas uniformemente en la sala, se dispondrá de una red de tuberías y difusores distribuidos tanto en ambiente como por el suelo técnico.

El sistema vendrá equipado con todos los accesorios necesarios (tipo SEVO) para realizar adecuadamente la extinción de incendios.

Está también contemplado realizar pruebas de presurización (DFT) en las salas a fin de determinar el nivel de estanqueidad de cada una.

En caso de extinción, el sistema responderá de manera a aislar la zona afectada y asegurar la estanqueidad del sistema para que el agente actúe eficazmente.

El sistema será comandado por una central de extinción ubicada en el exterior de cada sala, dicha central incorporará baterías para autonomía y una placa/modulo con relés auxiliares.

El sistema tendrá pulsadores de bloqueo/paro y de disparo en caso de emergencia a la entrada de la salas con extinción automática, de manera que en caso de aviso de disparo intempestivo sea posible la interrupción del aviso de disparo al panel de control del sistema de extinción, o en caso de fallo del sistema automático de disparo el pulsador de emergencia para disparo permita su activación por simple actuación de una persona. Habrá letreros luminosos que se

activaran en caso de aviso de disparo; dichos letreros están ubicados junto a dintel de puerta de acceso.

La actuación del sistema de extinción está programada para una detección cruzada. Es decir, el comienzo de la extinción se realizará cuando entren en alarma dos detectores.

Este sistema será instalado en las siguientes salas:

- Salas IT (Convencional y Cofre)
- Sala UPS y Baterías A, supervisado por un único sistema
- Sala UPS y Baterías B, supervisado por un único sistema

Extinción manual

La extinción manual debe estar prevista en el proyecto según normativa local. Ahora bien, se realizará de acorde a las exigencias de un centro de procesamiento de datos. Así para cada uno de los espacios será utilizado un sistema de extinción manual diferente.

Salas IT (Convencial y sala Cofre)

No se requerirá ningún extintor manual, debido a la existencia de dispositivos de disparo manual (pulsadores) del sistema de extinción automática.

Sala UPS y de baterías

No se requerirá ningún extintor manual, debido a la existencia de dispositivos de disparo manual (pulsadores) del sistema de extinción automática.

Sala NOC, sala de crisis, sala CERT-PY y sala de reuniones

Se preverán los extintores manuales adecuados según normativa vigente.

Salas proveedores y sala de Telecomunicaciones

Se preverán los extintores manuales adecuados según normativa vigente.

Almacén, sala seguridad, sala capacitación y mantenimiento.

Se preverán los extintores manuales adecuados según normativa vigente.

Espacios comunes

Se preverán los extintores manuales adecuados según normativa vigente.

Grupos electrógenos y depósitos de combustible

Se preverán los extintores manuales adecuados según normativa vigente.

Casetas de transformación

Se preverán los extintores manuales adecuados según normativa vigente.

Zonas exteriores

Se preverá una boca de incendios equipada (BIE) para su uso únicamente en el exterior y no dentro del Centro de Datos.

Adicionalmente se preverá un hidrante de incendio para uso de bomberos.

5.5.4 *Racks*

Los racks deben ser especialmente concebidos para instalaciones donde la seguridad y la estabilidad son importantes factores para ser considerados.

Los armarios son muy flexibles posibilitando la instalación de toda la diversidad de equipos IT y networking disponible en el mercado para tamaños estándares. Entre otros: cableado estructurado, networking, servidores, equipos IT…

Los armarios están fabricados de acorde a las normativas ANSI T1.336 y ANSI T1.336.

Los racks están compuestos por:

- Montantes de la caja estructural 19”.
- Conexión a tierra directa.
- Soportes ajustables en altura.
- Soportes antisísmicos.
- Puertas especiales para equipos IT, asegurando ventilación y apantallamiento electromagnético.
- Paneles laterales desmontables.
- Puerta delantera de acero de una hoja con perforación del 83 %, y puerta trasera de acero de doble hoja con perforación del 83 %.
- Patas niveladoras (0-25 mm), capacidad de carga 15.000 N estático.
- Bastidor con estructura de aluminio ligera y con unión en las esquinas con piezas macizas para el anclaje de perfiles dando mayor rigidez a su estructura.

Los racks previstos a ser instalados serán:

40 racks para equipos IT repartidos entre la sala convencional (30 racks) y la Sala Cofre (10 racks). Todos estos racks serán cerrados con paneles perforados en su parte delantera y trasera (con doble puerta), disponiendo de cerradura de llave y combinación.

Adicionalmente se contemplan 6 racks de distribución HDA.

Todos los racks serán de la misma altura de 42 unidades (“u” de rack) para una homogeneidad y facilidad de cerramiento del pasillo frio.

En los dos cuartos de proveedores de servicios 1 y 2 se contempla la capacidad de instalar 4 racks en cada uno (montándose 3 de inicio), así como ODFs para finalización de los cableados de fibra óptica.

El cuarto de telecomunicaciones contará con 2 Racks tipo MDA (Main Distribution Area – Core para comunicaciones) y 6 Racks tipo GC (rack de comunicaciones).

Todos los racks irán anclados al suelo sobre una estructura de suportación a fin de mitigar los efectos de sismos.

Todos los racks tendrán provista una conexión directa al mallado de tierra a fin de cumplir con los requisitos de la TIA-942 y BICSI-002.

5.5.5 *Cableado de datos*

Esquema de distribución

El cableado de datos ha sido diseñando los criterios de la TIA-942 y BICSI-002.

Se ha seguido un diseño jerárquico cumpliendo con todos los requisitos del nivel Tier III, y la máxima cantidad de los niveles de la TIA-942.

El esquema de distribución sería el siguiente:

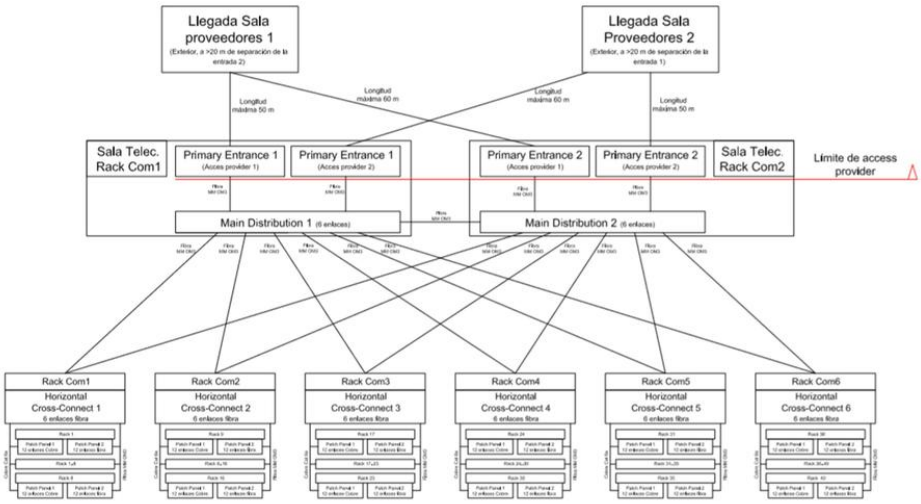


Figura 32 Esquema del cableado de datos estructurado

Se considera dos salas de proveedores de acceso de comunicaciones. Los accesos de cableados estarán físicamente separados en el exterior por una distancia superior a los 20 metros, tal y como estipula la TIA-942.

De cada punto de acceso se hará llegar mediante canal soterrada de metal flexible una conexión a las dos entradas primarias del Centro de Datos, tal y como estipulado en la TIA-942. Es decir, cada entrada primaria estará conectada con ambos proveedores de acceso.

Tanto las entradas primarias como los puntos de distribución principales estarán situados en dos racks de comunicaciones independientes y separados.

El límite de responsabilidad de los proveedores de acceso de comunicaciones acaba justo en el enlace de los racks.

De cada acceso primario, partirá cableado de fibra óptica de calidad MM OM3 hacia los puntos de distribución principales.

Habrá un enlace de fibra óptica MM OM3 entre los dos puntos de distribución principales, de manera a aumentar la redundancia.

De cada punto de distribución principal se realizarán 6 enlaces de fibra MM OM3 a cada punto de distribución horizontal.

Los puntos de distribución horizontal estarán situados rack tipo end-row de cada fila.

En cada punto de distribución horizontal se realizará un precableado entre el rack end-row y cada rack con fibra óptica y cable de cobre según las características de la fila:

- enlaces de cobre Cat 6a
- enlaces de fibra MM OM3

Cableado de cobre

Todo el cableado de cobre debe garantizar la calidad del producto y servicio.

Todas las salidas/conectores de telecomunicaciones deberán ser categoría 6A de 500 MHz, estar diseñadas para la terminación de cable de cobre de par trenzado balanceado apantallado de cuatro pares, y poseer como mínimo las siguientes características:

- Exceder el rendimiento de componente para categoría 6A en el rango de frecuencias de 1 hasta 500 MHz.
- Estar disponible en 12 colores.
- Que su diseño permita su instalación desde el frente o desde atrás de la placa frontal permitiendo su paso a través de la placa sin necesidad de reterminaciones.
- Que su diseño permita su montaje en la placa en orientación plana o angulada.
- Permitir su terminación completa en 60 segundos.
- Que incluya módulo de terminación libre de cruzamientos de pares.
- Proveer una herramienta de terminación por cada paquete de 20 conectores.
- Ser compatible retroactivamente con hardware y cables de menor categoría manteniendo el máximo rendimiento de éstos.
- Permitir ambas opciones de configuración T568A o T568B en cada toma modular.
- Que tenga los contactos en diagonal para maximizar distancia entre hilos y minimizar ANEXT
- Que incluya cuatro iconos diferentes para identificación de circuitos.
- Permitir un mínimo de 5 reterminaciones sin degradación de señal.
- Estar fabricado con nylon reforzado con vidrio de alto impacto.

- Tener una cobertura de blindaje metálico de 360°.
- Estar construido con un termoplástico retardante a la flama UL 94 V-0.
- Estar libre de plomo, libre de PVC y libre de halógenos.
- Que su interfaz (jack) permita hasta 2500 ciclos de inserciones de plugs.
- Soportar PoE y PoE+.
- Cumplir y exceder las normas TIA-568-B.2-10, ISO/IEC 11801:2002 1a enmienda, IEC 60603-7, IEEE 802.3an, IEEE 802.3af y TIA-968-A.
- Tener disponible una opción que pueda ser montada en una abertura IEC 60603-7 (keystone).
- Deberá estar certificado por Underwriters Laboratories o entidad acreditada similar.

Todos los patch panels deberán permitir la conexión cruzada y la interconexión por medio de cordones modulares, cumplir con los requisitos de montaje en racks de 19" y poseer como mínimo las siguientes características:

- Estar disponible en versiones de paneles vacíos o precargados con conectores blindados categoría 6A.
- Estar disponible en versiones planas y anguladas de 24 puertos en 1 unidad de rack (1RMS = 44.5 mm [1.75 in.]).
- Estar disponible en versiones planas y anguladas de 48 puertos en 1 unidad de rack (1RMS = 44.5 mm [1.75 in.]).
- Estar diseñados para montaje en racks de 19".
- Permitir la conexión automática a tierra de sus módulos blindados al ser insertados.
- Estar fabricados con acero ligero de alta resistencia mecánica con un acabado durable en color negro.
- Tener lengüetas de rápida liberación que permite desinstalar fácilmente los módulos individuales incluso en situaciones de alta densidad.
- Tener números de identificación de puertos en el frente del panel
- Tener integrado un organizador de cable posterior.
- Estar provistos con portaetiquetas magnificadores de alta visibilidad que pueden contener etiquetas de papel o iconos para identificación de puertos.

Todos los cables F/UTP deberán ser categoría 6A de 500 MHz y poseer como mínimo las siguientes características:

- Tener un forro de cable de forma cilíndrica disponible en opciones LSOH, CMR, CMP, CM y con un diámetro externo nominal menor o igual a 7.4 mm (0.29 in)

- Tener una construcción consistente en cuatro pares de conductores de cobre sólido de 0.57mm (0.02 in) (24AWG) de diámetro, con un elemento aislador central que mantenga la geometría de par para un rendimiento óptimo en NEXT
- Tener una película de celofán que rodee todo el conjunto de los pares del cable, un alambre de drenado y una pantalla de aluminio rodeando todo el conjunto.
- Estar disponible en carretes de 305 m, 500 m y 1000 m
- Estar disponible en varios colores de forro. Azul – CMR y CMP, Gris – CMX, y Violeta - LSOH
- Cumplir con los parámetros de rendimiento y eléctricas de la TIA-568.

Cableado de fibra

Todos los centros de interconexión, paneles y unidades de bandejas para fibra óptica deberán tener los medios y accesorios que permitan la conexión cruzada, interconexión, empalme, acomodo y administración de jumpers y pigtails; además de poseer como mínimo las siguientes características:

- Su tamaño no debe ser mayor a una U y debe poder acomodar hasta 48 puertos dúplex en cassetes MPO con adaptadores LC en el otro extremo, o bien 3 adaptadores MTP-MTP de hasta 8 conectores cada uno.
- Debe tener placas adaptadoras ciegas para crecimiento futuro de la infraestructura de fibra.
- Debe tener placas adaptadoras de 6, 8 y 12 puertos (dúplex) de fibra que permitan la codificación por colores de los conectores.
- Debe tener placas adaptadoras con mecanismo de engarce y retiro utilizando un solo dedo.
- Debe tener una cubierta frontal que pueda usarse como superficie de rotulado y para proteger los jumpers. Esta cubierta debe permitir su reubicación a otra posición durante la terminación para mantener la identificación de circuitos.
- Los modelos de tres adaptadores deben estar disponible con un mecanismo deslizable que permita al panel deslizarse hacia el frente o hacia atrás, y debe tener seguros desmontables que permitan su retiro del rack o gabinete.
- Debe estar certificado por Underwriters Laboratories.

Todos los cables de fibra óptica multimodo, usados para el cableado de datos, deberán poseer como mínimo las siguientes características:

- Estar disponible en cualquier longitud en incrementos de 5m, y otras longitudes bajo pedido.

- Cable RazorCore de diámetro 3mm (para 12 fibras), que debe estar disponible con cubierta CMR, CMP y LSOH.
- Estar disponible en fibra multimodo standard 50/125□m, 62.5/125□m y 50/125□m optimizada para láser.
- Tener un sistema de conexión sencillo, que sólo consiste en introducir los enchufes en los módulos, y éstos en la bandeja de fibra
- Estar disponible en bobinas con conectores MTP de 12 fibras en cada extremo.
- Venir equipadas con una "asa de tracción" en un extremo para facilitar su instalación.
- Ofrecer la posibilidad de una bobina de "alargo" para permitir añadidos en las instalaciones existentes Plug & Play, e incluir un adaptador para unir el alargo con el extremo de la bobina. .
- Estar testeado en fábrica el 100%.
- Cumplir como mínimo con los rendimientos de la TIA-568.

5.5.6 *Emergency Power Off (EPO)*

La última actualización de la normativa de la TIA-942 no exige ningún requerimiento en relación a los sistemas de parada de emergencia – EPO (Emergency Power Off).

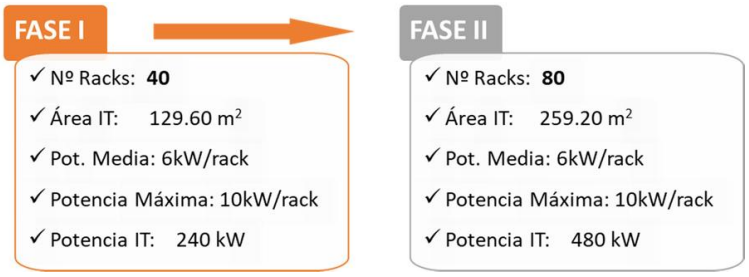
Así mismo, la Tier Topology del Uptime Institute avisa de ser un sistema que introduce un punto singular de fallo.

De esta manera se decide no instalar ningún sistema EPO en la instalación.

Ahora bien, durante la implementación del proyecto y si fuese necesario para seguridad de los operarios de mantenimiento se podrá contemplar la instalación de sistemas EPO individuales en aquellos equipos donde se considere por parte de SENATICs para evitar riesgos durante la puesta en funcionamiento de los equipos durante su mantenimiento. En ningún caso estos sistemas afectarán al resto de equipos ni a la operación del Centro de Datos.

5.6 Descripción de las fases de la solución propuesta

El Centro de datos propuesto se puede desarrollar en dos fases, en dependencia del crecimiento y necesidades. Ambas fases se han diseñado para una disponibilidad TIER III y con una fachada de panel de acero lacado.



FASE I

Nº Racks: 40

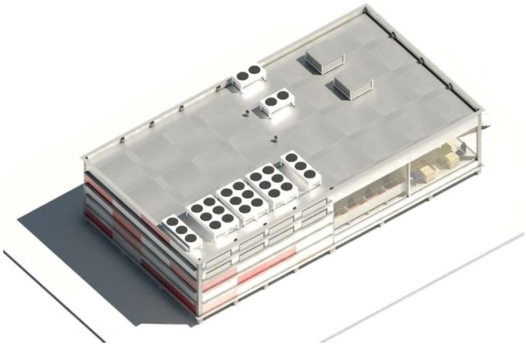
Pot. Media: 6kW/rack

Potencia Máxima: 10kW/rack

Potencia IT: 240 kW

Disponibilidad Tier III

Fachada: Panel Acero Lacado



FASE II

Nº Racks: 80

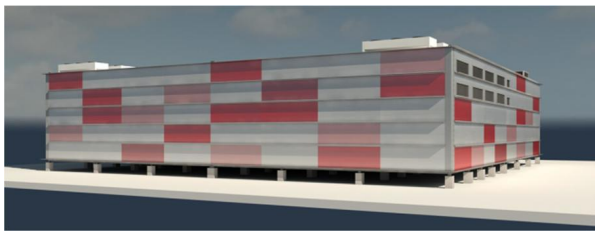
Pot. Media: 6kW/rack

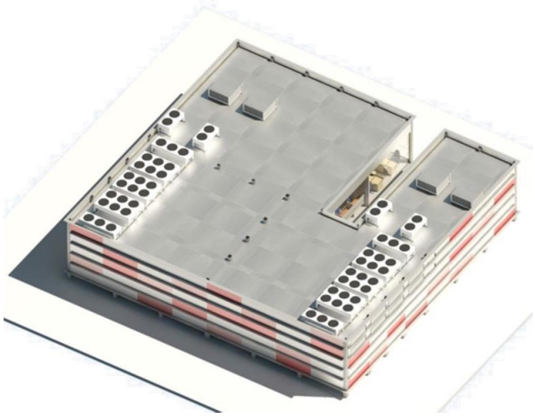
Potencia Máxima: 10kW/rack

Potencia IT: 480 kW

Disponibilidad: Tier III

Fachada: Panel Acero Lacado





5.7 Gestión del proyecto

Para la gestión del proyecto hay cuatro componentes básicos a tener en cuenta:

- Ingeniería de apoyo.
- Project management.
- Controles de calidad.
- Planificación del proyecto.

5.7.1 *Ingeniería de apoyo*

Es preciso contar con un equipo de oficina técnica que será responsable de:

- Realizar el diseño de todas las soluciones técnicas y de la integración de las mismas
- Realizar todos los planos y documentación necesaria para llevar a cabo el proyecto
- Dar soporte en la coordinación y dirección de obra
- Dar soporte en el proceso de compras
- Dar soporte en los controles estipulados de puesta en marcha y entrega de proyecto

El equipo de oficina técnica estará formado al menos de:

- 1 Ingeniero especializado en diseño y ejecución de Centro de Datos
- 1 Ingeniero geotécnico para revisión de la obra civil
- 1 Arquitecto superior para diseño y dirección de obra civil
- 1 Ingeniero eléctrico especializado en Centro de Datos y servicios críticos
- 1 Ingeniero termodinámico especializado en instalaciones mecánicas de servicio crítico
- 1 Técnico especialista en ejecución y puesta en marcha de Centro de Datos Modulares
- 1 Ingeniero de telecomunicaciones especializado en networking.

5.7.2 *Project management*

La dirección facultativa del proyecto debe ser ejecutado por un especialista asignado, Project Manager. El P.M. es responsable de:

- Aprobación de cada una de las fases del proyecto
- Aprobación de todas las soluciones técnicas.
- Entregar todos los componentes acordados en el pedido del cliente.
- Transporte y coordinación el descargar en el sitio de cliente.
- Coordinación de los instaladores.
- Horario y planeamiento de la instalación, según lo que quede acordado con la SENATICs.
- Supervisión de la instalación y coordinación en sitio.
- El control de calidad de las pruebas necesarias.
- Vigilancia y correcciones en los acabados.
- Obtención del certificado de emisión de calidad.

Cada partida se planifica individualmente y toda la información de horarios y tiempo se comparte y se ajusta con los instaladores.

El control de calidad es verificado por el P.M. según las pruebas siguientes:

- Inspección visual de todos los componentes.
- Pruebas aleatorias de cada componente.
- Relación cercana durante la instalación.
- Prueba funcional de cada componente según el método de prueba previamente definido para cada equipo o sistema, en general según fabricante.

Cualquier corrección requerida será hecha por el instalador específico. Ningún instalador puede considerar su trabajo terminado hasta obtener la aprobación firmada por el P.M.

La entrega de la documentación incluye:

- Memoria de la ingeniería y de instalación.
- Libros con instrucciones y garantías.
- Manual de operación y mantenimiento del Centro de Datos
- Planos y esquemas as-built de la instalación.
- Certificados y documentación adicional de los materiales y/o equipos.

5.7.3 *Controles de calidad*

Para cada una de las fases del proyecto se requerirá la aprobación del cliente (la SENATICs o quien se asigne en representación para dichas cuestiones) para poder proseguir con las tareas. Los puntos importantes son: ingeniería básica e ingeniería de detalle.

Para los principales equipos se requerirá pruebas en fábrica: Factory Acceptance Test, que deberán ser aprobadas por el equipo de Commissioning, el P.M. y el cliente (las personas que defina para tal efecto la SENATICs).

Durante la ejecución del proyecto y a medida que se vayan ejecutando las partidas se realizará el comisionado y la puesta en marcha individual de los sistemas. Se requerirá la aprobación del equipo de Commissioning y el P.M. para cada una de ellas.

Antes de la entrega a la SENATICs, se realizará una prueba del sistema completa: Integrated System Test, en el cual se simulará la operación del Centro de datos mediante bancos de prueba. Se realizará pruebas, el protocolo de las cuales deberá ser aprobado por el los participantes en el proceso (equipo de Commsioning, el P.M. y la SENATICs) antes.

Antes de la entrega de llaves (finalización formal de los trabajos), se realizará una aceptación del proyecto: Site Acceptance Test. En el cual, la SENATICs revisará todos y cada uno de los sistemas para verificar que se cumplen los requerimientos establecidos en el contrato de construcción del Centro de Datos.

Por último se realizará una formación detallada al personal que vaya a gestionar el Centro de Datos, y una formación resumida a las personas que la SENATICs considere oportuno.

5.7.4 *Planificación del proyecto*

El proyecto está previsto en poder ser ejecutado en un plazo de 9 meses desde el momento que se cuenten con los permisos y aprobaciones pertinentes para su inicio.

Todos los retrasos debidos a terceras empresas y/o obtención de permisos no estarían considerados en la previsión descrita.

5.8 Certificación del proyecto

El proyecto ha sido completamente evaluado para que la SENATICs, en caso de requerirlo, pueda certificarlo según el nivel **Tier III** del **Uptime Institute**, tanto en documentos de diseño como proyecto construido.

Es preciso que durante todo el desarrollo del proyecto desde la fase más incipiente con el desarrollo de soluciones y diseño se cuente con empresa de apoyo que supervise y garantice que toda la documentación y trabajos de construcción están alineados para obtener la certificación. Se requerirá el apoyo de empresas especializadas en dicha materia que deben avalar su experiencia al respecto con casos concretos contrastables.

Los servicios a requerir son:

- Preparación de la documentación para certificación de los documentos de diseño.
- Acompañamiento durante la certificación de los documentos de diseño.
- Preparación de la documentación para certificación del proyecto construido.
- Acompañamiento durante las pruebas de la certificación del proyecto construido.
- Acompañamiento durante la certificación del proyecto construido.

6 Partidas del proyecto

A continuación, se presenta el contenido de las diferentes partidas consideradas en el proyecto de Centro de Datos. Se han considerado los mejores fabricantes y mejores soluciones para cada caso.

6.1 EXTERIORES

6.1.1 Vallado perimetral

6.1.1.1	Valla de alta seguridad especialmente diseñada de un modo que no se puedan trepar ni cortar. La separación entre los centros de los alambres comprende 12,7 mm (vertical) x 76,2 mm (horizontal) Compuesta por paneles de mallazo plano electrosoldado constituido a partir de alambre de acero Tipo 5T22 (Norma UNE 36 089) de 4 mm de diámetro (AWG 8).	1
6.1.1.2	La valla va sujeta a unos postes que son vigas tipo IPE 120 embutidas en dados de hormigón de 0,4 m x 0,4 m x 1 m. Los paneles estándar de alambre de acero electrosoldado tendrán una altura de 4 m y una anchura máxima de 2,5 m.	1
6.1.1.3	Puerta automática metálica corredera de una hoja o movimiento horizontal deslizante. Compuesta por una hoja de bastidor rectangular de barrotes. Con sistema de control de acceso incluido	1
6.1.1.4	Puerta giratoria mecanizada formada por tres hojas de 2,20 cm de altura, de diámetro 2000 mm. Puertas y cilindro de protección formadas por perfiles tubulares de acero. Control de acceso incluido.	1
6.1.1.5	Sistema de videoportero para puertas peatonal y de vehículos	2
6.1.1.6	Sistema de CCTV compuesto por 8 cámaras con infrarrojos (2 en cada lado del perímetro exterior)	1
6.1.1.7	Sistema ANPR para reconocimiento automático de números de matrícula de autos	1

6.1.2 Cimentación

6.1.2.1	Excavación de rasa para losa de cimentación de suelo compacto mediante retroexcavadora hasta 2 metros de profundidad y transporte de tierras con camión.	1
6.1.2.2	Relleno de material granular de piedra granítica (gravas), de 50 a 70 mm de grosor, en tongadas de 25 cm como máximo (debajo de losa de cimentación), colocación y compactación del mismo.	1
6.1.2.3	Hormigón para losa de cimentación de 25 cm de canto (aligeramiento) HA-25/B/20/IIa de consistencia blanda y tamaño máximo del árido de 20 mm, desde camión, con una cuantía media de 25 kg/m2.	1
6.1.2.4	Hormigón para losa de cimentación de 40 cm de canto (aligeramiento) HA-25/B/20/IIa de consistencia blanda i tamaño máximo del árido de 20 mm, desde camión, con una cuantía media de 30 kg/m2.	1

6.1.2.5	Hormigón de limpieza para losa de cimentación, de espesor 10 cm HM-20/B/20/IIa de consistencia blanda i tamaño máximo del árido de 20 mm, desde camión.	1

6.1.3 Solera

6.1.3.1	Pavimento de hormigón HM-30/b/20/I+F de consistencia blanda tamaño máximo del gran. de 20mm escampado con transporte interior mecánico y vibrado mecánico y acabado manual	1
6.1.3.2	Boca de incendios equipado (BIE)	1

6.1.4 Urbanización parcela y viales

6.1.4.1	Preparación del terreno total que cubrirá la parcela/vallado	1
6.1.4.2	Acondicionado y asfaltado de las zonas de tránsito para vehículos, incluida la parte proporcional de pintura para su delimitación	1
6.1.4.3	Aparcamientos para autos (con zonas diferencias para visitas y clientes, así como para carga y descarga de materiales)	1
6.1.4.4	Acondicionamiento de espacio para punto limpio donde se ubicaran de jaulas/contenedores de reciclaje	1
6.1.4.5	Preparación del terreno donde se colocaran los servicios exteriores (Centros de transformación y grupos electrógenos y depósitos de combustible asociados)	1
6.1.4.6	Canalizaciones eléctricas soterradas de suministro de compañía eléctrica hasta Centros transformación Estará compuesta de 4 tubos corrugados 90mm. Incluidas las arquetas prefabricadas de hormigón para apoyo a la instalación y a su futuro mantenimiento.	2
6.1.4.7	Canalizaciones eléctricas soterradas desde los Centros transformación al Centro de Datos	2
6.1.4.8	Canalizaciones eléctricas soterradas desde Grupos electrógenos al Centro de Datos	2
6.1.4.9	Canalizaciones telecomunicaciones soterradas Consistentes en 6 tubos corrugados 90mm desde arqueta exterior del vallado, desde donde accederán los proveedores (carriers). Incluida la instalación de 2 monotubos 40mm en dos de los tubos corrugados (total 4 monotubos) para facilitar la instalación de los primeros cables de fibra óptica. Incluidas las arquetas prefabricadas de hormigón para apoyo a la instalación y a su futuro mantenimiento.	2

6.1.5 Instalación y gestión del proyecto

6.1.5.1	Estudio Geotécnico del terreno	1
6.1.5.2	Ingeniería de apoyo a la definición de aspectos constructivos	1
6.1.5.3	Pruebas de calidad por empresa de commissioning	1
6.1.5.4	Dirección del proyecto de obra civil	1
6.1.5.5	Documentación as-built y memoria del proyecto	1
6.1.5.6	Contenedores reciclaje de material	1

6.2 CIVIL

6.2.1 Estructura

6.2.1.1	Pilares metálicos tubulares de acero S275JR de diámetro 323mm y espesor 6 mm de hasta 6 metros de altura.	1
6.2.1.2	Perfiles metálicos tubulares rectangulares de acero S275JR para cordones de cercha de cubierta de dimensiones 250x160 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras a taller incluidas.	1
6.2.1.3	Perfiles metálicos tubulares rectangulares de acero S275JR para montantes y diagonales de cercha de cubierta de dimensiones 180x120 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras a taller incluidas.	1
6.2.1.4	Perfiles metálicos tubulares rectangulares de acero S275JR para bigas riostra de cubierta de dimensiones 300x200 mm y espesor 6 mm de hasta 6 metros de longitud. Soldaduras a taller incluidas.	1
6.2.1.5	Perfiles metálicos IPN400 de acero S275JR para bigas secundarias cubierta de hasta 6 metros de longitud. Soldaduras a taller incluidas.	1
6.2.1.6	Hormigón HA-25/B/20/IIa de relleno de los pilares tubulares, con una cuantía media de 25kg/m3.	1
6.2.1.7	Acero en pletinas S275JR para soporte de pilares en cimentación. Pernos de anclaje incluidos. Soldaduras a taller incluidas.	1
6.2.1.8	Montaje de chapa grecada de acero inoxidable para forjado colaborante de cubierta, 1 mm de espesor y de entre 200 y 210 mm de canto.	1
6.2.1.9	Hormigón para losa de cimentación de 12 cm de canto HA-25/B/20/IIa de consistencia blanda y tamaño máximo del árido de 20 mm, desde camión, con una cuantía media de 15 kg/m2.	1
6.2.1.10	Pintura intumescente de protección antiincendio para una protección R120 de la estructura (pilares y perfilería) (Grosor de hasta 3000 µm)	1
6.2.1.11	Espuma de protección antiincendio para una protección R60 de la cubierta (forjado sandwich). RF120 se obtendrá con armadura.	1

6.2.2 Envolvente fachada

6.2.2.1	Fachada de Panel Acero Lacado, fijados por medios mecánicos; colocado	1

6.2.3 Envolvente cubierta

6.2.3.1	Solución finalizada para ser practicable en la zona donde se vayan a alojar las unidades exteriores de climatización.	1
6.2.3.2	Membrana de densidad superficial 1,15 kg/m2 y espesor 1 mm, de una lámina de etileno propileno dieno (EPDM), colocada no adherida	1
6.2.3.3	Lima hoya de plancha de aluminio de 0,7 mm de espesor, preformada y 45 cm de desarrollo, colocada con fijaciones mecánicas	1
6.2.3.4	Bajante de tubo de PVC-U de pared maciza, área de aplicación B según norma UNE-EN 1329-1, de DN 75 mm, incluidas las piezas especiales y fijado mecánicamente con bridas	1

6.3 INSTALACIONES

6.3.1 Potencia, cableado e iluminación

6.3.1.1	Transformador MT/BT de 1600 kVA	1
6.3.1.2	Transformador redundante MT/BT de 1600 kVA	1
6.3.1.3	Edificio prefabricado de hormigón Compañía/Abonado 2 puertas (1 celda y 1 trf). Contiene separadores recintos de transformadores, tierras interiores, alumbrado interior (2 puntos de luz).	1
6.3.1.4	Cuadro eléctrico de MT III+N (Para sistema TNS) 3 celdas de línea +remonte Automático de protección general + Medida 3TT 3TI + 2 celdas de automático para protección de los trafo con sus relés correspondientes	
6.3.1.5	Centro de transformación redundante	1
6.3.1.6	Generador Diésel 750 kVA	1
6.3.1.7	Generador Diésel redundante 750kVA	1
6.3.1.8	Depósito de combustible 10.000 litros	2
6.3.1.9	Sistema de bombeo de combustible (con doble bomba de trasiego)	2
6.3.1.10	ATS Red-Grupo	2
6.3.1.11	Cableado principal línea A	1
6.3.1.12	Cableado redundante línea B	1
6.3.1.13	Alumbrado 400 lux/m2	1
6.3.1.14	Alumbrado de emergencia	1
6.3.1.15	Protección contra descargas atmosféricas	1
6.3.1.16	Instalación eléctrica	1
6.3.1.17	Instalación eléctrica redundante	1

6.3.2 Sistema de climatización

6.3.2.1	Unidad de clima, incluye sistema free-cooling indirecto mediante intercambiador de placas polimérico, sistema de refrigeración frigorífico DX, ventiladores EC, filtros F5, Interfaz para monitorización	3
6.3.2.2	Unidad de clima redundante, con idénticas especificaciones a las mencionadas en la partida anterior	2
6.3.2.3	Sensores adicionales en pasillo frío y caliente, de temperatura, humedad y presión	1
6.3.2.4	Conductos de retorno/impulsión internos	3
6.3.2.5	Conductos redundantes de retorno/impulsión internos	2
6.3.2.6	Conductos de aspiración/expulsión externos	3
6.3.2.7	Conductos redundantes de aspiración/expulsión externos	2
6.3.2.8	Compuertas cortafuegos RF120	3
6.3.2.9	Compuertas cortafuegos RF120 redundante	2

6.3.3 Protección contra incendios

6.3.3.1	Detectores para salas de grupos electrógenos y centros de transformación conectadas a lazo específico de la central de detección principal	2
6.3.3.2	Extintores manuales	1

6.3.4 Instalaciones especiales

6.3.4.1	Sistema de detección de fuga de líquidos (incluidos central de gestión y cableado con metraje), conectado a BMS	1

6.3.5 BMS

6.3.5.1	Software de gestión de alarmas mediante protocolo abierto	1
6.3.5.2	Controladores para recoger todas las señales de campo, incluidas pasarelas, módulos entradas/salidas tanto de señales digitales como analógicas	1

6.3.6 Sistemas Seguridad

6.3.6.1	Sistema intercomunicadores y videoporteros	1
6.3.6.2	Sistema de control de accesos	1
6.3.6.3	Sistema CCTV basado en tecnología IP-POE, incluyendo cámaras interiores y dos videograbadores de 16 canales	1
6.3.6.4	Sistema de detección de intrusión (con panel central, volumétricos y detectores)	1
6.3.6.5	Cajetines para custodia y gestión de llaves	1

6.3.7 Instalación y gestión del proyecto

6.3.7.1	Pre Auditoria	1
6.3.7.2	Diseño del proyecto según estándar Tier III (Ingeniería Básica y constructiva)	1
6.3.7.3	Pruebas de calidad por empresa de commissioning	1
6.3.7.4	Estudio de Selectividad	1
6.3.7.5	Dirección del proyecto	1
6.3.7.6	Documentación as-built y memoria del proyecto	1
6.3.7.7	Preparación documentación para certificación Uptime Institute	1
6.3.7.8	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.3.7.9	Contenedores reciclaje de material	1

6.4 Salas de proveedores (Carriers)

6.4.1 Estructura

6.4.1.1	Paneles paredes	1
6.4.1.2	Paneles suelo	1
6.4.1.3	Paneles techo	1
6.4.1.4	Estructura de soportación de paneles de techo	1
6.4.1.5	Estructura metálica auxiliar para instalaciones	1
6.4.1.6	Perfilería y acabados	1
6.4.1.7	Puerta con control de acceso	1
6.4.1.8	Estructura completa 2x15 m2	1
6.4.1.9	Pasacables	1
6.4.1.10	Falso suelo carga 1250 kg/m2	1

6.4.2	***Racks y canalizaciones***	
6.4.2.1	Bandeja de datos de 200x60x3000 mm con soportes de refuerzo	2
6.4.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	2
6.4.2.3	Rack Salas de proveedores 42U 600x1000, 1000 kg	6
6.4.2.4	ODFs	2
6.4.3	***Potencia, cableado e iluminación***	
6.4.3.1	Cableado principal de servicios	2
6.4.3.2	Cableado redundante para servicios	2
6.4.3.3	Alumbrado	2
6.4.3.4	Alumbrado de emergencia	2
6.4.3.5	Instalación eléctrica	2
6.4.3.6	Instalación eléctrica redundante	2
6.4.4	***Sistema de climatización***	
6.4.4.1	Unidad de Expansión Directa	1
6.4.5	***Protección contra incendios***	
6.4.5.1	Detector analógico direccionable conectado a la central de detección	2
6.4.5.2	Extinción manual	2
6.4.6	***Control, monitorización, gestión y seguridad***	
6.4.6.1	Control de accesos por lector de tarjeta	2
6.4.7	***Cableado de datos***	
6.4.7.1	Instalación cobre	2
6.4.7.2	Instalación fibra	2
6.4.7.3	Certificación y gestión de garantía cobre	2
6.4.7.4	Certificación y gestión de garantía fibra	2
6.4.8	***Instalación y gestión del proyecto***	
6.4.8.1	Pre Auditoria	1
6.4.8.2	Pruebas de calidad por empresa de commissioning	1
6.4.8.3	Dirección del proyecto	1
6.4.8.4	Documentación as-built y memoria del proyecto	1
6.4.8.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.4.8.6	Contenedores reciclaje de material	1

6.5 Salas de Telecomunicaciones, IXP e interconexión

6.5.1 Estructura

6.5.1.1	Paneles paredes	1
6.5.1.2	Paneles suelo	1
6.5.1.3	Paneles techo	1
6.5.1.4	Estructura de soportación de paneles de techo	1
6.5.1.5	Estructura metálica auxiliar para instalaciones	1
6.5.1.6	Perfilería y acabados	1
6.5.1.7	Puerta con control de acceso	1
6.5.1.8	Estructura completa 20 m2	1
6.5.1.9	Pasacables	1
6.5.1.10	Falso suelo carga 1250 kg/m2	1

6.5.2 Racks y canalizaciones

6.5.2.1	Bandeja de datos de 200x60x3000 mm con soportes de refuerzo	2
6.5.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	2
6.5.2.3	Rack tipo MDA (Main Distribution Area)	2
6.5.2.4	Rack tipo GC de comunicaciones	6

6.5.3 Potencia, cableado e iluminación

6.5.3.1	Cableado principal de servicios	1
6.5.3.2	Cableado redundante para servicios	1
6.5.3.3	Alumbrado	1
6.5.3.4	Alumbrado de emergencia	1
6.5.3.5	Instalación eléctrica	1
6.5.3.6	Instalación eléctrica redundante	1

6.5.4 Sistema de climatización

6.5.4.1	Unidad de Expansión Directa	1

6.5.5 Protección contra incendios

6.5.5.1	Detector analógico direccionable conectado a la central de detección	1
6.5.5.2	Extinción manual	1

6.5.6 Control, monitorización, gestión y seguridad

6.5.6.1	Control de accesos por lector de tarjeta	1

6.5.7 Cableado de datos

6.5.7.1	Instalación cobre	2
6.5.7.2	Instalación fibra	2
6.5.7.3	Certificación y gestión de garantía cobre	2
6.5.7.4	Certificación y gestión de garantía fibra	2

6.5.7.5	Cableado cobre cat 6a 6 enlaces	1
6.5.7.6	Cableado fibra MM OM3 6 enlaces	1
6.5.7.7	Cableado fibra MM OM3 12 enlaces	1
6.5.7.8	Cableado fibra MM OM3 24 enlaces	1

6.5.8 Instalación y gestión del proyecto

6.5.8.1	Pre Auditoria	1
6.5.8.2	Pruebas de calidad por empresa de commissioning	1
6.5.8.3	Dirección del proyecto	1
6.5.8.4	Documentación as-built y memoria del proyecto	1
6.5.8.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.5.8.6	Contenedores reciclaje de material	1

6.6 Salas IT

6.6.1 Estructura - Sala Cofre RF120 EN1047-2

6.6.1.1	Paneles paredes	1
6.6.1.2	Paneles suelo	1
6.6.1.3	Paneles techo	1
6.6.1.4	Estructura de soportación de paneles de techo	1
6.6.1.5	Estructura metálica auxiliar para instalaciones	1
6.6.1.6	Perfilería y acabados	1
6.6.1.7	Puerta RF120 WK4	1
6.6.1.8	Estructura completa 140 m2 con certificación	1
6.6.1.9	Pasacables	1
6.6.1.10	Falso suelo carga 1250 kg/m2	1

6.6.2 Racks y canalizaciones

6.6.2.1	Bandeja de datos de 200x60x3000 mm con soportes de refuerzo	2
6.6.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	2
6.6.2.3	Rack IT (EDA) 42U 600x1000, 1000 kg	40
6.6.2.4	Rack de Distribución (HDA) 42U 600x1000, 1000 kg	6
6.6.2.5	Blanking pannels para rack 800 mm	46

6.6.3 Potencia, cableado e iluminación

6.6.3.1	Cableado principal de servicios	1
6.6.3.2	Cableado redundante para servicios	1
6.6.3.3	Busbar rack alta densidad con interruptores hot-swap	1
6.6.3.4	Caja de derivación rack alta densidad 32A 3F+N+T IP31 portafus.	80
6.6.3.5	PDU Inteligente trifásica de 32A, c/12 salidas C13, c/12 salidas C19	80
6.6.3.6	Alumbrado	1
6.6.3.7	Alumbrado de emergencia	1
6.6.3.8	Instalación eléctrica	1
6.6.3.9	Instalación eléctrica redundante	1

6.6.4 Sistema de climatización

6.6.4.1	Cerramiento de pasillo frio, con puerta deslizante	3
6.6.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF120	1

6.6.5 Protección contra incendios

6.6.5.1	Central de detección y extinción de incendios convencional con sensores ópticos y alarma centralizada	2
6.6.5.2	Sistema de detección temprana	1
6.6.5.3	Sistema de extinción Novec 1230 con fijaciones metálicas, tuberías, boquillas y manómetro, disparo mecánico manual	2
6.6.5.4	Door Fan Test	2
6.6.5.5	Extinción manual	2

6.6.6 Control, monitorización, gestión y seguridad

6.6.6.1	Sistema de monitorización y control autónomo incluyendo sensores de temperatura y humedad, detección de agua y lectura de alarmas (central de incendios, UPS, clima...). Comunicación vía acceso web, email, SMS y SNMP.	1
6.6.6.2	Instalación sistema de monitorización	1
6.6.6.3	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	2
6.6.6.4	Cámaras CCTV en los accesos, desde el interior (zona segura)	2

6.6.7 Cableado de datos

6.6.7.1	Patch panels de cobre 24 puertos, vacío	1
6.6.7.2	Patch Panels de fibra vacío - espacio para 3 cassettes	1
6.6.7.3	Cassete para 12 fibras / 6 conexiones	1
6.6.7.4	Cassete para 24 fibras / 12 conexiones	1
6.6.7.5	Tapa ciega para panel de fibra, espacio sin cassettes	1
6.6.7.6	Latiguillo cobre 1m	1
6.6.7.7	Latiguillo cobre 2m	1
6.6.7.8	Latiguillo cobre 3m	1
6.6.7.9	Latiguillo cobre 5m	1
6.6.7.10	Trunks de cobre: 6 enlaces por trunk	1
6.6.7.11	Certificación y gestión de garantía cobre	1
6.6.7.12	Certificación y gestión de garantía fibra	1

6.6.8 Instalación y gestión del proyecto

6.6.8.1	Pre Auditoria	1
6.6.8.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.6.8.3	Diseño del proyecto según estándar Tier III (Ingeniería Básica y constructiva)	1
6.6.8.4	Dirección del proyecto	1
6.6.8.5	Documentación as-built y memoria del proyecto	1

6.6.8.6	Preparación documentación para posible certificación Uptime Institute	1
6.6.8.7	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.6.8.8	Contenedores reciclaje de material	1
6.6.8.9	Puesta en marcha y Site Acceptance Test (SAT)	1
6.6.8.10	Integrated System Test (IST), incluyendo alquiler de aerotermos	1

6.7 Sala UPS y Baterías A y B

6.7.1 Estructura

6.7.1.1	Paneles paredes	1
6.7.1.2	Paneles suelo	1
6.7.1.3	Paneles techo	1
6.7.1.4	Estructura de soportación	1
6.7.1.5	Estructura metálica auxiliar para instalaciones	1
6.7.1.6	Perfilería y acabados	1
6.7.1.7	Estructura completa 40+20 m2 con certificación	1
6.7.1.8	Puerta RF120 WK4	2
6.7.1.9	Pasacables RF120 120x120	1
6.7.1.10	Falso suelo carga 1250 kg/m2	1

6.7.2 Canalizaciones

6.7.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.7.2.2	Bandeja de potencia de 300x60x3000 mm con soportes de refuerzo	1

6.7.3 Potencia, cableado e iluminación

6.7.3.1	Cuadro Media Tensión A	1
6.7.3.2	Cuadro media Tensión B	1
6.7.3.3	Cuadro Distribución B.T. A	1
6.7.3.4	Cuadro Distribución B.T. B	1
6.7.3.5	Cuadro UPS IT A	1
6.7.3.6	Cuadro UPS IT B	1
6.7.3.7	Cuadro UPS Servicios A	1
6.7.3.8	Cuadro UPS Servicios B	1
6.7.3.9	Cuadro Servicios No Críticos	1
6.7.3.10	Cuadro UPS Operaciones	1
6.7.3.11	Analizador de Redes (en cada cuadro principal), conectados a BMS	1
6.7.3.12	Interruptor Estático (STS)	1
6.7.3.13	ATS unidades Clima y servicios comunes	1
6.7.3.14	UPS 300 kW, modular, con doble rama de baterías 10 min	2
6.7.3.15	Sistema DC (48v) 20 kW con doble rama de baterías 30 min	2
6.7.3.16	Cuadro DC Servicios A	1
6.7.3.17	Cuadro DC Servicios B	1
6.7.3.18	Sistema de monitorización de baterías	1

6.7.3.19	Cableado principal en el interior de la sala para el sistema de refrigeración, SAIs, Racks, Iluminación, Sistema de extinción, etc. (solo potencia)	1
6.7.3.20	Cableado redundante en el interior de la sala para el sistema de refrigeración, SAIs, Racks, Iluminación, Sistema de extinción, etc. (solo potencia)	1
6.7.3.21	Alumbrado 400 lux/m2	1
6.7.3.22	Alumbrado de emergencia	1
6.7.3.23	Instalación eléctrica	1
6.7.3.24	Instalación eléctrica redundante	1

6.7.4 Sistema de climatización

6.7.4.1	Unidad de clima, incluye sistema free-cooling directo, sistema de refrigeración frigorífico DX, ventiladores EC, filtros G4, Interfaz para monitorización	2
6.7.4.2	Sensores adicionales por sala, de temperatura y humedad	1
6.7.4.3	Compuertas cortafuegos RF120	2
6.7.4.4	Conductos	1

6.7.5 Protección contra incendios

6.7.5.1	Central de extinción de incendios, gobernada por central de detección principal, con sensores ópticos y alarma centralizada	1
6.7.5.2	Sistema de detección temprana	1
6.7.5.3	Sistema de extinción Novec 1230 con fijaciones metálicas, tuberías, boquillas y manómetro, disparo mecánico manual	2
6.7.5.4	Door Fan Test	1
6.7.5.5	Extinción manual	2

6.7.6 Control, monitorización, gestión y seguridad

6.7.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	2
6.7.6.2	Cámaras interiores conectadas al sistema CCTV	2

6.7.7 Instalación y gestión del proyecto

6.7.7.1	Pre Auditoria	1
6.7.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.7.7.3	Diseño del proyecto según estándar Tier III (Ingeniería Básica y constructiva)	1
6.7.7.4	Dirección del proyecto	1
6.7.7.5	Documentación as-built y memoria del proyecto	1
6.7.7.6	Preparación documentación para certificación Uptime Institute	1
6.7.7.7	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.7.7.8	Contenedores reciclaje de material	1

6.8 Almacén

6.8.1 Estructura

6.8.1.1	Paneles paredes	1
6.8.1.2	Paneles suelo	1
6.8.1.3	Paneles techo	1
6.8.1.4	Estructura de soportación	1
6.8.1.5	Perfilería y acabados	1
6.8.1.6	Puerta RF120 WK4	1
6.8.1.7	Pasacables Roxtec RF120 120x120	2
6.8.1.8	Estructura completa 25 m2	1

6.8.2 Canalizaciones

6.8.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.8.2.2	Bandeja de potencia de 60x60x3000 mm con soportes de refuerzo	1

6.8.3 Potencia, cableado e iluminación

6.8.3.1	Cableado servicios	1
6.8.3.2	Cableado de UPS	1
6.8.3.3	Alumbrado 400 lux/m2	1
6.8.3.4	Alumbrado de emergencia	1
6.8.3.5	Instalación eléctrica	1

6.8.4 Sistema de climatización

6.8.4.1	Climatizadora de comfort 3,3 kW	1
6.8.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.8.5 Protección contra incendios

6.8.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.8.5.2	Extinción manual	1

6.8.6 Control, monitorización, gestión y seguridad

6.8.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.8.6.2	Cámaras interiores conectadas al sistema CCTV	1

6.8.7 Instalación y gestión del proyecto

6.8.7.1	Pre Auditoria	1
6.8.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.8.7.3	Dirección del proyecto	1
6.8.7.4	Documentación as-built y memoria del proyecto	1
6.8.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.8.7.6	Contenedores reciclaje de material	1

6.9 Sala NOC

6.9.1 Estructura

6.9.1.1	Paneles paredes	1
6.9.1.2	Paneles suelo	1
6.9.1.3	Paneles techo	1
6.9.1.4	Estructura de soportación	1
6.9.1.5	Perfilería y acabados	1
6.9.1.6	Puerta RF120 WK4	1
6.9.1.7	Pasacables Roxtec RF120 120x120	2
6.9.1.8	Estructura completa 35 m2	1

6.9.2 Canalizaciones

6.9.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.9.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1

6.9.3 Potencia, cableado e iluminación

6.9.3.1	Cableado servicios	1
6.9.3.2	Cableado de UPS	1
6.9.3.3	Alumbrado 500 lux/m2	1
6.9.3.4	Alumbrado de emergencia	1
6.9.3.5	Instalación eléctrica	1

6.9.4 Sistema de climatización

6.9.4.1	Climatizadora de comfort 3,3 kW	1
6.9.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.9.5 Protección contra incendios

6.9.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.9.5.2	Extinción manual	1

6.9.6 Control, monitorización, gestión y seguridad

6.9.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.9.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1
6.9.6.3	PC y monitor asociado, para BMS	1
6.9.6.4	Conjunto de monitores para visualización de sistemas de seguridad (Control de accesos y CCTV).	1
6.9.6.5	Conjunto de monitores para visualización de sistema contra incendios (esquemas y gráficos de ubicación de detectores)	1
6.9.6.6	Consola para visualizar las llamadas de los videoporteros e intercomunicadores	1

6.9.6.7	Puesto de trabajo completo (mesa, silla, ordenador y pantalla de altas prestaciones -funcionamiento continuo-).	6

6.9.7 Instalación y gestión del proyecto

6.9.7.1	Pre Auditoria	1
6.9.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.9.7.3	Dirección del proyecto	1
6.9.7.4	Documentación as-built y memoria del proyecto	1
6.9.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.9.7.6	Contenedores reciclaje de material	1

6.10 Sala CERT-PY

6.10.1 Estructura

6.10.1.1	Paneles paredes	1
6.10.1.2	Paneles suelo	1
6.10.1.3	Paneles techo	1
6.10.1.4	Estructura de soportación	1
6.10.1.5	Perfilería y acabados	1
6.10.1.6	Puerta RF120 WK4	1
6.10.1.7	Pasacables Roxtec RF120 120x120	2
6.10.1.8	Estructura completa 25 m2	1

6.10.2 Canalizaciones

6.10.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.10.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1

6.10.3 Potencia, cableado e iluminación

6.10.3.1	Cableado servicios	1
6.10.3.2	Cableado de UPS	1
6.10.3.3	Alumbrado 500 lux/m2	1
6.10.3.4	Alumbrado de emergencia	1
6.10.3.5	Instalación eléctrica	1

6.10.4 Sistema de climatización

6.10.4.1	Climatizadora de comfort 3,3 kW	1
6.10.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.10.5 Protección contra incendios

6.10.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.10.5.2	Extinción manual	1

6.10.6 Control, monitorización, gestión y seguridad

6.10.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.10.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1
6.10.6.3	Puesto de trabajo completo (mesa, silla, ordenador y pantalla de altas prestaciones -funcionamiento continuo-).	6

6.10.7 Instalación y gestión del proyecto

6.10.7.1	Pre Auditoria	1
6.10.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.10.7.3	Dirección del proyecto	1
6.10.7.4	Documentación as-built y memoria del proyecto	1
6.10.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.10.7.6	Contenedores reciclaje de material	1

6.11 Sala de Crisis

6.11.1 Estructura

6.11.1.1	Paneles paredes	1
6.11.1.2	Paneles suelo	1
6.11.1.3	Paneles techo	1
6.11.1.4	Estructura de soportación	1
6.11.1.5	Perfilería y acabados	1
6.11.1.6	Puerta RF120 WK4	1
6.11.1.7	Pasacables Roxtec RF120 120x120	2
6.11.1.8	Estructura completa 25 m2	1

6.11.2 Canalizaciones

6.11.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.11.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1

6.11.3 Potencia, cableado e iluminación

6.11.3.1	Cableado servicios	1
6.11.3.2	Cableado de UPS	1
6.11.3.3	Alumbrado 500 lux/m2	1
6.11.3.4	Alumbrado de emergencia	1
6.11.3.5	Instalación eléctrica	1

6.11.4 Sistema de climatización

6.11.4.1	Climatizadora de comfort 3,3 kW	1
6.11.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.11.5 Protección contra incendios

6.11.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.11.5.2	Extinción manual	1

6.11.6 Control, monitorización, gestión y seguridad

6.11.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.11.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1
6.11.6.3	Video Wall	1

6.11.7 Instalación y gestión del proyecto

6.11.7.1	Pre Auditoria	1
6.11.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.11.7.3	Dirección del proyecto	1
6.11.7.4	Documentación as-built y memoria del proyecto	1
6.11.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.11.7.6	Contenedores reciclaje de material	1

6.12 Sala de Reuniones

6.12.1 Estructura

6.12.1.1	Paneles paredes	1
6.12.1.2	Paneles suelo	1
6.12.1.3	Paneles techo	1
6.12.1.4	Estructura de soportación	1
6.12.1.5	Perfilería y acabados	1
6.12.1.6	Puerta RF120 WK4	1
6.12.1.7	Pasacables Roxtec RF120 120x120	2
6.12.1.8	Estructura completa 20 m2	1

6.12.2 Canalizaciones

6.12.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.12.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1

6.12.3 Potencia, cableado e iluminación

6.12.3.1	Cableado servicios	1
6.12.3.2	Cableado de UPS	1
6.12.3.3	Alumbrado 500 lux/m2	1
6.12.3.4	Alumbrado de emergencia	1
6.12.3.5	Instalación eléctrica	1

6.12.4 Sistema de climatización

6.12.4.1	Climatizadora de comfort 3,3 kW	1
6.12.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.12.5 Protección contra incendios

6.12.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.12.5.2	Extinción manual	1

6.12.6 Control, monitorización, gestión y seguridad

6.12.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.12.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1

6.12.7 Instalación y gestión del proyecto

6.12.7.1	Pre Auditoria	1
6.12.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.12.7.3	Dirección del proyecto	1
6.12.7.4	Documentación as-built y memoria del proyecto	1
6.12.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.12.7.6	Contenedores reciclaje de material	1

6.13 Sala de Capacitación y de mantenimiento

6.13.1 Estructura

6.13.1.1	Paneles paredes	1
6.13.1.2	Paneles suelo	1
6.13.1.3	Paneles techo	1
6.13.1.4	Estructura de soportación	1
6.13.1.5	Perfilería y acabados	1
6.13.1.6	Puerta RF120 WK4	1
6.13.1.7	Pasacables Roxtec RF120 120x120	2
6.13.1.8	Estructura completa 25 m2	1

6.13.2 Canalizaciones

6.13.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.13.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1

6.13.3 Potencia, cableado e iluminación

6.13.3.1	Cableado servicios	1
6.13.3.2	Cableado de UPS	1
6.13.3.3	Alumbrado 500 lux/m2	1
6.13.3.4	Alumbrado de emergencia	1
6.13.3.5	Instalación eléctrica	1

6.13.4 Sistema de climatización

6.13.4.1	Climatizadora de comfort 3,3 kW	1
6.13.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1

6.13.5 Protección contra incendios

6.13.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.13.5.2	Extinción manual	1

6.13.6 Control, monitorización, gestión y seguridad

6.13.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.13.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1
6.13.6.3	Puesto de trabajo completo (mesa, silla, ordenador y pantalla).	2

6.13.7 Instalación y gestión del proyecto

6.13.7.1	Pre Auditoria	1
6.13.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.13.7.3	Dirección del proyecto	1
6.13.7.4	Documentación as-built y memoria del proyecto	1
6.13.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.13.7.6	Contenedores reciclaje de material	1

6.14 Sala de Guardia y recepción

6.14.1 Estructura

6.14.1.1	Paneles paredes	1
6.14.1.2	Paneles suelo	1
6.14.1.3	Paneles techo	1
6.14.1.4	Estructura de soportación	1
6.14.1.5	Perfilería y acabados	1
6.14.1.6	Puerta RF120 WK4	1
6.14.1.7	Pasacables Roxtec RF120 120x120	2
6.14.1.8	Estructura completa 25 m2	1

6.14.2	***Canalizaciones***	
6.14.2.1	Bandeja de datos de 60x60x3000 mm con soportes de refuerzo	1
6.14.2.2	Bandeja de potencia de 100x60x3000 mm con soportes de refuerzo	1
6.14.3	***Potencia, cableado e iluminación***	
6.14.3.1	Cableado servicios	1
6.14.3.2	Cableado de UPS	1
6.14.3.3	Alumbrado 500 lux/m2	1
6.14.3.4	Alumbrado de emergencia	1
6.14.3.5	Instalación eléctrica	1
6.14.4	***Sistema de climatización***	
6.14.4.1	Climatizadora de comfort 3,3 kW	1
6.14.4.2	Unidad de renovación de aire de sobrepresión, incluyendo control externo, filtros F9, compuerta de sobrepresión y compuerta cortafuegos RF90	1
6.14.5	***Protección contra incendios***	
6.14.5.1	Detectores y sirenas integrados en lazo con el sistema de detección de la central principal	1
6.14.5.2	Extinción manual	1
6.14.6	***Control, monitorización, gestión y seguridad***	
6.14.6.1	Control de accesos, mediante doble chequeo con tarjeta y con teclado (PIN).	1
6.14.6.2	Cámara enfocando el acceso desde el exterior a dicha sala, conectada al sistema CCTV	1
6.14.6.3	PC y monitor asociado, para gestión de operaciones habituales del puesto de seguridad	1
6.14.6.4	PC y monitor asociado, para BMS	1
6.14.6.5	PC y conjunto de dos monitores asociados, para gestión de sistemas de seguridad (Control de accesos y CCTV).	1
6.14.6.6	PC y monitor asociado, para sistema gráfico del sistema contra incendios	1
6.14.6.7	Consola para visualizar las llamadas de los videoporteros e intercomunicadores	1
6.14.7	***Instalación y gestión del proyecto***	
6.14.7.1	Pre Auditoria	1
6.14.7.2	Pruebas de calidad y funcionamiento por empresa de commissioning	1
6.14.7.3	Dirección del proyecto	1
6.14.7.4	Documentación as-built y memoria del proyecto	1
6.14.7.5	Limpieza técnica a la finalización del proyecto según ISO14644	1
6.14.7.6	Contenedores reciclaje de material	1

7 Análisis económico y financiero. Cronograma

En cualquier país que quiera dar un paso firme hacia el cada vez más tecnológico futuro, es preciso además de tener una red extensa fibra óptica, y con buena capilaridad a través de las distintas regiones, así como unas buenas conexiones internacionales, disponer de un centro de datos que sea el punto central para gestionar, dentro del mismo, todos los servicios que se van a desarrollar consiguiendo mantener todas las instituciones en el punto de vanguardia que se requiere.

Este análisis cubre la necesidad de la construcción del Centro de Datos TIER III sito en Asunción, que será donde se alojará todo el equipamiento preciso para la prestación de los servicios actuales y futuros de la SENATICs.

Se ha realizado una estimación de los equipos IT a considerar, pero será preciso evaluar los servicios y estado de los mismos en el momento que este el nuevo Centro de Datos operativo de cara a definir cuáles son las necesidades reales llegado ese instante. No es el hardware el que decide el modelo, sino los servicios que queremos ofrecer, adaptando el hardware a ellos.

A continuación se presenta la inversión inicial (CAPEX) a realizar acorde con el estudio técnico y los gastos operativos (OPEX) para los primeros 5 años[3].

7.1 Inventario de las inversiones a realizar acorde con el estudio técnico

La estimación para los costos de inversión ascendería a **$19.767.205,08**, repartido en cuatro montos principales que comprenderían cada una de las fases de construcción del centro de datos; el apoyo al desarrollo del proyecto con los costos relacionados con la ingeniería de apoyo, la dirección facultativa, commissioning y soporte inicial; y los costos de certificaciones TIER con las estimaciones para la certificación, incluyendo la parte de la consultoría y de las tasas tanto de diseño como de construcción.

[3] Todos los cálculos se han realizado de acuerdo al tipo de cambio a fecha actual

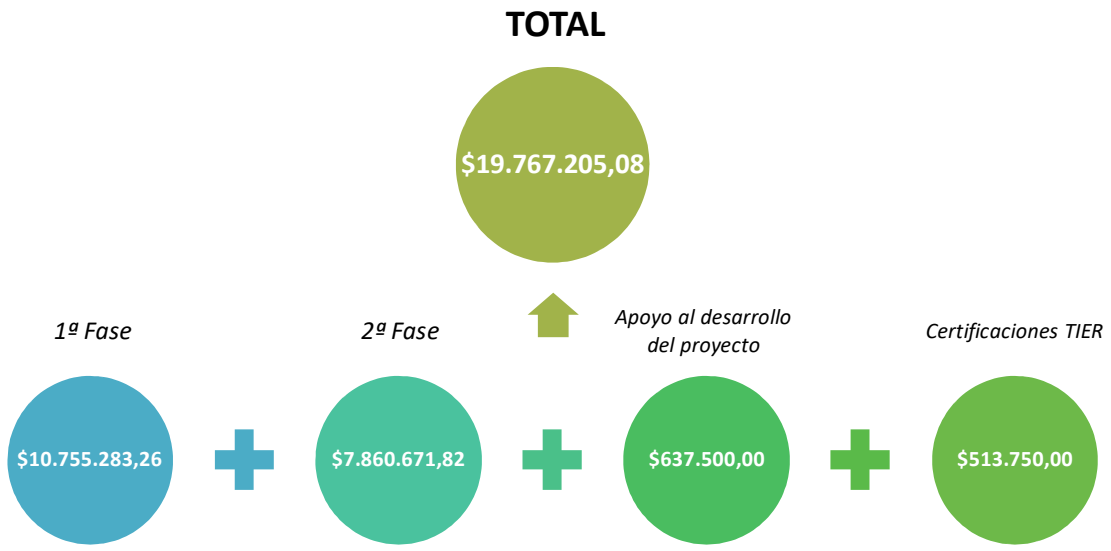
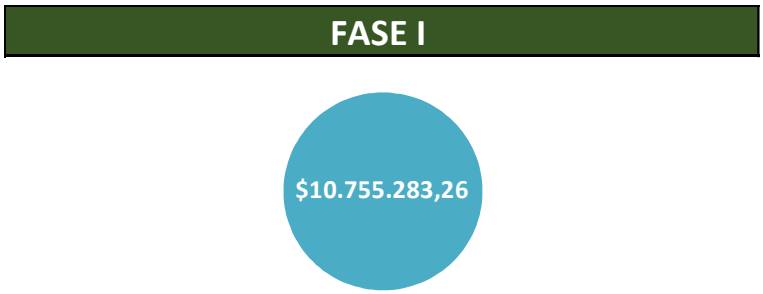


Figura 33 CAPEX total para la implantación del centro de datos en Paraguay

Así, para alcanzar el costo total anteriormente indicado, a continuación se desglosa el costo correspondiente a cada una de estas cuatro partidas principales, explicadas detalladamente en los capítulos anteriores de Propuesta del centro de datos y Partidas del proyecto.

7.1.1 *Desglose Fase I de construcción*

La primera fase, que se consideraría realizar durante los ***doce primeros meses***, requeriría una inversión de **$10.755.283,26** repartidos de la siguiente manera en exteriores, civil, instalaciones y equipamiento:



EXTERIORES	
VALLADO PERIMETRAL	$185.445,94
URBANIZACION + CIMENTACION	$921.091,30
	$1.106.537,24

CIVIL	
ESTRUCTURA	$555.886,59
CERRAMIENTOS EXTERIORES	$453.797,76
DIVISIONES INTERIORES	$90.822,27
TECHOS	$25.507,50
ACABADOS INTERIORES	$98.985,70
CARPINTERIA DE MADERA	$17.688,00
CARPINTERÍA METÁLICA Y CERRAJERÍA	$122.815,19
EQUIPAMIENTO	$40.214,35
CARGA DE MÓDULOS	$32.095,86
GRUA Y MEDIOS AUXILIARES	$79.770,63
TRANSPORTE	$500.439,36
MONTAJE	$70.812,00
SEGURIDAD Y SALUD	$51.081,14
CALIDAD Y MEDIO AMBIENTE	$34.054,24
	$2.173.970,59

INSTALACIONES	
Estim. Acometida desde subestación	$191.834,80
INSTALACIONES OFICINAS	$76.992,30
CENTROS DE APOYO OPERATIVO	$169.334,84
CENTRO DE SECCIONAMIENTO	$76.133,06
CENTROS DE TRANSFORMACION	$452.667,21
INST. ELECTRICIDAD	$1.687.133,25
INST. PROTECCION CONTRA DESCARGAS ATMOSFERICAS	$26.748,18
INS FUEL	$62.517,00
INST. CLIMATIZACION	$510.662,22
INST. INCENDIOS	$123.456,00
INST. FONTANERIA	$8.974,63
INST. SANEAMIENTO	$7.407,00
INST. ESPECIALES (DETECCION DE AGUA)	$20.331,00
INST. BMS	$156.643,35
INST. SEGURIDAD	$185.451,88
CANALIZACION TELECOMUNICACIONES	$38.556,00
	$3.794.842,69

EQUIPAMIENTO	
RACKS	$115.200,00
CERRAMIENTOS PASILLOS FRIOS	$75.024,00
PDU'S INTELIGENTES	$252.000,00
EQUIPAMIENTO PARA CONEXIÓN CON RED F.O.	$326.000,00
	$768.224,00

EQUIPAMIENTO IT	
Seguridad perimetral	$342.000,00
Balanceo	$118.000,00
Switching central	$190.240,00
Switching almacenamiento	$83.800,00
Cabina almacenamiento principal	$240.000,00
Cabina copia respaldo	$140.000,00
Computación	$390.812,00
Conectividad computación	$36.000,00
Cabina principal almacenamiento	$200.000,00
Cabina back-up	$100.000,00
Blades UCS computación	$488.515,00
Contingencia	$582.341,75
	$2.911.708,75

7.1.2 *Desglose Fase II de construcción*

La segunda fase de ***nueve meses*** de duración aproximadamente, se consideraría realizar después de transcurrido un año en funcionamiento tras la fase I de construcción. Esta fase requeriría una inversión de **$7.860.671,82** repartidos de la misma manera que la primera fase en exteriores, civil, instalaciones y equipamiento, pero con algunas partidas desglosadas menos debido a que ya se habrían implementado en el primer año:

FASE II

EXTERIORES	
CIMENTACION	$50.000,00
	$50.000,00

CIVIL	
ESTRUCTURA	$409.001,88
CERRAMIENTOS EXTERIORES	$261.876,66
DIVISIONES INTERIORES	$36.488,88
TECHOS	
ACABADOS INTERIORES	$85.573,23
CARPINTERIA DE MADERA	
CARPINTERÍA METÁLICA Y CERRAJERÍA	$11.739,00
EQUIPAMIENTO	
CARGA DE MÓDULOS	$32.520,54
GRUA Y MEDIOS AUXILIARES	$72.232,50
TRANSPORTE	$415.792,32
MONTAJE	$56.322,00
SEGURIDAD Y SALUD	$41.456,14
CALIDAD Y MEDIO AMBIENTE	$21.679,24
	$1.444.682,39

INSTALACIONES	
INSTALACIONES OFICINAS	
CENTRO DE SECCIONAMIENTO	
CENTROS DE TRANSFORMACION	$55.000,00
INST. ELECTRICIDAD	$1.687.133,25
INS FUEL	$10.520,40
INST. CLIMATIZACION	$510.662,22
INST. INCENDIOS	$118.956,09
INST. FONTANERIA	$3.974,63
INST. SANEAMIENTO	$7.407,00
INST. ESPECIALES (DETECCION DE AGUA)	$11.106,25
INST. BMS	$93.643,35
INST. SEGURIDAD	$18.556,25
CANALIZACION TELECOMUNICACIONES	$8.556,00
	$2.525.515,43

EQUIPAMIENTO	
RACKS	$115.200,00
CERRAMIENTOS PASILLOS FRIOS	$75.024,00
PDU'S INTELIGENTES	$252.000,00
	$442.224,00

EQUIPAMIENTO IT	
Cabina principal almacenamiento	$720.000,00
Cabina back-up	$336.000,00
Blades UCS computación	$1.641.000,00
Switching UCS	$21.600,00
Contingencia	$679.650,00
	$3.398.250,00

7.1.3 *Desglose de Apoyo al desarrollo del proyecto*

El tercer monto principal se refiere al apoyo al desarrollo del proyecto con los costos relacionados con la ingeniería de apoyo, requiriendo una inversión de **$637.500,00** repartidos de la siguiente manera en la dirección de apoyo, dirección facultativa, commissioning y soporte inicial:

APOYO AL DESARROLLO DEL PROYECTO

INGENIERÍA DE APOYO	$187.500,00
DIRECCIÓN FACULTATIVA	$50.000,00
COMMISSIONING	$250.000,00
SOPORTE 1er AÑO EN LA OPERACIÓN Y ELABORACIÓN DE PROCEDIMIENTOS, MANUALES, AJUSTES, ETC.	$150.000,00
	$637.500,00

7.1.4 *Desglose para la Certificación Tier III*

Po último, el cuarto monto principal se refiere a los costos para las certificaciones TIER, requiriendo una inversión de **$513.750,00** repartidos para la certificación de diseño y de construcción y, a su vez, con estimaciones tanto para la parte de la consultoría como para las tasas de obtención de la certificación:

CERTIFICACIÓN TIER III

TIER III DISEÑO	
CONSULTORÍA CERTIFICACIÓN TIER III - DISEÑO	$161.250,00
TASAS CERTIFICACIÓN TIER III - DISEÑO	$75.000,00
	$236.250,00

TIER III CONSTRUCCIÓN	
CONSULTORÍA CERTIFICACIÓN TIER III - CONSTRUCCIÓN	$183.750,00
TASAS CERTIFICACIÓN TIER III - CONSTRUCCIÓN	$93.750,00
	$277.500,00

7.1.5 *Resumen del CAPEX en los primeros 5 años*

A modo de resumen, se expone la inversión prevista para los 5 primeros años durante los cuales se propone desarrollar la implementación de la primera fase de construcción en los primeros doce meses, y trascurrido un año en funcionamiento de la misma, unos nueve meses para la segunda fase:

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
Fase I	$10.755.283,26					**$10.755.283,26**
Fase II			$7.860.671,82			**$7.860.671,82**
Apoyo al desarrollo del proyecto	$487.500,00	$150.000,00				**$637.500,00**
Certificaciones TIER III		$513.750,00				**$513.750,00**
TOTAL CAPEX	**$11.242.783,26**	**$663.750,00**	**$7.860.671,82**	**$0,00**	**$0,00**	**$19.767.205,08**

Figura 34 CAPEX para los 5 primeros años

En el primer año se imputan las partidas de ingeniería de apoyo, dirección facultativa y commissioning dado que forman parte esencial de la construcción de la primera fase del centro de datos, necesitando el soporte al primer año de operación para el segundo año (que corresponderá con el primer año en que se comience con la gestión y funcionamiento del centro de datos).

Las certificaciones TIER III se planifican para su imputación en el segundo año, pues será justo al acabar la primera fase cuando se deba considerar dicho costo.

7.2 Cálculo de los gastos operativos en los primeros 5 años

Para la operación del centro de datos, los costos que se deben tener en cuenta a lo largo del periodo que se ha analizado serían los siguientes:

Considerando la ampliaciónde la Fase II durante el 2-3 año

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
COSTE ENERGIA*	$325.138,00	$325.138,00	$561.086,51	$561.086,51	$561.086,51	**$2.333.535,52**
OPERACIÓN Y MANTENIMIENTO	$430.000,00	$430.000,00	$650.000,00	$650.000,00	$650.000,00	**$2.810.000,00**
SEGURIDAD Y VIGILANCIA	$150.000,00	$150.000,00	$150.000,00	$150.000,00	$150.000,00	**$750.000,00**
AGUA**	$355,53	$355,53	$675,09	$675,09	$675,09	**$2.736,35**
GASOIL***	$3.515,50	$3.515,50	$7.031,00	$7.031,00	$7.031,00	**$28.123,98**
	$909.009,03	**$909.009,03**	**$1.368.792,60**	**$1.368.792,60**	**$1.368.792,60**	**$5.924.395,85**

* SEGÚN TARIFA ANDE (Administración Nacional de Electricidad) - Pliego de Tarifas nº 21
** SEGÚN TARIFAS ESSAP (AUTORIDAD DE AGUA POTABLE Y SANEAMIENTO)
*** SEGÚN TARIFA PETROPAR

Considerando la ampliaciónde la Fase II durante el 2-3 año

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
Costes de interconexión f.o.	$170.566,31	$170.566,31	$170.566,31	$170.566,31	$170.566,31	**$852.831,57**
Costes de mantenimiento equipamiento IT	$336.302,36	$336.302,36	$728.800,24	$728.800,24	$728.800,24	**$2.859.005,43**
Acceso de redes de Fibra Optica	$117.720,00	$26.936,00	$26.936,00	$26.936,00	$26.936,00	**$225.464,00**
	$624.588,67	**$533.804,67**	**$926.302,55**	**$926.302,55**	**$926.302,55**	**$3.937.301,00**

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
TOTAL OPEX	**$1.533.597,70**	**$1.442.813,70**	**$2.295.095,15**	**$2.295.095,15**	**$2.295.095,15**	**$9.861.696,85**

Figura 35 Estimación del OPEX para los 5 primeros años

8 Definición de los principales hitos y metas

A continuación se presentan a modo de recomendación los siguientes aspectos fundamentales a la hora de desarrollar los trabajos de ejecución y construcción del centro de datos. Se trata de indicar cuáles serían los principales hitos y metas a ir cumpliendo según se vaya avanzando en la implementación del mismo.

CONSTRUCCIÓN DEL CENTRO DE DATOS
PRINCIPALES HITOS Y METAS
SELECCIÓN DE EMPRESA PARA LA INGENIERIA DE APOYO
ELABORACIÓN DEL PLAN DE DESARROLLO POR LA INGENIERA DE APOYO
SELECCIÓN DE EMPRESA DE CONTROL QUE REALIZARA LAS PRUEBAS DE PUESTA EN MARCHA Y VALIDACIÓN
CONCURSO PARA LA ADJUDICACIÓN DE LOS TRABAJOS
SOPORTE A LA SELECCIÓN DE EMPRESAS COLABORADORAS Y A LA ADJUDICACIÓN DE LOS TRABAJOS
ADJUDICACION DE LOS TRABAJOS
SOPORTE A LA IMPLEMENTACIÓN
URBANIZACION+ CIMENTACION
COMPRA DE EQUIPAMIENTOS Y SISTEMAS QUE COMPONDRAN LAS INSTALACIONES DE APOYO
CONSTRUCCIÓN DE MODULOS
PRUEBAS EN FÁBRICA
TRANSPORTE A UBICACIÓN FINAL
MONTAJE Y AJUSTES EN UBICACIÓN FINAL
PRUEBAS DE INTEGRACIÓN
PRUEBAS FINALES DE PUESTA EN MARCHA (antes de entrar en producción)
ACEPTACIÓN Y RECEPCIÓN DEL CENTRO DE DATOS
ELABORACIÓN DE PROCEDIMIENTOS
PROGRAMA FORMATIVO PARA EL PERSONAL INVOLUCRADO EN LA OPERACIÓN DEL CENTRO DE DATOS.

9 Conclusiones y recomendaciones

La República del Paraguay tiene un gran reto por delante de cara a proveer a sus instituciones, empresas y ciudadanos, las herramientas tecnológicas que les permitan seguir avanzando, a la vez que les ayuden a ser competitivos en el mundo global en el que estamos.

A la hora de plantear la construcción de los nuevos Centro de Datos previstos por la SENATICs debemos tener muy presente que hoy en día la eficiencia energética y lo que ello conlleva en cuanto al menor impacto ambiental y el aprovechamiento adecuado de los recursos, nos hace considerar que todos los equipamientos sean modulares, para crecer según vayamos necesitándolos.

Se propone la creación del Centro de Datos de forma modular, consiguiendo asegurar una inversión inicial menor y posibilidad de crecimiento futuro sin interrupción del servicio.

Una de las cuestiones fundamentales para garantizar el éxito del proyecto es tener los adecuados compañeros de viaje, para ello sugerimos tratar de manera independiente las siguientes actuaciones/empresas, que implican poner especial cuidado a la hora de elegir **la empresa de ingeniería que apoye el desarrollo del proyecto en las fases iniciales y durante su implementación**, **la empresa instaladora/constructora que lo ejecute** (la cual sugerimos sea una entidad muy especializada en la construcción e implementación de Centro de Datos), y **la empresa que realice todas las pruebas de puesta en marcha antes de comenzar con la operación** del centro de datos. A todas ellas se les debe pedir una dilata experiencia en proyectos similares.

Anexo I – Propuesta de capacitación sobre el Estudio técnico

Como parte de la socialización de este estudio técnico se incluye una capacitación impartida por expertos de Networld Consulting con el fin de transferir nuestro conocimiento técnico para llevar a cabo las implantaciones técnicas y los diferentes aspectos que consideramos sirvan de ayuda a la SENATICs para sacar el máximo rendimiento a este proyecto.

Entre los temas a incluir en esta capacitación estarían:

Propuesta de capacitación	
1	Exposición de los principales resultados de esta componente: *Estudio técnico para el despliegue de un centro de datos en Paraguay.*
2	Propuesta de la solución diseñada: partidas y coste del proyecto.
3	Recomendaciones para la operación del centro de datos.
4	Recomendaciones para la estrategia de gestión del centro de datos.
5	Recomendaciones técnicas.
6	Mejores prácticas internacionales y compartición de experiencias.
7	Recomendaciones para la implantación y mantenimiento de la certificación TIER III.

Figura 36 Propuesta de capacitación

Esta capacitación trata de poner en valor los objetivos principales de los servicios de operación del Centro de Datos:

- Mantener un alto nivel de disponibilidad y confiabilidad de equipos y sistemas.
- Desarrollar métodos específicos para optimizar el funcionamiento y prolongar la vida útil de los equipos y sus componentes.
- Reducir los costos de manutención y de materiales de reposición que actúan sobre los factores que causan el desgaste y la ayuda en la gestión de inventario de piezas de repuesto.
- Supervisar y gestionar los consumibles, tales como combustible, electricidad, filtros, correas, agua, lámparas y lubricantes. Indicación y aplicación de medios para optimizar el uso e indicando el momento propicio para la adquisición de los mismos.
- Producir informes periódicos que contengan información importante para gestión y crecimiento. Además de mantenimiento predictivo.

- Plan de Operación, Manutención y Control, desarrollo de procedimientos operativos y de los programas de manutención detallados.
- El monitoreo regular de la planta a través de rutas con la verificación e inspección de registro de datos que permite la observación de las tendencias.
- Registro completo de todos los eventos y actividades realizadas, la generación de la evidencia y de la historia.
- Análisis y Tratamiento de las fallas a través de métodos avanzados que permitan evitar la repetición de la falla y generar el aprendizaje evitando fallos similares en los sistemas.
- Realizar todas las actividades con un enfoque en la calidad y la seguridad (personal, bienes, procesos y medio ambiente).
- Toma de decisiones, con la información relacionada con las actividades y servicios de Centro de Datos.
- Seguimiento de los servicios prestados por otras empresas, observando y cuidando que se mantengan los niveles de calidad requeridos para el medio ambiente y evitar la ocurrencia de fallas;
- Programa de formación. Plan de formación continua y de renovación.

En la siguiente tabla se propone una agenda tentativa para esta fase de socialización del proyecto del diseño del centro de datos.

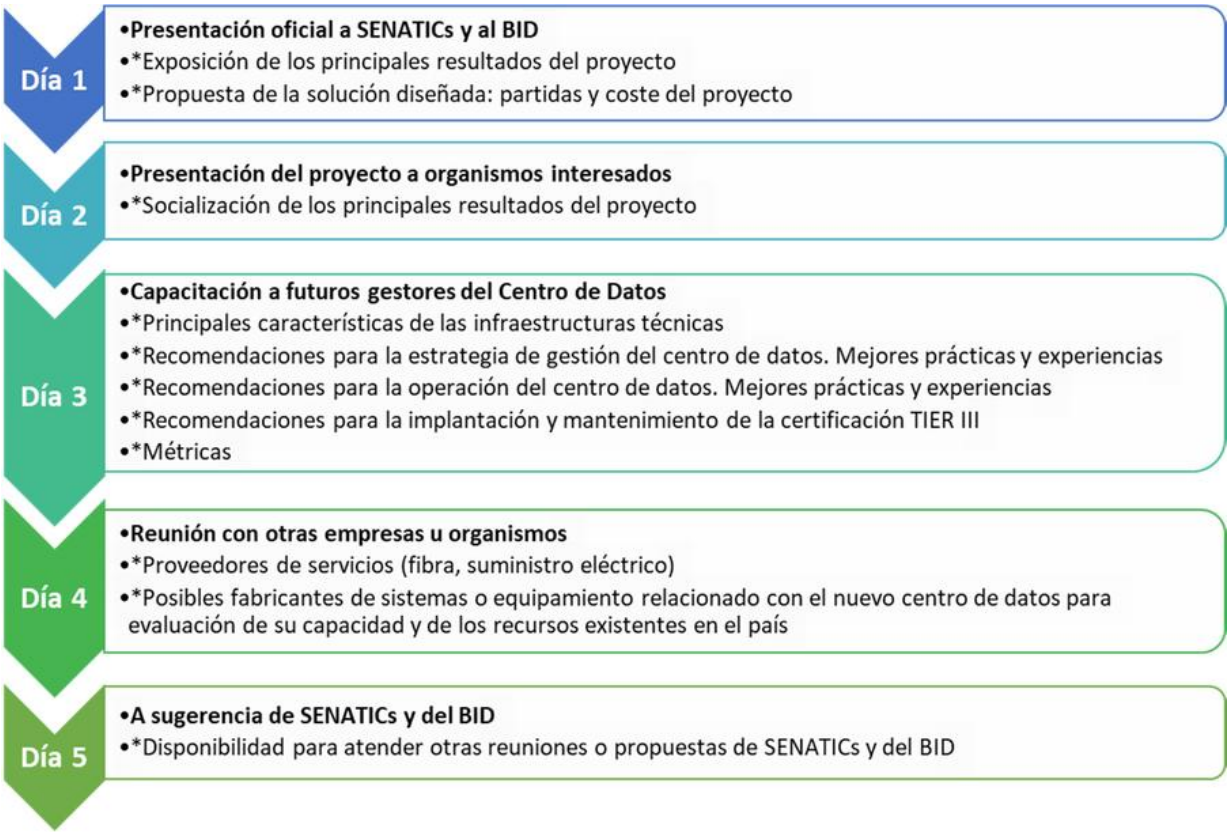


Figura 37 Propuesta de agenda tentativa para la socialización del proyecto

Finalmente, a continuación se presenta parte del contenido de esa capacitación con la intención de mostrar las mejores recomendaciones para la operación y la gestión del centro de datos.

Recomendación para la operación del Centro de Datos

El equipo técnico residente consistiría en 12 personas.

Figura 38 Equipo en el Centro de Datos

El horario de funcionamiento y la composición mínima del equipo técnico residente está definido de la siguiente manera:

1 x Gerente de Operación

Jornada: Comercial

Responsabilidades principales:

Coordinación de las actividades de campo;

Soporte para el personal de campo;

Elaboración del plan de gestión

Interfaz con la Supervisión de la SENATICs

1 x Asistente Administrativo

Jornada: Comercial

Responsabilidades principales:

Coordinación de las actividades de campo;

Soporte para el personal de campo;

4 x Técnicos electricistas

Jornada: 24 horas x 7 días

Responsabilidades:

Seguimiento técnico;

Mantenimiento correctivo - Servicios de Emergencia;

Mantenimiento preventivo - Rutinas periódicas

4 x mecánico de refrigeración

Jornada: 24 horas x 7 días

Responsabilidades:

Seguimiento técnico

Mantenimiento correctivo - Servicios de Emergencia

Mantenimiento preventivo - Rutinas periódicas

1 x Técnico de Telecom / Automatización

Jornada: Comercial

Responsabilidades:

Implantaciones nuevas - circuitos y equipos en el Centro de Datos

Operación y Mantenimiento Preventivo - rutina periódica

Mantenimiento de la infraestructura de cableado (bandejas aéreas, barras, etc.)

Pasada de cable de red para oficinas;

Pasada de cables de red y las fibras ópticas dentro de las áreas críticas (Centro de Datos, Área de Comunicaciones, etc.);

1 x Técnico Servicios Generales

Jornada: Comercial

Responsabilidades:

Servicios generales del Centro de Datos.

Se ha considerado el equipo necesario para gestionar el nuevo centro de datos a nivel operativo en cuanto a las infraestructuras técnicas (principalmente electro mecánica y sistemas asociados a la operativa general para el correcto y seguro funcionamiento del Centro de Datos).

No se contemplan los costes de otros equipos dado que los recursos específicos para gestiones de los servicios IT, para la sala NOC y para CERT-PY, se consideran que ya existen actualmente

y por tanto solo hará falta reubicación, siendo además recursos no asociados directamente a la operación física del nuevo centro de datos.

Recomendación de la estrategia de gestión del Centro de Datos en 5 años

Para poder desarrollar una correcta operación de nuestro centro de datos, una vez que esté en funcionamiento es importante definir, desde la fase de diseño, una serie de documentos, políticas y procedimientos que organicen todo correctamente y nos permitan hacer una gestión eficiente de nuestras instalaciones. Es importante tener muy claro desde el principio cuáles son dichos documentos.

Asimismo, hay que preparar una lista lo más completa posible de algunos documentos técnicos que serán imprescindibles durante la operación para tenerlos en cuenta en la fase de diseño o de construcción:

- Planos de aspectos constructivos, estructuras, servicios (acometidas eléctricas, agua, luz, desagües, bajantes, etc.), patinillos para el paso de los distintos cableados y líneas, etc. Estudiando la posibilidad de disponerlos en BIM
- Sistema de cableado de datos y comunicaciones
- Planos de distribución en planta de los distintos equipamientos
- Planos eléctricos generales y de cada cuadro de distribución con sus correspondientes esquemas unifilares. En un formato editable para poder ir aplicando actualizaciones cuando corresponda (tipo Autocad).
- Toda la información disponible de climatización (distribución de tuberías, etc.).
- Planos y configuraciones de todos los sistemas de Seguridad (protección contra incendios, CCTV y control de accesos).

Podemos empezar diciendo que aunque en muchas ocasiones es algo muy obvio, no por ello debemos considerar que no hay que prestarle una especial atención al **contrato de mantenimiento** para todas las infraestructuras técnicas. Dicho documento es vital y por tanto el tiempo que se dedique a definir bien el alcance que queremos cubrir con el mismo será altamente apreciado durante la explotación del centro de datos. Este documento debe reflejar claramente las tareas y mantenimientos básicos y/o regulatorios, así como el alcance que se acuerde necesitar con los principales fabricantes de los distintos sistemas principales (SAIs, grupo electrógeno, rectificadores, interruptores estáticos, sistemas de climatización, BMS, sistema de protección contra incendios, CCTV, control de accesos, etc). Dependiendo del tamaño que vaya alcanzando el centro de datos y de los propios recursos para su gestión, podemos evaluar si merece la pena tener un único contrato con la empresa principal y que ella cierre los acuerdos con los principales fabricantes de los sistemas y equipos más

representativos, o si, por el contrario, lo separamos y contratamos directamente con los fabricantes.

Al definir el plan de mantenimiento que queremos desarrollar, algo que debe estar basado en la necesidades y criticidades de los servicios que vamos a soportar, vamos a tener que definir los recursos económicos y técnicos para cubrirlo.

Desde el primer momento que empecemos la operación debemos tener establecido un **Procedimiento de escalado de alarmas.** Es imprescindible especificar cómo y dónde se recibirán las alarmas que se origen desde los distintos sistemas (normalmente recibidas por un sistema BMS). Dependiendo de la solución que se acuerde implementar se deberán definir las prioridades de todas y cada una de las alarmas que vayamos a recibir, además de los protocolos de actuación y escalado a aplicar en cada caso. Lógicamente en los acuerdos de mantenimiento con cualquiera de las empresas mantenedoras o fabricantes (si hacemos el contrato con ellos de manera directa) se deben establecer los SLAs y tiempos de respuesta para personarse en la instalación en caso de necesitar una intervención de urgencia/emergencia.

Los vigilantes de seguridad deben ser parte de la gestión de la operación del centro de datos, dado que son una parte vital para identificar posibles incidencias durante las **rondas de supervisión por las instalaciones**, así como para notificar/escalar las alarmas que se vayan recibiendo en el sistema de monitorización a tal efecto (BMS), principalmente en horarios donde pueda no existir personal de operaciones o técnicos de mantenimiento en la instalación. Para todo ello es importante definir un procedimiento desde el primer día donde se definan todas **las tareas e instrucciones que los vigilantes deben realizar en su operativa** (gestión de accesos, control de llaves, notificación de incidencias, escalados de alarmas, etc.).

Para tener todo bien preparado y asegurar el cumplimiento de medidas concretas ante determinadas actuaciones es preciso tener definidos algunos **Permisos Especiales** (permiso de Trabajos en Caliente, permiso para trabajos en Alta Tensión,…). En ellos debe quedar perfectamente recogido quien solicita la actuación, la fecha de la misma, la hora de inicio, etc. y debe quedar expresamente recogido que se debe notificar la finalización de los trabajos y del permiso justo cuando se acaben.

Dichos permisos deberán ser solicitados con al menos 48h de antelación al responsable de infraestructuras del centro de datos y sin su aprobación no se podrán implementar los trabajos.

Uno de los documentos que confiamos no se tenga que usar casi nunca pero que hay que tener muy bien definido, por si llegase el caso saber perfectamente cómo actuar, es el **Procedimiento de Evacuación** de todo el personal que esté en el centro de datos en caso de producirse dicha necesidad. Es muy importante que todas las visitas y empresas colaboradoras conozcan cómo actuar en caso de necesitar evacuar la instalación. Una buena práctica es entregar la información básica sobre cómo actuar ante una situación de emergencia a todas las visitas, así como realizar formaciones regulares a todos los implicados en la operación diaria. Es muy recomendable realizar al menos un simulacro de evacuación, por sorpresa, al año. Habrá que medir los tiempos que se tarda en llevar a todo el personal al punto de encuentro que se defina a tal efecto y que debe estar establecido en el procedimiento.

Siguiendo con las cuestiones que afectan al **mantenimiento** debemos documentar los **procedimientos** implicados en dichas cuestiones. Podríamos aglutinarlos en dos grandes grupos:

- Escribiremos procedimientos paso a paso, bien documentados, orientados a la tarea, con casillas de verificación (Procedimientos operativos estándar, SOP) y alineados con la definición del método de trabajo a desarrollar y el análisis de los riesgos asociados (tanto para el servicio que presta el equipo, sistema, proceso, tarea, etc., como para la persona o técnicos que tengan que implementarlo). Debe aplicarse a todos los proveedores y a todo el personal, sin importar su experiencia.
- Los que cubrirán planes de respaldo y que deben estar disponibles para situaciones imprevistas (Procedimientos operativos de emergencia, EOP).

Hay que definir y preparar con el mayor detalle posible todos estos procedimientos que van a ser tan necesarios ante determinadas situaciones que pueden surgir:

SOP (Standard Operation Procedure)
Procedimientos Operativos Estándar
SOP - Prueba con carga real al generador
SOP - Arranque manual del generador
SOP - Prueba con banco de carga al generador
SOP - Como poner la UPS en Bypass
SOP - Como apagar la UPS
SOP - Como reiniciar la UPS
SOP - Reemplazo de un rectificador en el sistema de continua
SOP - Anulación del sistema de Extinción de Incendios
SOP - Prueba de alarmas del sistema de Protección contra Incendios
SOP - Acoplamiento de Barras entre Cuadros Generales
SOP - Como poner el STS en Bypass
SOP - Recarga de combustible (Tanque principal y en el que tenga el propio grupo)
SOP - Aislamiento/Desconexión del transformador y celdas de alta tensión
SOP - Arranque de unidades de climatización

EOP (Emergency Operation Procedure)
Procedimientos Operativos de Emergencia
EOP - Arranque y puesta en operación de la instalación desde una parada total
EOP - Como actuar ante un fallo de arranque del generador
EOP - Reseteo total al sistema de automatización (PLC)

SOP (Standard Operation Procedure)
EOP - Operación manual de las instalaciones ante un fallo en el control o automatización de la misma (PLC)
EOP - Operación manual o arranque forzado de las enfriadoras
EOP - Bypass mecánico de las enfriadoras
EOP - Llenado rápido del sistema de climatización (agua)
EOP - Operación manual de bombas (sistema de climatización)
EOP - Aislamiento/Desconexión de bombas (sistema de climatización)
EOP - Conexión de grupo electrógeno móvil
EOP - Evacuación del edificio
EOP - Brigada de bomberos en la instalación

Si el planteamiento es tener una red de centro de datos, es muy importante generar documentos que estandaricen todas las instalaciones, de manera que cuanto más similares sean unas a otras más facilidades surgirán en la operación y más sinergias se podrán conseguir entre los distintos centros.

Lógicamente todos esos procedimientos deben estar alineados con la operativa diaria de los sistemas y deben mantenerse en una actualización permanente. Hay que mantener actualizados todos los procedimientos operativos y obtener, si hay cambios reseñables, la conformidad de todos los implicados. Ante los cambios que se puedan ir produciendo por mejoras o actuaciones que impliquen modificaciones, hay que volver a validar dichas variaciones en los procedimientos con todos los que tienen relación con los mismos. Debemos poner especial atención para que con el paso del tiempo los operarios y operadores del centro de datos no se salten pasos o busquen atajos debido a que se sientan familiarizados con la instalación. Hay que evitar que por rutina diaria se produzcan caminos abreviados en la forma de actuar. Para ello es muy recomendable disponer de procedimientos claros y bien documentados, facilitando a los usuarios de los mismos su cumplimiento y aplicación. En centro de datos con cierto grado de madurez se tienen implantadas **metodologías ITIL** (Biblioteca de Infraestructura de Tecnologías de Información), que implica desarrollar las actuaciones mediantes **Trabajos Planificados** que deben ser aprobados por los departamentos y áreas implicadas, y pueden requerir el rellenar documentos (tipo Check List) que garanticen que se hacen las comprobaciones definidas en el procedimiento durante su implementación.

Debemos dedicar el tiempo necesario a realizar **análisis de riesgos** para las operaciones especiales, con el fin de analizar las posibles situaciones que se puedan presentar así como mitigar posibles factores de error humano. Asegurémonos de que todas las operaciones especiales de mantenimiento forman parte de la gestión de cambio de TI y de los procedimientos de revisión paralelos.

Se deben establecer procedimientos paso a paso para las tareas complejas, marcando o pegando etiquetas temporales numeradas con las acciones que deben realizarse para ajustarse a los pasos de cada tarea en todos los interruptores, disyuntores, protecciones y válvulas.

Para que todo se pueda identificar correctamente hay que disponer de un **Etiquetado preciso.** Esta tarea tan importante, sobre todo según van pasando los años y posiblemente haya habido rotaciones de personas, la podemos basar en un procedimiento específico para ello. Hay por tanto que definir desde el principio un modelo de identificación para cualquier elemento y aplicarlo rigurosamente en todos los puntos precisos:

- Disyuntores y protecciones principales de los distintos paneles de control, interruptores y disyuntores de cada PDU, regletas de corriente, etc.
- El número de disyuntores, interruptores y protecciones debe mantenerse correctamente identificados, y en una línea única, en los diagramas unifilares y en los archivos de control que se vayan generando.
- Etiquetar todos los circuitos que se vayan instalando para suministrar la potencia a los racks/gabinetes con el objetivo de asegurarse que las regletas en los racks se ajustan a los disyuntores/interruptores de las PDU.

Dentro del plan de mantenimiento debemos establecer revisiones rutinarias que nos permitan garantizar que todos esos etiquetados corresponden con los esquemas.

Tenemos que asegurarnos que todos los **diagramas unifilares y esquemáticos** de los distintos sistemas (principalmente en lo referente a la distribución eléctrica y de climatización) están actualizados, son legibles y están expuestos en las paredes de las distintas salas técnicas de planta, en los paneles de control y los PDU/paneles de distribución. Las referencias que puedan aparecer en dichos diagramas deben corresponder meticulosamente con las etiquetas que tengamos colocadas.

Una buena política de mantenimiento incluye realizar comprobaciones físicas diarias de la planta en su conjunto, y aunque no debemos dudar de ellos tampoco podemos confiar únicamente en los sistemas de monitorización remota (BMS o similares), dado que como equipos que son también pueden fallar. En este sentido las personas con la adecuada formación suelen ser buenas detectando problemas.

Por tanto hay que revisar que los PMP (Procedimientos de mantenimiento planificado) están completos y se ajustan a las recomendaciones del fabricante o a una autoridad superior (normalmente por obligatoriedad de la legislación que corresponda).

Una buena práctica que debemos dejar recogida en los procedimientos de mantenimiento pero que por su importancia hay que explicar a todos los que trabajan y operan el centro de datos es el identificar (si finalmente se instalase alguno) todos los **botones del Apagado de emergencia (EPO)** y en la medida de las posibilidades dejarlos protegidos. Ocurre que como en algunas instalaciones los EPO suelen ubicarse en las salidas pueden activarse erróneamente durante una emergencia, como si fueran los interruptores de la luz o un pulsador para liberar la apertura de la puerta.

Una vez tengamos todos los documentos, políticas y procedimientos establecidos debemos tener presente la importancia de la **recopilación mensual de KPIs y capacidades** de nuestros sistemas. Nuevamente, en función del tamaño del centro de datos puede realizarse de una manera manual por los operarios o podríamos implementar una herramienta/software que nos permita obtener muchos de ellos de manera automática. Lógicamente esta segunda opción tiene un costo y por ello debemos ser conscientes de si realmente lo necesitamos.

Métricas

Está muy claro que es importante obtener datos y medir continuamente para tener información real que nos permita tomar las mejores decisiones para nuestro negocio. De manera que si nos preguntarnos ¿qué esperamos de las métricas?, debemos perseguir que sean:

- Sencillas.
- Objetivas. Intentando evitar supuestos o interpretaciones particulares.
- Incorporen todos los elementos del negocio.
- Puedan utilizarse para realizar comparaciones con otros y comprender cuáles son más eficientes.
- Comprender la eficiencia de cada parte.
- Establecer objetivos para mejorar las distintas partes.

A través de unas métricas adecuadas conseguiremos definir acciones a implementar y además focalizar el esfuerzo en el lugar óptimo para nuestro negocio, lo cual traerá consigo hábitos y comportamientos de trabajo más adecuados.

Métricas de espacio	Métricas de alimentación
• Diseño de los racks.	• Diseño de la alimentación.
• Racks consumidos / ocupados.	• Potencia consumida.
• Racks que pueden utilizarse ahora.	• Potencia asignada no consumida.
• Racks reservados.	• Potencia que puede utilizarse ahora.
• Racks posibles.	• Potencia reservada.
• Racks incrementales sobre lo diseñado.	• Potencia posible.
	• Potencia incremental sobre lo diseñado.

Si entramos a evaluar algunas de las métricas específicas para los Centros de datos, debemos decir que desde hace ya unos años la métrica más ampliamente adoptada para las instalaciones es la **PUE**. Con ella vamos a evaluar la efectividad del consumo energético (Creado por The Green Grid en 2007). Mientras que la PUE es un ratio la DCiE es un porcentaje.

PUE = Energía total de la instalación / Energía del equipamiento de TI.

DCiE = 1/PUE = Energía del equipamiento de TI / Energía total de la instalación x 100%.

Anexo II – Detalle Equipamiento IT

En este anexo se presenta un detalle de la partida sobre equipamiento IT que compondrá la primera y segunda fase de la etapa de construcción de la solución propuesta.

Diseño técnico y modelado de la infraestructura global de computación en la nube o cloud

En el diseño y modelado de una infraestructura de computación en la nube o cloud (en su acepción en inglés) existen diversas arquitecturas de diseño válidas, con distintos pros y contras, en las que, en función de los servicios a desplegar, la integración de dichos servicios en los usuarios y plataformas de comunicaciones e IT vinculadas, así como la necesidad de realizar un diseño que permita el crecimiento de la plataforma ligada al aumento de la demanda de servicios, da como resultado la arquitectura de virtualización más adecuada a las necesidades precisas.

Por ello, se deben tener presentes los principales puntos:

- **Capacidad de adaptación de la computación en la nube** a los servicios de IT precisos, tanto para el usuario final como para entornos empresariales y gubernativos en Paraguay.
- **Flexibilidad** en el crecimiento del servicio facilitado por la arquitectura de computación en la nube para satisfacer de manera dinámica la demanda de servicios, escalable y de baja complejidad.
- **Sencilla integración** en plataformas públicas de virtualización, que permita la posible creación de nube híbrida, pública y privada.
- **Entorno seguro** que permita la explotación de los servicios garantizando la integridad, disponibilidad y confidencialidad de los datos.

La base de una plataforma de computación en la nube es la infraestructura física, la conectividad de dicha infraestructura con los demandantes de servicios y el software que sustentan los servicios, tomando como herramienta básica el entorno de virtualización.

La decisión de la adopción de un entorno de virtualización impacta en el diseño técnico y los componentes que se emplearán en la creación de la arquitectura como servicio.

Una infraestructura virtual permite compartir recursos físicos de computación y almacenamiento entre distintas máquinas, empleando una infraestructura física común. Esta labor es realizada por el hipervisor de virtualización.

La capa correspondiente al hipervisor de virtualización es software y se ubica entre el hardware físico y el sistema operativo de los entornos IT virtualizados, siendo responsabilidad del hipervisor garantizar el rendimiento de los entornos IT en producción, maximizando el

empleo del hardware físico entre los distintos sistemas en todo momento, consiguiendo de este modo rentabilizar desde el punto de servicio la infraestructura en producción en el Centro de datos.

Desde Networld Consulting sí consideramos que se debe optar por arquitecturas certificadas por los distintos fabricantes como válidas, y que se haya comprobado en elevado número de plataformas su total compatibilidad y rendimiento, tanto entre los componentes del hardware como con el hipervisor.

Para la construcción física de la computación en la nube, los fabricantes deben ser totalmente compatibles con la arquitectura anterior y tener disponibilidad de distribuidores autorizados en el propio Paraguay o país cercano, lo cual permita disponer del correcto soporte técnico del fabricante tanto las averías e incidencias, como para las ampliaciones e instalaciones de las mismas.

Plataforma de centro de datos unificados. Computación

En el diseño se ha contado con una plataforma de centro de datos unificados que combine el estándar de la industria de IT empleando servidores con arquitectura x86 usando servidores tipo Blade, servidores de rack, redes y gestión de alto rendimiento en un único sistema y a nivel de comunicaciones con un entorno de seguridad con una pareja de Firewalls que permiten tener los servicios básicos de filtrado basado en regla, al igual que los sistemas más avanzados basados en técnicas de identificación y prevención de ataques.

La configuración de la infraestructura IT es totalmente personalizable, en este caso se ha considerado un entorno totalmente redundado con una capacidad de computo que se hace desde los servidores UCS. Esta infraestructura estará interconectada con dos capas de switching; una de consolidación de todas las comunicaciones del Centro de Datos en los equipos de Core y otra específica dentro de cada armario que intercomunica los servidores dentro del mismo y el switch de Core. Todos los equipos estarán diseñados para soportar grandes anchos de banda. En los siguientes puntos se explica con mayor detalle cada uno de los equipos. El ecosistema hardware se interconecta velando por el rendimiento, seguridad y facilidad de administración. Los componentes de este hardware serían:

Switching core

Diseñado para satisfacer los retos de la nueva generación de centros de datos, incluidos los multisockets densos, los multinúcleos y los servicios optimizados de máquinas virtuales, en los que la expansión de la infraestructura y las cargas de trabajo cada vez más exigentes son habituales.

El conmutador debe brindar una estructura unificada sobre 10 Gigabit Ethernet para tráfico de clústeres, LAN y SAN. Esta unificación permite la consolidación y utilización de infraestructuras y cables separados previamente, lo cual reduce la cantidad de adaptadores y cables necesarios y elimina los conmutadores redundantes. Este conmutador simplificará la administración de

cables, lo cual permite que los hosts se conecten a cualquier red a través de una interfaz Ethernet unificada.

- 10 Gigabit Ethernet de alto rendimiento y baja latencia.
- Estructura unificada opcional con Fibre Channel over Ethernet (FCoE) para la consolidación de E/S.
- Servicios optimizados de máquinas virtuales para un mayor uso de los activos.

Switching UCS

Con un único punto para la conectividad y gestión dentro del armario. Dada la criticidad de este equipamiento, la recomendación de Networld Consulting es implementarlos en activo-pasivo. El equipo debería gestionar todas las operaciones de E/S de forma eficiente y segura en un solo punto, velando por la latencia de E/S independientemente de cada servidor virtual.

En el diseño estimado para la presente computación en la nube se considera la incorporación de 4 equipos, que soportan en el espacio de 1 U de rack, 48 puertos capaces de soportar hasta 80 Gigabit Ethernet, Fiber Channel sobre Ethernet o conectividad Fiber Channel nativa.

Blades UCS computación

Los servidores blade tradicionales replican todos los componentes del rack dentro de cada chasis, evitando el aumento de los costos. Los equipos considerados unifican la gestión de datos y los datos con el chasis blade o rack de servidores, concentrando hasta tres capas de red en una sola. De este modo, todo el sistema se convierte en un chasis blade virtual distribuido, separando la complejidad de la capacidad, permitiendo aumentar la capacidad en función del crecimiento, uno de los requerimientos de la plataforma de computación en la nube considerada para Paraguay.

En la arquitectura propuesta, se considera añadir un equipo que consigue duplicar el ancho de banda del chasis blade hasta 160 Gbps, utilizando además una tarjeta que llega a cuadruplicar el ancho de banda hasta el servidor mediante interfaces 40Gb duales, soportando 256 interfaces virtuales.

También se considera un equipo que ofrezca una solución escalable y flexible basado en un chasis de blade o “cuchilla”. El chasis utilizado en la solución propuesta tiene un tamaño de 6 unidades de rack (6RU) de altura y se pueden montar en un rack estándar como el resto de equipamiento propuesto en el diseño de Networld Consulting.

Con cuatro alimentaciones monofásicas, y fuentes de alimentación intercambiables en caliente, la alta disponibilidad de potencia dentro del chasis estaría garantizada. La parte trasera del chasis utilizado contiene ocho ventiladores intercambiables en caliente, cuatro conectores de alimentación (uno por cada fuente de alimentación), y dos compartimientos de E/S. Con respecto a la capacidad de procesamiento del backplane, algo básico para no tener cuellos de botella en la arquitectura, proporciona hasta 40 Gbps de ancho de banda de E/S por cada blade server y hasta 80 Gbps de ancho de banda de E/S. El chasis sería capaz de soportar futuros estándares Ethernet 80 Gigabit.

Además, se han considerado chasis compuestos de Blades que serían los responsables de facilitar a las máquinas virtuales que orquestarían el hipervisor utilizado de los recursos de computación, vCPU y vRAM.

Cada uno de los servidores propuestos tendrá 2CPUs Intel y 32GB RAM, con capacidad de dos unidades de estado sólido (SSD) o unidades de disco duro (HDD) y hasta 80 Gbps de conectividad. En total 24 ranuras para módulos de memoria DIMM (RDIMM) o DIMM DIMM (LR) para hasta 768 GB de capacidad de memoria total. Siendo compatibles con conectores de red que soportan Ethernet y FCoE (Fibre Channel over Ethernet).

Estos servidores proporcionarían la flexibilidad de crecimiento que sea preciso para el servicio, siendo posible ir alimentando los chasis con los blades de que sean precisos o, si el crecimiento de la demanda lo solicita, escalar en modelos hasta los más potentes.

Almacenamiento

Una infraestructura en Nube tiene como origen y fin el almacenamiento de datos, ya sea por el dato en sí mismo, o bien porque mediante los datos almacenados se crean los entornos virtuales que dan servicio a los usuarios gubernativos o finales.

El almacenamiento de los datos debe cumplir con las mismas directrices de diseño que tiene una arquitectura Nube:

- Disponibilidad.
- Reducción de costos.
- Alta disponibilidad.
- Rendimiento adaptado al servicio.
- Cumplimiento normativo.
- Confidencialidad.
- Integridad.
- Etc.

Existen una gran variedad de arquitecturas de almacenamiento, tanto respecto a fabricantes, como a tecnologías y hardware implicado.

En Networld Consulting hemos propuesta una arquitectura basada en hardware y software que cumple con los siguientes requerimientos:

- Totalmente integrado y verificado con el resto de los componentes de la arquitectura.
- Se parte de una arquitectura inicial que permite el crecimiento gradual en función del crecimiento de la demanda.
- La arquitectura hardware se adapta a los servicios de los demandantes, y no al revés. Esto implica en el caso del almacenamiento, que será posible modelizar distintos tipos de almacenamiento, con características de rendimiento de disco, velocidad de acceso,

velocidad de entrada y salida de datos, para de este modo, crear paquetes de servicio fácilmente entendibles y asignables a entornos de producción, en función de las necesidades, bien de rendimiento o de costo. Por ejemplo, se podrá realizar asignación de almacenamiento de bajo rendimiento y gran capacidad para la asignación de servicios gubernativos a bajo precio.

- La arquitectura está verificada y comprobada su rendimiento y estabilidad, cumpliendo con estándares de servicio que certifican la estabilidad de la misma.

La arquitectura de almacenamiento propuesta tiene como centro del servicio unas cabinas de almacenamiento que permiten garantizar la disponibilidad de almacenamiento de datos ante el esperable crecimiento de la demanda en los próximos años.

Los elementos hardware y software de la arquitectura de almacenamiento son los siguientes:

Cabina principal almacenamiento

Sistema de almacenamiento que cumplen con los requisitos que deben cumplir un servicio como el necesario para la nube de Paraguay:

- Simplicidad. Las soluciones de almacenamiento híbrido son el nuevo estándar de sistemas dedicados de almacenamiento, debido a su rapidez de instalación y puesta en marcha, flexibilidad y capacidad de crecimiento.
- Adaptación a las novedades del servicio.

Las cabinas de almacenamiento de datos utilizadas para la propuesta permiten el almacenamiento de datos tanto en modo SAN como NAS. Disponen de almacenamiento híbrido, tanto de tipo flash para el almacenamiento de datos de datos de rápido acceso y disponibilidad, como de discos SAS de 2.5“o 3.5”.

Permiten almacenar desde 1.2 Terabytes (1200 Gigabytes) hasta 4.0 Petabytes (4.000.000 Gigabytes). Sirva como ejemplo de lo que supone esta capacidad de almacenamiento, que se estima que en 1.5 Petabytes se almacenan 10 billones de fotos de Facebook. Utilizan una arquitectura basada en procesadores Intel E5-2600 con soporte nativo NAS, iSCSI y protocolos FibreChannel. Es importante destacar su capacidad de duplicación en relación 1:2, que implica duplicar la capacidad de almacenamiento real.

El almacenamiento propuesto tendrá capacidad de asignar hasta 5 TB por máquina virtual en las diferentes fases.

Cabina de back-up

Es imprescindible que los datos almacenados cuenten con un respaldo de los mismos, empleando para ello un elemento hardware adicional y externo, en el que se guardarán las copias de respaldo de manera automatizada, siguiendo la política de retención que se decida para cada servicio, así como la periodicidad de la ejecución de dicho servicio de copia de

respaldo. Se han considerado cabinas específicas de copias de respaldo consistentes en un sistema de almacenamiento de duplicación en línea.

Desde Networld Consulting consideramos interesante la opción de este diseño por su capacidad de deduplicación de longitud variable, que toma un enfoque más inteligente para la deduplicación, variando el tamaño de los segmentos cuando se busca puntos de datos comunes. Cuando los datos llegan a la cabina, el controlador de la cabina analiza estos datos y los rompe en pedazos o segmentos. Cada pieza o segmento tendrá un hash o identificador que será reconocido como único. Dividiendo los datos en trozos, el hash o identificador puede ser identificado y referenciado como datos almacenados previamente mediante una tabla hash. Los datos entrantes se identifican y se deduplican inline, dejando sólo los datos únicos para ser escrito en el disco, que reduce el espacio ocupado por los datos en una relación 1 a 10, esto es, con una cabina de 100 Terabytes, se haría copia de respaldo equivalente a 1 Petabyte. Con cada sistema propuesto se tiene la capacidad de hacer copia de seguridad de hasta 90 PB utilizando las técnicas de deduplicación.

Se ha tenido en cuenta que la cabina de almacenamiento esté en consonancia con la cabina principal, para este servicio, y con el objetivo de poder estimar una infraestructura inicial.

Para el servicio de copias de respaldo es recomendable añadir un software que sea capaz de aplicar las políticas de copia y retención precisas, y que garantice la correcta restauración de los datos, independientemente si provienen de un servidor, una base de datos o de un aplicativo. El licenciamiento de estos softwares va alineado al volumen de datos salvados, por lo que suponen un incremento de costos flexible y no es preciso hacer una alta inversión al comienzo del servicio.

Switching de almacenamiento

El acceso desde la plataforma de computación a la plataforma de almacenamiento es crítico. Por ello, la solución recomendada sería contar con switches específicos que faciliten la conectividad entre el switching de la computación en la nube y al acceso a datos. Se han tenido en cuenta unos switches diseñados específicamente para el acceso a almacenamiento SAN mediante Fiber-channel, con velocidad de transferencia de 16Gb/s, optimizado para entornos cloud, consiguiendo tanto la compatibilidad entre plataformas como alta disponibilidad.

Balanceo global, ruptura SSL y balanceo interno

El servicio de balanceo en un entorno cloud es, junto a la seguridad perimetral, la puerta de entrada a los servicios facilitados por la computación en la nube.

Contar con un servicio de balanceo, basado en hardware dedicado, incorporado en la plataforma de virtualización, permite tres factores clave:

Balanceo entre Centros de datos

Cuando se afronta un diseño de la envergadura del propuesto para este Data Center en Paraguay, es preciso contar como opcionales con los servicios que podrán ser demandados en un futuro, según el crecimiento de la demanda y evolución del entorno en la adopción de la cloud.

Dentro de estos servicios, la continuidad de negocio está ligada a los servicios críticos, especialmente importantes, por ejemplo, en el Gobierno Electrónico, dado que existe un amplio número de plataformas digitales que no podrán verse afectadas en su producción por incidencias graves que afecten al centro de datos donde se encuentre operativo.

Por ello, es el hardware de balanceo para entornos virtuales aporta la funcionalidad de GSLB (Global Server Load Balancing), que permite realizar arquitecturas activo-pasivo en lo que se refiere al centro de datos, o incluso activo-activo, repartiendo las cargas de computación según sea más interesante para el servicio.

Balanceo de servicios externos

Independientemente del servicio que facilite la cloud a las empresas o los ciudadanos, (correo electrónico, publicaciones Web, acceso herramientas Gobierno Electrónico, servicio de almacenamiento de datos, etc), la arquitectura habitualmente será la misma.

Existirá una serie de máquinas virtuales que harán la funcionalidad de recoger las peticiones de los usuarios remotos y hacer de nexo conductor con los servicios finales (bases de datos, buzones de correo, servidores de producción, etc).

Es en este punto donde es primordial el papel de los balanceadores, para poder repartir las peticiones de servicio, procedentes desde el exterior de la cloud, hacia los servidores frontales, empleando para ello una serie de protocolos de balanceo, que deberá ir desde Round-robin, a asignación con servidor de menor latencia, asignación por cookies persistentes, etc.

Los balanceadores realizan una labor adicional, que consiste en verificar de manera activa la disponibilidad de todos los elementos que componen un servicio en concreto, evitando que se realice la asignación de tráfico a ese destino en el caso de detectar previamente la existencia de alguna incidencia que afecte a la productividad y tiempos de entrega.

Balanceo de servicios internos

Contar con un hardware dedicado de balanceo permite crear entornos virtuales de balanceo, tanto para los servicios publicados como para los servicios internos de la propia nube que son necesarios para el correcto funcionamiento de los mismos.

Ruptura de túnel SSL

Al disponer de un hardware capaz de balancear cargas de servicios, es posible redireccionar el tráfico interno en función de los parámetros que el rendimiento precisen, garantizando de nuevo la asignación de tráfico a componentes correctamente operativos.

Los servicios publicados en Internet tienden a ser encriptados mediante SSL extremo a extremo, y más en el caso de Gobierno Electrónico.

El poder contar con una herramienta hardware de altas prestaciones que sea capaz de romper el túnel SSL permite dos objetivos primordiales:

- Liberar a la computación de las máquinas virtuales del consumo de recursos relativos al mantenimiento del túnel SSL.
- Aplicar políticas de seguridad al tráfico proveniente de los usuarios antes de entregarlo a la plataforma final.

Adicionalmente a estos servicios, y en función del fabricante del hardware elegido para la plataforma, es posible contar con servicios de valor añadido. Para la solución propuesta se ha tenido en cuenta una opción con alto rendimiento en capacidad de balanceo de caudales a la vez que el servicio de balancero de centro de datos y entornos virtuales incorpore un importante número de funcionalidades de seguridad como son servicio DDoS, servicio WAF, single sing-on, multitenant y aceleración de datos, todos ellos activados por defecto sin necesidad de incorporar licenciamiento adicional. Estos equipos serían capaces de gestionar un caudal de 30 Gbps, contando con un chip dedicado y diseñado específicamente para la ruptura de tráfico SSL. De nuevo, la recomendación de Networld Consulting es contar con 4 unidades en activo-pasivo por cada Centro de datos, pudiendo dar de este modo servicio de continuidad de negocio.

Seguridad en Nube Privada. Firewall perimetral y control navegación

Cuando hablamos de una plataforma de Computación en la nube privada, la seguridad del servicio debe ser analizada y observada desde el principio, dado que contar un diseño robusto y que contemple la seguridad como directiva adicional a tener en cuenta, permitirá cumplir tanto con las expectativas de los usuarios como la normativa internacional.

En este sentido, debemos tener presente cual es el uso mayoritario que tendrá la cloud para de este modo centrar el diseño de seguridad en los servicios mayoritarios en explotación.

Atendiendo al estudio de Cloud Security Alliance de 2015, se tiene:

Figura 39 Servicios demandados en entorno Nube 2015 Global.

Fuente: Cloud Security Alliance

Tomando esta información, pondremos foco en los tres primeros servicios, por ser lo que superan el 25% de demanda:

Correo electrónico

El alojamiento de servicios de correo electrónico, tanto para terceros como para el funcionamiento del Gobierno Electrónico, es un servicio clave en entornos cloud. Nos proporciona los valores clásicos de entornos cloud, como son la convergencia de servicio, costo contenido y predecible, disponibilidad, añadiendo servir de puerta de entrada y salida controlada de la comunicación vía correo electrónico, algo esencial desde el punto de vista de la seguridad IT.

Las mayores brechas de seguridad tienen como origen o puerta de acceso el correo electrónico, por lo que un servicio de seguridad de correo en la propia plataforma de Computación en la nube permitirá añadir servicio a las empresas u organismos que tengan intención de migrar o adoptar la nube privada, redundando un aumento de la demanda.

La incorporación de elementos hardware que securicen el correo alojado en el Computación en la nube puede y debe hacerse de manera ajustada al crecimiento de la demanda, debiéndose contemplar no sólo los clásicos servicios de antivirus y antispam, sino añadir las funcionalidades de análisis de URLs embebidas, análisis de adjuntos para aplicación de políticas de prevención de pérdida de datos (DLP), que cobra especial importancia en entornos gubernativos.

Almacenamiento y servicios Web

El acceso a datos ubicados en la plataforma cloud, ya sea para su lectura o almacenamiento, o la consulta a servicios Web, claves en el Gobierno Electrónico, deben ser controlados y seguros.

Es en este punto donde se debe introducir el concepto de firewall clásico, pero con una serie de mejoras. Los firewalls tradicionales eran firewalls de capa 4, esto quiere decir, entendían de puertos origen y destino y de direccionamiento IP, pero no de las aplicaciones que estaban siendo protegidas o denegadas.

Con la incorporación de los firewalls con tecnología Next-Generation, el firewall escala hasta la capa 7 de los niveles OSI, pudiendo aplicar políticas de seguridad por aplicación, y de este modo, las políticas de seguridad se alinean con los servicios demandados y alojados en la plataforma de cloud.

La plataforma de firewalls que dan la seguridad perimetral debe ser multitenant, esto es, debe ser capaz de crear entornos virtuales completamente aislados, y capaces de tener segmentados por entornos el número de sesiones concurrentes.

La incorporación de estos equipos a la plataforma permite garantizar la seguridad perimetral de los servicios a publicar, así como dar servicios de valor añadido, propios de firewalls de última generación, como son servicios de IPS en línea, antivirus y el destacable control de la navegación.

En la propuesta de Networld Consulting, atendiendo a todas estos puntos, se ha optado por una solución de 4 unidades con cortafuegos de rendimiento de 10 Gbps, 4Gbps de rendimiento de VPN IPSec, con 120.000 nuevas sesiones por segundo hasta 2 millones de nuevas sesiones y sistemas virtuales de 25/125 (base/máx.^{2}). Llegaría a admitir 12 puertos de 10/100/1000 Gb, 8 puertos SFP y 4 puertos SFP+ de 10 Gb. Además de 2 puertos de 10/100/1000 Gb de alta disponibilidad, 1 puerto de gestión fuera de banda de 10/100/1000 Gb y 1 puerto de consola RJ-45.

Control de la navegación por Internet

Como es bien sabido, la conectividad en la cloud es primordial para la adopción del servicio, por lo que contar con un back-bone de red capaz de dar la capilaridad necesaria, así como con una conectividad de nodo en la ubicación del Centro de datos donde se aloja es necesario para la explotación de todas las bondades de la propia cloud.

Es debido a estas necesidades de conectividad que, desde Networld Computing, consideramos que existirá conectividad mediante red privada WAN entre, por ejemplo los organismos gubernativos y los servicios del centro de datos. En esa circunstancia, es posible la explotación de un nuevo servicio aprovechando la infraestructura de seguridad de la Nube Privada.

Al estar ubicados los equipos de seguridad en un Centro de datos con una potente salida a Internet, nos encontramos en un entorno óptimo para poder encaminar la navegación a Internet de los usuarios, aplicando políticas de filtrado de navegación, antivirus, control de protección de datos e visibilidad y trazabilidad de la navegación.

Nos encontramos ante un nuevo servicio de valor añadido colateral que maximiza los servicios minimizando los costos.

Normativa y certificación de seguridad en la nube

Una de las principales razones por la que la computación en la nube pública no es recomendable para entornos gubernativos o con información sensible, es la relacionada con la seguridad del dato almacenado.

Es preciso tener presente la alta exigencia de garantías de seguridad precisas, destacándose en particular las garantías sobre confidencialidad, disponibilidad y privacidad.

La Continuidad de Negocio debe ser muy valorada en entornos de computación en la nube, dado que permite garantizar la operatividad de los servicios alojados.

Está contrastado mediante informes, como el realizado por la Cloud Security Alliance (CSA) en 2015, que las situaciones sobre los incidentes de seguridad en la nube mejoran desde su adopción, tanto en volumen (se tienen menos incidentes o los mismos), como en criticidad (los incidentes que ocurren son de menor importancia).

El disponer de un entorno de computación permite controlar con la legislación local el control del dato, pero es recomendable cumplir con una serie de estándares internacionales que deben ser valorados como buenas prácticas, que garanticen la correcta gestión de la información desde el punto de vista de la seguridad.

Atendiendo a la plataforma y la gestión del Centro de Datos, debe tenerse como referencia:

- *ISO 27001:2013.* Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).
- *ISO 20000-1:2011***.** Promueve la adopción de un enfoque de procesos integrados para una provisión de servicios gestionados, que satisfaga los requisitos solicitados y de los usuarios a través de la mejora continua mediante el modelo PDCA indicado anteriormente. Con la implantación de la Norma UNE-ISO/IEC 20000-1 se logra que los servicios TI estén orientados al objetivo básico y fundamental del área de explotación/ producción, dando un servicio con la máxima calidad bien a la propia organización, o bien a sus clientes externos.

Como referencias adicionales, deben valorarse los siguientes referentes:

- *CCN STIC 823***.** Guía de seguridad de las TIC, utilización de servicios en la nube.
- *ISO 27002:2013.* Código de controles para la seguridad de la información.

Seguridad en la Cloud. Enfoque tecnológico 360º

En la seguridad de la información en general, y en las plataformas Nube en particular, el enfoque clásico de la seguridad de zona perimetral y zona segura se está diluyendo, dado que los servicios Nube están difuminando la existencia de un perímetro claro sobre el cual cimentar la arquitectura estática de la seguridad IT.

Cuando la infraestructura de una organización abarca las instalaciones físicas, como el Nube privado y público, simplemente garantizar una visión precisa de los riesgos de seguridad es un esfuerzo considerable.

Dado que la información es el principal activo del servicio propuesta, la seguridad de dicha información, más allá de su ubicación, medio o forma, es el principal objetivo de la arquitectura de seguridad, tomando como válidos los clásicos conceptos para su articulación: *Disponibilidad, integridad y confidencialidad.*

Disponibilidad

El servicio debe estar en todo momento y ante cualquier circunstancia disponible, sin disrupción del mismo bajo ninguna premisa.

Los principales riesgos de seguridad relacionados con la disponibilidad tienen dos vectores de ataque externos, los ataques de denegación distribuida de servicio (DDoS) y los ataques dirigidos a los aplicativos Web y la explotación de las vulnerabilidades de las plataformas o del código, para lo cual se emplean servicios de Web Application Firewall, (WAF).

La naturaleza del servicio, en la que deberemos proteger a la plataforma de Computación en la nube de ataques del exterior hacen recomendable incorporar un elemento dedicado para la protección de ataques de denegación en línea.

De igual modo, la incorporación de un elemento WAF permitirá evitar que un atacante pueda extraer información de la plataforma Nube empleando un fallo o vulnerabilidad de los accesos Web de entornos publicados, o evitar la modificando de la información en dichos entornos, siendo especialmente crítico cuando nos referimos a Gobierno Electrónico y datos de la población.

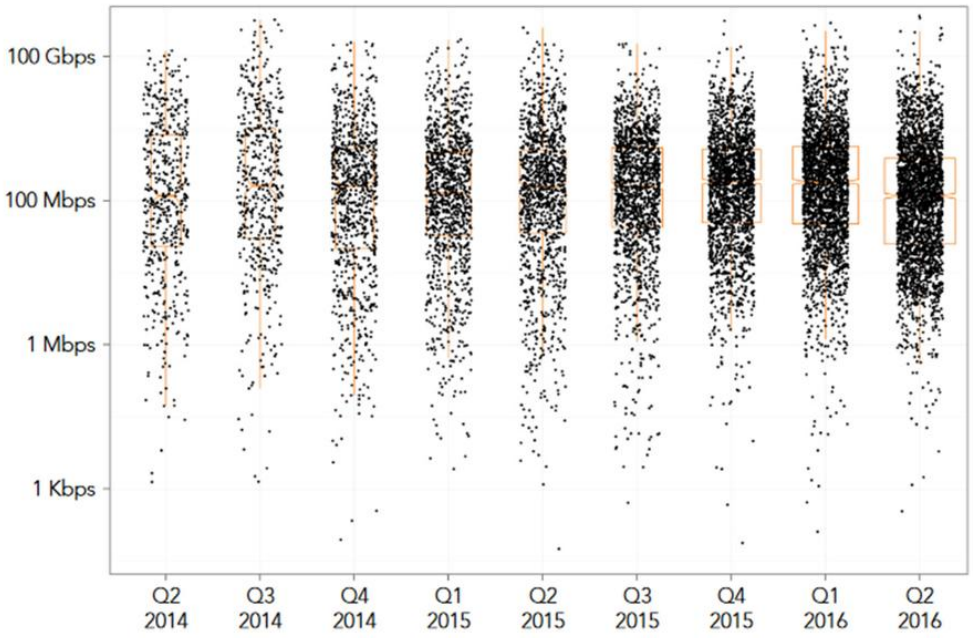


Figura 40 Tamaño y frecuencia de ataques DDoS a nivel mundial en función del tiempo.

Fuente: Akamai

Los servicios anti-DDoS y WAF están enfocados a los accesos y peticiones de tráfico desde Internet, siendo los direccionamientos públicos los vinculados a dichos servicios.

En el caso de la protección de ataques DDoS, dado que este tipo de ataques están estrechamente vinculados a consumir los caudales de acceso a Internet y recursos asociados (sesiones abiertas, tiempo de latencia, etc), este servicio de protección de Internet de publicación de contenidos está habitualmente ofrecido por el proveedor de acceso a Internet, dado que es quien puede poner los medios técnicos oportunos en las zonas de intercambio de Internet con otros proveedores de Internet, (Peering) para la protección de los caudales de acceso a los Centros de datos.

Integridad

La integridad de la información es básica en cualquier entorno empresarial o productivo, pero más si cabe en un servicio como el que ofrecerá la plataforma de Computación en la nube para el Gobierno Electrónico del país, en el que la información y garantizar que dicha información no es modificada sin autorización es primordial.

Para conseguir este objetivo Networld Consulting propone dos enfoques dentro de los servicios de Centro de datos, independientemente de su ubicación física:

- Sistema de sandboxing basado en bastionado previo y análisis del comportamiento, incluyendo servicio de parcheo virtual de aplicativos.
- Servicio de protección de almacenamiento NAS.

Confidencialidad

Es preciso poder garantizar que el acceso a la información impida la divulgación de la misma de manera no controlado o autorizada.

La seguridad de la información no sólo debe contemplarse desde su ubicación acotada en el Centro de datos, sino que debe tenerse control de ella en todo momento, para poder tanto analizar como filtrar, así como disponer de un seguimiento y ubicación en todo momento de la misma.

Con esta premisa, se recomienda incorporar servicios en modalidad cloud para la gestión de los permisos de acceso a la información (IRM), que permiten el control del acceso a los archivos independientemente de su ubicación. Dichos servicios IRM son el complemento perfecto para las soluciones de prevención de la pérdida de información (DLP), consiguiendo de este modo tanto garantizar la no modificación de la información existente, como la no extracción de dicha información ni envío ni modificación.

Como tercera componente básica de la confidencialidad se contempla las soluciones de agentes de seguridad de acceso de nube (CASBs), cuyo objetivo son los puntos de aplicación de políticas de seguridad de acceso a la nube. Los servicios de CASBs consolidan en una única solución las políticas de acceso a los datos, siendo el complemento perfecto a los servicios IRM y DLP.

Figura 41 Enfoque Nube Access Security Broker.

Fuente: Gartner

Detalle del CAPEX del Equipamiento IT

A partir de la especificación técnica realizada, se expone a continuación la estimación del CAPEX para cada funcionalidad descrita, incluyendo el número de unidades de cada una de ellas para cada fase de la etapa de construcción de la solución propuesta.

FASE I			
Funcionalidad	**Precio medio unitario en dólares**	**Unidades**	**Precio total en dólares**
ARQUITECTURA COMÚN BASE			
Seguridad perimetral: Firewall perimetral y control navegación	$85.500,00	4	$342.000,00
Balanceo global, ruptura SSL y balanceo interno	$29.500,00	4	$118.000,00
Switching Core	$31.920,00	4	$127.680,00
Switching UCS	$15.640,00	4	$62.560,00
Switching almacenamiento	$20.950,00	4	$83.800,00
COMPUTACIÓN Y ALMACENAMIENTO PARA 500 SERVIDORES VIRTUALES			
Cabina principal almacenamiento	$120.000,00	2	$240.000,00
Cabina copia respaldo: Cabina back-up	$70.000,00	2	$140.000,00
Computación: Blades UCS computación 6x32 RAM	$97.703,00	4	$390.812,00
Conectividad computación: Switching UCS	$9.000,00	4	$36.000,00
COMPUTACIÓN Y ALMACENAMIENTO PARA 1000 SERVIDORES VIRTUALES			
Cabina principal almacenamiento	$100.000,00	2	$200.000,00
Cabina back-up	$50.000,00	2	$100.000,00
Blades UCS computación 6x32 RAM	$97.703,00	5	$488.515,00

FASE II			
COMPUTACIÓN Y ALMACENAMIENTO PARA PODER LLEGAR A 5000 SERVIDORES VIRTUALES			
Cabina principal almacenamiento	$360.000,00	2	$720.000,00
Cabina back-up	$168.000,00	2	$336.000,00
Blades UCS computación 6x32 RAM	$58.607,00	28	$1.641.000,00
Switching UCS	$5.400,00	4	$21.600,00

Figura 42 Detalle del CAPEX del Equipamiento IT

En la partida de Equipamiento IT se ha incluido además el concepto de contingencia de un 25% sobre este CAPEX, de acuerdo con las mejores prácticas internacionales para este tipo de casos y con el fin de contemplar un monto adecuado que optimice la solución final en el momento de la implantación. Esta acción supone un $582.341,75 para la primera fase y $679.650,00 para la segunda fase, alcanzando la partida del Equipamiento IT para la Fase I un total de $2.911.708,75 y un total de $3.398.250,00 para la Fase II, tal y como se indica en el capítulo de *Inventario de las inversiones a realizar acorde con el estudio técnico*.

Anexo III – Detalle Costos operativos

En este anexo se presenta un detalle de los gastos operativos que se estiman para la operación del centro de datos. El ejercicio se ha realizado para los cinco primeros años. La experiencia y el correcto análisis durante este periodo de operación permitirán obtener la previsión más realista para los siguientes años.

Suministros

Las principales partidas a tener en cuenta relacionadas con los suministros serían la electricidad, el agua y el gasoil.

Coste Energía

El costo de energía o electricidad se contempla a partir de las tarifas de la Administración Nacional de Electricidad de Paraguay (ANDE) en su pliego de tarifas Nº21. Las características serían una potencia reservada mínima de 2.000 kW, una potencia reservada máxima de 6.000 kW y una tensión de abastecimiento de 23.000 V.

	ANDE (Administración Nacional de Electricidad) - Pliego de Tarifas nº 21						
	CARGO FIJO por POTENCIA			CARGO POR ENERGIA			Coste Anual
	Potencia Reservada (kW)	$/kW-mes	Total/mes	kWh /año	$/kWh	Total	Total
FASE 1	2000	$3,72	$7.432,46	4.716.923	0,05	$235.948,51	$325.138,00
FASE 2	2000	$3,72	$7.432,46	9.433.846	0,05	$471.897,03	$561.086,51

Figura 43 Detalle OPEX - Costo energía

Agua

A partir de las tarifas oficiales del Ente Regulador de Servicios Sanitarios (ERSSAN), se estiman el cargo básico y el cargo por consumo para cada año.

	Cargo Básico	m3	> 40 m3	$/mes	Total mes	Total año
FASE 1	$3,49	53	$0,49 /m³	$26,14	$29,63	$355,53
FASE 2	$3,49	107	$0,49 /m³	$52,77	$56,26	$675,09

Figura 44 Detalle OPEX - Costo agua

Gasoil

A partir de las tarifas oficiales de la compañía de Petróleos Paraguayos (Petropar), se estima el costo para cada año en el que incurriría el consumo de combustible en el centro de datos.

	$/litro	litros/mes	Total mes	Total año
FASE 1	$0,98	300	$292,96 /mes	$3.515,50
FASE 2	$0,98	600	$585,92 /mes	$7.031,00

Figura 45 Detalle OPEX - Costo gasoil

Operación y mantenimiento

Las principales partidas a tener en cuenta relacionadas con la operación y mantenimiento serían de personal y de mantenimiento electro-mecánico y de control.

Personal

Para ambas fases se ha estimado la necesidad de contar con el siguiente equipo para gestionar operativamente el centro de datos:

Figura 46 Equipo en el Centro de Datos

Es decir:

- 1 x Gerente de operación o Jefe de departamento
- 1 x Asistente administrativo
- 4 x Técnicos eléctricos
- 4 x Técnicos mecánicos de refrigeración
- 1 x Técnico de telecomunicaciones o automatización
- 1 x Técnico servicios generales o de mantenimiento general.

A partir de los salarios base publicados por la propia SENATICs para sus profesionales, se ha estimado el salario medio de cada perfil operativo ascendiendo esta partida a $156.352,85 cada año.

Mantenimiento electro-mecánico y de control

Se ha estimado que se necesitarán realizar una serie de acciones para la operación y mantenimiento del centro de datos relacionadas con distintos equipos. En función de cada

fase y de la envergadura de las revisiones se ha estimado el costo asociado. Los puntos a tener en cuenta serían:

- Transformadores.- 1 revisión al año por empresa acreditada.
- Grupos electrógenos.- 1 revisión al año por parte del fabricante o su representante oficial en el país.
- SAIs y sus baterías asociadas.- 2 revisiones al año por parte del fabricante o su representante oficial en el país.
- Rectificadores y sus baterías asociadas .- 2 revisiones al año por parte del fabricante o su representante oficial en el país.
- Climatización.- 1 revisión al año por parte del fabricante o su representante oficial en el país.
- BMS (protocolo abierto).- 1 revisión al año por parte del fabricante o su representante oficial en el país.
- Plan de limpieza de las instalaciones.
- Presupuesto para mejoras y correctivos.

De este modo, para la fase I este monto ascendería a $273.647,15 y para la fase II a $493.647,15.

Seguridad y vigilancia

Esta partida se compondría de dos conceptos: vigilantes de seguridad y mantenimiento de los sistemas de seguridad. A partir de salarios medios en Paraguay y de estimaciones para las revisiones anuales se han imputado $150.000,00 anuales para este punto.

Vigilante de seguridad

El servicio requeriría de dos vigilantes que cubrieran 24h los 7 días de la semana.

Mantenimiento de sistemas de seguridad

Se ha estimado que se necesitarán realizar una serie de acciones para el mantenimiento del sistema de seguridad. Los puntos a tener en cuenta serían:

- CCTV.- 2 revisiones al año por empresa acreditada.
- Control de accesos.- 2 revisiones al año por empresa acreditada.
- PCI (Protección Contra Incendios).- 4 revisiones al año por empresa acreditada (anual, semestral y trimestral).

Costes de mantenimiento equipamiento IT

De acuerdo con las mejores prácticas internacionales y a partir de un ejercicio de cálculo del OPEX real en centros de datos ya operativos, se ha considerado un porcentaje en torno al 10%-12% del CAPEX acumulado anualmente para destinar a la previsión del mantenimiento del propio equipamiento IT.

Costes relacionados con la fibra óptica

Se han considerado dos partidas relacionadas con la conectividad del centro de datos: costes de interconexión y acceso de redes.

A partir de las características de acceso de fibra óptica en la ubicación del centro de datos y de las tarifas proporcionadas de la Compañía Paraguaya de Comunicaciones (COPACO), se estima la necesidad de dos accesos dedicados a la mayor velocidad ofrecida hasta el momento.

	Accesos	Total año	Total año
Internet DEDICADO de 55Mbps	2	$85.283,16	$170.566,31

Figura 47 Detalle OPEX – Costos de interconexión de fibra óptica

De acuerdo a las mejores prácticas, se ha incluido una partida para tener en cuenta los posibles gastos operativos sobre el acceso de las redes de fibra óptica referentes al mantenimiento de la conexión entre el centro de datos y las redes troncales de fibra óptica. Se han estimado $ 117.720,00 para el inicio de la actividad y $ 26.936,00 de remanente anual.

Detalle del OPEX estimado

A continuación se presenta a modo de resumen las distintas partidas estimadas para el mantenimiento y operación del propio centro de datos. Como se ha indicado, la experiencia y el correcto análisis una vez puesto en operación permitirán obtener la previsión más realista para los siguientes años.

Considerando la ampliaciónde la Fase II durante el 2-3 año

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
COSTE ENERGIA*	$325.138,00	$325.138,00	$561.086,51	$561.086,51	$561.086,51	**$2.333.535,52**
OPERACIÓN Y MANTENIMIENTO	$430.000,00	$430.000,00	$650.000,00	$650.000,00	$650.000,00	**$2.810.000,00**
SEGURIDAD Y VIGILANCIA	$150.000,00	$150.000,00	$150.000,00	$150.000,00	$150.000,00	**$750.000,00**
AGUA**	$355,53	$355,53	$675,09	$675,09	$675,09	**$2.736,35**
GASOIL***	$3.515,50	$3.515,50	$7.031,00	$7.031,00	$7.031,00	**$28.123,98**
	$909.009,03	**$909.009,03**	**$1.368.792,60**	**$1.368.792,60**	**$1.368.792,60**	**$5.924.395,85**

* SEGÚN TARIFA ANDE (Administración Nacional de Electricidad) - Pliego de Tarifas nº 21
** SEGÚN TARIFAS ESSAP (AUTORIDAD DE AGUA POTABLE Y SANEAMIENTO)
*** SEGÚN TARIFA PETROPAR

Considerando la ampliaciónde la Fase II durante el 2-3 año

Centro de Datos	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	TOTAL
Costes de interconexión f.o.	$170.566,31	$170.566,31	$170.566,31	$170.566,31	$170.566,31	**$852.831,57**
Costes de mantenimiento equipamiento IT	$336.302,36	$336.302,36	$728.800,24	$728.800,24	$728.800,24	**$2.859.005,43**
Acceso de redes de Fibra Optica	$117.720,00	$26.936,00	$26.936,00	$26.936,00	$26.936,00	**$225.464,00**
	$624.588,67	**$533.804,67**	**$926.302,55**	**$926.302,55**	**$926.302,55**	**$3.937.301,00**

Figura 48 Estimación del OPEX para los 5 primeros años

Anexo IV - Recomendación de los estándares para la compatibilidad con la normativa ecológica y legal

En este anexo se presentan referencias a tener en cuenta a la hora implementar un centro de datos, como son:

- Referencia de normativas técnicas.
- Estándares en un centro de datos.
- Métricas de eficiencia del centro de datos.

TABLA DE REFERENCIA DE NORMATIVAS TECNICAS	
REFERENCIA	**NOMBRE NORMATIVA TECNICA**
ASHRAE TC 9.9	*Guía medioambiental para Equipamiento del Centro de Datos*
ASHRAE 90.4-2016	*Energy Standard for Data Centers*
IEEE	*Estándares del Institute of Electrical and Electronic Engineers Inc*
NFPA	Códigos y Estándares NFPA para Prevención y Supresión contraincendios
TIA-942	Estándares de Infraestructura de Telecomunicaciones para Data Centers
Uptime Institute	Estándares para topología de Uptime Institute
ISO 8528	Reciprocating Internal Combustion Engine Driven Alternating Current Generating Sets – Ratings and Performance
USGBC	Guía de Referencia para Diseño y Construcción de edificios

Figura 49 Referencia de normativas técnicas para un centro de datos

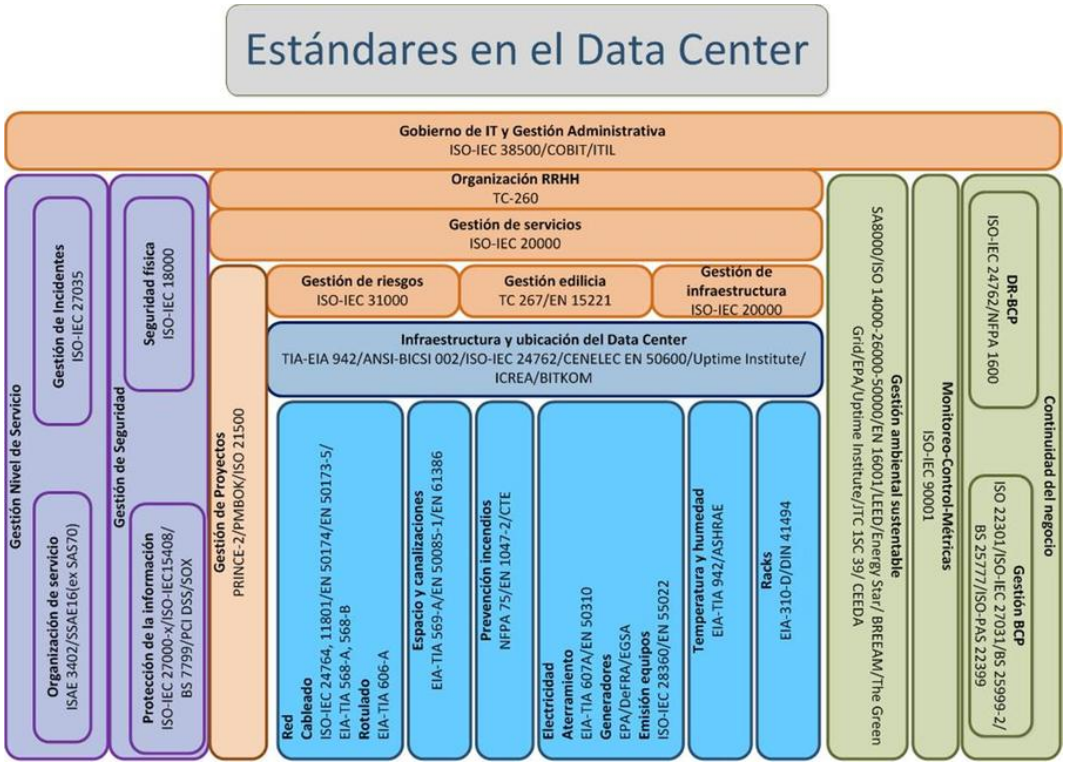


Figura 50 Referencia de estándares en un centro de datos

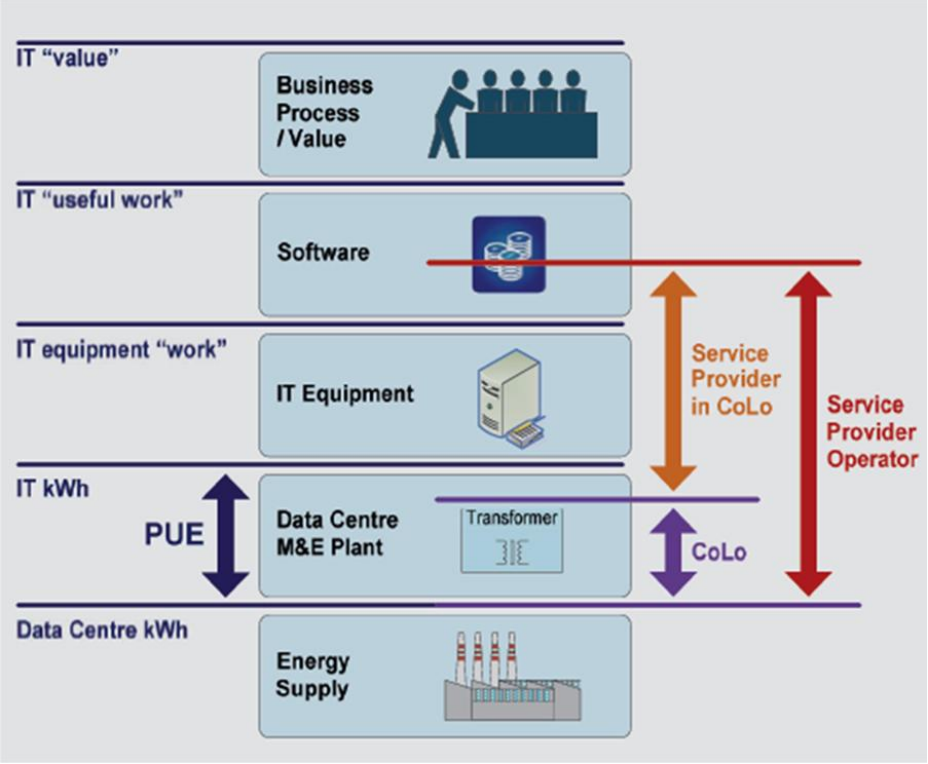


Figura 51 El futuro de las métricas de eficiencia del centro de datos.

Fuente: BCS

Acrónimos

BMS → Building Management System

CCTV → Circuito cerrado de Televisión/cámaras.

CPD → Centro de Proceso de Datos

Data Centers → Centros de Datos

DCIM → Data Center Infrastructure Management

Fps → Frames per second (Imagenes por Segundo).

KPI → *Key Performance Indicator*. Indicadores clave de rendimiento

NOC → *Network Operations Center*. Centro para las Operaciones de Red

PDU → *Power Distribution Unit*. Unidad de Distribución de Potencia

PSU → *Power Supply Unit*. Unidad de Suministro de Potencia

SAI → Sistema de Alimentación Ininterrumpida. *En inglés UPS → Uninterruptible Power Supply*

TI → Tecnología de la información. *En inglés IT → Information Technology*

TIC → Tecnologías de la Información y la Comunicación.

SENATICs → Secretaría Nacional de Tecnologías de la Información y Comunicación

CERT-PY → Centro de Respuesta ante Incidentes Cibernéticos de Paraguay

Bibliografía

- TIA-942: Telecommunications Infrastructure Standards for Data Centers
- Uptime Insitute: Data Center Site Infrastructure Tier Standard: Topology
- BICSI-002: Data Center Design and Implementation Best Practices
- EN1047-2: Secure storage units - Classification and methods of test for resistance to fire - Part 2: Data rooms and data container
- EN-1363: Ensayos de resistencia al fuego.
- EN-60529: Grados de protección proporcionados por las envolventes
- EN-1634: Ensayos de resistencia al fuego y de control de humo de puertas y elementos de cerramiento de huecos, ventanas practicables y herrajes para la edificación.
- EN1627: Puertas peatonales, ventanas, fachadas ligeras, rejas y persianas. Resistencia a la efracción. Requisitos y clasificación.
- EN1630: Puertas peatonales, ventanas, fachadas ligeras, rejas y persianas. Resistencia a la efracción.
- EN 61000: Compatibilidad electromagnética (CEM).
- ISO 1182: Ensayos de reacción al fuego de productos. Ensayo de no combustibilidad.
- DIN-4102: Fire behaviour of building materials and building components
- VDI-2054: Airconditioning systems for computer areas
- EN1815: Revestimientos de suelo resilientes y textiles. Evaluación de la propensión a la acumulación de cargas electrostáticas
- NFP 92-507: Fire test to building material
- 89/392/CE y Directiva de Baja Tensión 93/68/CE, así como EN 61008-1, EN 61009-1, EN 60730-2-7
- NFPA-101: Life Safety Code
- IEC 60076: Power transformers
- ASHRAE TC9.9: Particulate and Gaseous Contamination Guidelines for Data Centers.
- ISO 14644: Airborne Particulate Cleanliness Classes in Cleanrooms and Clean Zones
- NFPA 2001: Standard on Clean Agent Fire Extinguishing Systems

- TIA-568: Commercial building telecommunications cabling standard set
- IEC60364, Comisión electrotécnica internacional, instalaciones eléctricas en baja tensión.
- IEC62305, protección contra descargas atmosféricas
- ANSI/TIA 607 “General Telecomunications Bonding and Grounding for Costumer Permises”
- NEC 250, National Electrical Code, instalaciones eléctricas de EEUU.
- ASHRAE, American Society of Heating, Refrigeration and Air Conditioning Engineers.
- Euronorma EN ECB-S 1047/2