Modelo de Negocios



En términos generales un "Modelo de Negocios" es la forma en que una empresa crea, entrega y captura valor. Adaptada al ámbito de los data centers, el término "modelo de negocios" se refiere al enfoque estratégico que una empresa o proveedor de servicios adopta para ofrecer servicios de centro de datos a sus clientes. Esto implica cómo la empresa estructura sus operaciones,
establece precios, proporciona servicios y genera ingresos en el mercado de los centros de datos.

Algunos aspectos clave de un modelo de negocio en este contexto incluyen:

- ✓ **Tipo de Servicios Ofrecidos**: Esto puede incluir servicios de colocation, hosting, cloud computing, servicios de conectividad, servicios gestionados, entre otros. El modelo de negocio determina qué tipo de servicios se ofrecen y cómo se entregan a los clientes.
- ✓ **Estructura de Precios**: El modelo de negocio define cómo se estructuran los precios de los servicios de data center. Puede ser basado en tarifas fijas, tarifas por uso, modelos de suscripción, o una combinación de estos.
- ✓ **Segmento de Mercado**: Define a qué tipo de clientes se dirige la empresa, como empresas grandes, medianas o pequeñas, startups, industrias específicas, etc.
- ✓ **Diferenciación**: Esto se refiere a cómo la empresa se diferencia de la competencia. Puede ser a través de la calidad del servicio, la tecnología utilizada, la ubicación geográfica, el soporte al cliente, entre otros aspectos.
- ✓ **Escalabilidad y Flexibilidad**: Define la capacidad de la empresa

para adaptarse a las necesidades cambiantes del mercado y de los clientes. Puede incluir la capacidad de escalar la infraestructura según la demanda, ofrecer servicios personalizados o adaptarse a nuevas tecnologías emergentes.

- ✓ **Modelo de Ingresos**: Describe cómo la empresa genera ingresos a partir de sus servicios de data center. Puede incluir ingresos recurrentes de contratos a largo plazo, ingresos por servicios adicionales, ingresos por uso, entre otros.

El modelo de negocios en el ámbito de los data centers es fundamental para definir cómo una empresa proporciona valor a sus clientes, genera ingresos y se posiciona en el mercado de los servicios de infraestructura de TI. Es importante que el modelo de negocio esté alineado con las necesidades del mercado y sea capaz de ofrecer soluciones que satisfagan las demandas de los clientes de manera rentable.

¿Porque nos interesa ver estos enfoques?

Por un lado, puede que la empresa u organización requiera tener toda su infraestructura en forma propietaria, lo cual se conoce como "On-premise" (también escrito "on-premises") y como dijimos, se refiere a la práctica de alojar y ejecutar software, aplicaciones o infraestructura en las instalaciones físicas de una empresa u organización, en lugar de utilizar recursos en la nube o en servidores externos. En otras palabras, significa que los sistemas informáticos y los datos están ubicados y controlados directamente por la organización en su propio centro de datos o en sus propias instalaciones.

Cuando una empresa utiliza soluciones "on-premise", adquiere e implementa la infraestructura física (como servidores, almacenamiento, redes, etc.) y el software necesario para ejecutar sus aplicaciones en su propio entorno, en lugar de depender de servicios externos de alojamiento o de la nube.

El modelo "on-premise" puede ofrecer a las organizaciones un mayor control sobre sus sistemas y datos, así como la capacidad de personalizar y adaptar sus soluciones según sea necesario. Sin embargo, también puede

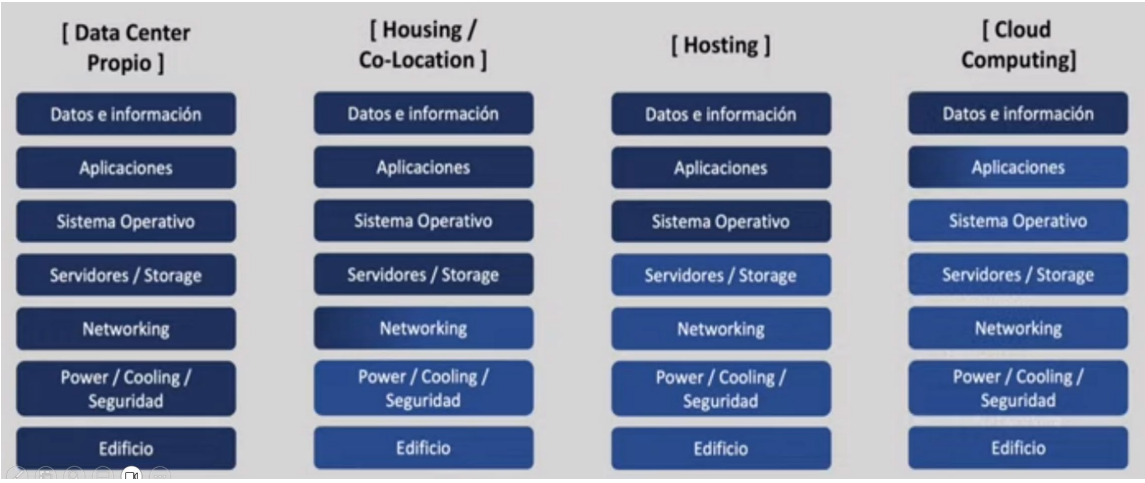
requerir una inversión inicial más alta en hardware, software y mantenimiento, así como la necesidad de personal técnico para administrar y mantener la infraestructura.

Este esquema no interesa dado que lo vamos a indicar en adelante como "Data Center Propio".

No obstante, cuando la empresa u organización entiende que ciertos procesos o infraestructura es posible tercerizarse, lo cual, generalmente responde a un tema relacionados con sus costos operativos, ve la posibilidad de utilizar los esquemas que indicaremos como colocation, hosting y cloud.

En estos casos podemos entender el modelo de negocios desde dos puntos de vista, uno de ellos será el cliente, donde se busca maximizar su performance de servicios tercerizando aquellos que las operaciones y la ley vigente nos permita y por el otro lado, el proveedor, dueño del espacio donde se ofrecerá el alojamiento a terceros.

En este caso podremos entender existen dos visiones. Una de quienes ofrecen el servicio y otra de quienes lo contratan.



A continuación, vamos a incluir los detalles salientes de cada una de las modalidades indicadas

Data Center Propio:

- **Control total**: Tener un data center propio proporciona a la empresa un control total sobre su infraestructura de TI y

datos. Esto significa que pueden personalizar la configuración y la seguridad según sus necesidades específicas.

- **Inversión inicial alta**: Construir y mantener un data center propio requiere una inversión inicial considerable en capital para adquirir hardware, software, sistemas de refrigeración, sistemas de seguridad, y más. Además, implica costos continuos de mantenimiento y actualización.
- **Escalabilidad limitada**: La capacidad de escalar en un data center propio puede ser limitada, ya que la infraestructura física está fija y puede requerir tiempo y recursos adicionales para expandirse.
- **Responsabilidad total de mantenimiento**: La empresa es responsable de mantener la infraestructura, lo que incluye la gestión de la energía, el control de temperatura y humedad, la seguridad física y digital, la administración de backups, entre otros aspectos.

Colocation:

- **Costos compartidos**: Al optar por la colocation, la empresa puede reducir los costos iniciales asociados con la construcción y mantenimiento de un data center propio. Sin embargo, sigue manteniendo el control total sobre sus servidores y equipos.
- **Flexibilidad y escalabilidad**: La colocation permite a las empresas escalar sus operaciones de manera más flexible que si tuvieran un data center propio. Pueden aumentar o disminuir la cantidad de espacio y recursos de TI según sea necesario.
- **Servicios de valor agregado**: Los proveedores de colocation suelen ofrecer servicios adicionales, como conectividad de red, servicios de seguridad, gestión de energía y monitoreo, que pueden mejorar la eficiencia y confiabilidad de la infraestructura.

Hosting:

- **Gestión de hardware por el proveedor**: En un modelo de hosting, la empresa cliente no es responsable de adquirir ni mantener hardware físico, ya que esto lo gestiona el proveedor de hosting.
- **Escalabilidad y flexibilidad**: El hosting puede proporcionar una gran flexibilidad y escalabilidad, ya que los recursos de TI pueden ajustarse rápidamente según las necesidades del negocio.
- **Menor control sobre la infraestructura física**: Aunque el hosting ofrece comodidades y simplifica la gestión de la infraestructura, la empresa tiene menos control directo sobre el hardware y la configuración física de los servidores.

*Hay una diferencia importante entre **colocation y housing**. Aunque a menudo se usan indistintamente, cada término se refiere a un tipo diferente de servicio que un proveedor de centro de datos puede ofrecer.*

*La diferencia principal entre colocation y housing radica en quién es **responsable del hardware físico**. En colocation, la empresa cliente proporciona y gestiona su propio hardware, mientras que en housing, el proveedor de servicios de alojamiento proporciona y gestiona el hardware para la empresa cliente.*

Aquí está la diferencia clave:

***Colocation**: En el modelo de colocation, una empresa alquila espacio en el centro de datos del proveedor y coloca sus propios servidores y equipos de red en ese espacio. La empresa es responsable de proporcionar y mantener su propio hardware, incluyendo servidores, almacenamiento y dispositivos de red. El proveedor de colocation es responsable de proporcionar la infraestructura física del centro de datos, como alimentación eléctrica, refrigeración, conectividad a internet y seguridad*

física. La empresa cliente tiene control total sobre sus servidores y equipos, incluyendo la configuración, el mantenimiento y la seguridad.

***Housing**: En el modelo de housing (también conocido como "dedicated hosting"), la empresa alquila un servidor completo o parte de él, pero el proveedor de servicios de alojamiento es responsable de proporcionar y mantener el hardware. La empresa cliente no tiene que preocuparse por adquirir ni mantener hardware físico, ya que todo el equipo necesario está provisto por el proveedor de housing. El proveedor de housing es responsable de proporcionar y mantener la infraestructura física del centro de datos, así como de la gestión y mantenimiento del hardware. La empresa cliente tiene control sobre el software y los datos que se ejecutan en el servidor, pero no sobre la infraestructura física subyacente*

Cloud Computing:

- **Modelo de pago por uso**: En la nube, los recursos se consumen según la demanda y se pagan únicamente por el uso real. Esto permite a las empresas reducir costos al eliminar la necesidad de invertir en hardware y software costosos de antemano.
- **Elasticidad y escalabilidad**: La nube ofrece una elasticidad excepcional, permitiendo a las empresas escalar hacia arriba o hacia abajo según las fluctuaciones en la demanda, sin preocuparse por la infraestructura subyacente.
- **Amplia gama de servicios**: Los proveedores de la nube ofrecen una amplia gama de servicios, desde infraestructura básica (IaaS) hasta soluciones de software completamente gestionadas (SaaS), lo que permite a las empresas encontrar la combinación adecuada para sus necesidades específicas.

Cada modelo de centro de datos tiene sus propias ventajas y desventajas, y la elección depende de factores como el control deseado, la inversión inicial disponible, la necesidad de escalabilidad y flexibilidad, y la

complejidad de la infraestructura requerida.

Otra forma de ver los diferentes sistemas es como **modelo de capas**, lo que nos ayudará a comprender cómo se estructuran y cómo interactúan entre sí en términos de funcionalidad y responsabilidades.

Data Center Propio como Modelo de Capas:

- **Capa de Infraestructura Física**: Esta es la capa más baja del modelo y comprende la infraestructura física del datacenter, como el suministro eléctrico, la refrigeración, el cableado de red y la seguridad física.
- **Capa de Hardware**: Encima de la capa de infraestructura física se encuentra la capa de hardware, que incluye servidores, almacenamiento, dispositivos de red, switches, enrutadores, firewalls y otros equipos de TI.
- **Capa de Virtualización y Sistema Operativo**: Esta capa proporciona la virtualización de recursos de hardware, lo que permite la creación de máquinas virtuales (VM) y la ejecución de múltiples sistemas operativos en un único servidor físico.
- **Capa de Middleware**: Aquí se encuentran los sistemas y software de middleware que facilitan la comunicación y la interoperabilidad entre aplicaciones, como bases de datos, servidores de aplicaciones, y herramientas de gestión de servicios.
- **Capa de Aplicación**: En la capa de aplicación residen las aplicaciones y servicios específicos que ejecuta la empresa para realizar sus operaciones comerciales, como sistemas ERP[1], CRM, correo

[1] **ERP (Enterprise Resource Planning)**: El sistema de planificación de recursos empresariales (ERP) es un software que integra y gestiona los procesos comerciales y operativos de una empresa en un sistema unificado. ERP típicamente abarca áreas como finanzas, contabilidad, gestión de inventario, compras, recursos humanos, producción, ventas y distribución.

CRM (Customer Relationship Management): El sistema de gestión de relaciones con el cliente (CRM) es una herramienta que ayuda a las empresas a gestionar las interacciones y relaciones con los clientes, tanto actuales como potenciales. Típicamente incluye funciones para gestionar contactos, oportunidades de ventas, actividades de marketing, seguimiento de clientes, servicio al cliente y análisis de datos relacionados con la relación con los clientes.

electrónico, y aplicaciones personalizadas.

- **Capa de Datos**: Esta es la capa superior del modelo y almacena todos los datos generados y utilizados por las aplicaciones de la empresa. Incluye bases de datos, sistemas de almacenamiento de archivos y otros repositorios de datos.

Colocation como Modelo de Capas:

- **Capa de Infraestructura Física**: Similar al modelo de data center propio, esta capa incluye la infraestructura física del centro de datos compartido, como alimentación eléctrica, refrigeración y seguridad física.
- **Capa de Hardware Propio**: La empresa cliente tiene su propia capa de hardware, que incluye servidores, almacenamiento y dispositivos de red, pero se ubica físicamente en el centro de datos del proveedor de colocation.
- **Capa de Middleware y Aplicación**: Estas capas son responsabilidad de la empresa cliente, que implementa y administra su propio software de middleware y aplicaciones sobre la infraestructura proporcionada por el proveedor de colocation.
- **Capa de Datos**: Al igual que en el modelo de data center propio, la capa de datos contiene todos los datos generados y utilizados por las aplicaciones de la empresa, gestionados por la empresa cliente.

Hosting como Modelo de Capas:

- **Capa de Infraestructura Física**: Esta capa es responsabilidad exclusiva del proveedor de hosting, que gestiona la infraestructura física del centro de datos, incluyendo alimentación, refrigeración y seguridad física.
- **Capa de Hardware Compartido**: En este modelo, múltiples clientes comparten los mismos servidores físicos y otros recursos de hardware

proporcionados por el proveedor de hosting.

- **Capa de Sistema Operativo y Middleware**[2]: El proveedor de hosting suele ofrecer una plataforma de hospedaje que incluye sistemas operativos y software de middleware preinstalados o disponibles para su instalación por parte del cliente.
- **Capa de Aplicación**: Los clientes implementan y gestionan sus propias aplicaciones en la plataforma de hospedaje proporcionada por el proveedor, sin preocuparse por la infraestructura subyacente.
- **Capa de Datos**: Los datos generados y utilizados por las aplicaciones de los clientes se almacenan en la infraestructura de almacenamiento proporcionada por el proveedor de hosting.

Cloud Computing como Modelo de Capas:

- **Capa de Infraestructura como Servicio (IaaS)**: Esta es la capa más baja del modelo de la nube e incluye recursos de infraestructura, como servidores virtuales, almacenamiento y redes, que se ofrecen como servicio.
- **Capa de Plataforma como Servicio (PaaS)**: Por encima de IaaS, PaaS proporciona un entorno de desarrollo y ejecución completo que incluye sistemas operativos, middleware, herramientas de desarrollo y otros servicios, permitiendo a los desarrolladores crear y ejecutar aplicaciones sin preocuparse por la infraestructura subyacente.
- **Capa de Software como Servicio (SaaS)**: Esta es la capa más alta del modelo de la nube y ofrece aplicaciones completas como servicio, listas para usar y accesibles a través de internet. Los usuarios pueden acceder a estas aplicaciones a través de un navegador web sin necesidad de instalar software adicional.
- **Capa de Datos**: Al igual que en los otros modelos, la capa de datos almacena todos los datos generados y utilizados por las aplicaciones,

[2] Un **sistema operativo** es un software fundamental que proporciona una interfaz entre el hardware de una computadora y las aplicaciones de software. Por otra parte, el **middleware** es un tipo de software que actúa como intermediario entre distintas aplicaciones, sistemas operativos o dispositivos en una red de computadoras.

pero en la nube, estos datos pueden ser gestionados por servicios de almacenamiento en la nube como bases de datos, sistemas de archivos distribuidos, o almacenamiento de objetos.

Estos modelos de capas proporcionan una estructura útil para comprender la arquitectura y las responsabilidades asociadas con cada uno de los sistemas de centro de datos.

Resumen

A modo de resumen detallamos qué capas son propias de la empresa u organización cliente y cuáles son proporcionadas por el proveedor de servicios en cada uno de los modelos:

1. Data Center Propio:
    - Propias:
        - Capa de Infraestructura Física: La empresa es responsable de adquirir, instalar y mantener la infraestructura física del data center, como sistemas de energía, refrigeración y seguridad física.
        - Capa de Hardware: La empresa es responsable de adquirir, instalar y mantener los servidores, almacenamiento y equipos de red.
        - Capa de Middleware, Aplicación y Datos: La empresa es responsable de instalar, configurar y mantener el software de middleware, las aplicaciones y los datos que se ejecutan en la infraestructura del datacenter.
    - Proporcionadas por la empresa:
        - Todas las capas son responsabilidad directa de la empresa, ya que posee y gestiona todo el data center.
2. Colocation:
    - Propias:
        - Capa de Middleware, Aplicación y Datos: La empresa es responsable de instalar, configurar y mantener el software de middleware, las aplicaciones y los datos

que se ejecutan en sus servidores.

- Proporcionadas por el proveedor de colocation:
    - Capa de Infraestructura Física: El proveedor de colocation es responsable de proporcionar y mantener la infraestructura física del data center, incluyendo alimentación, refrigeración y seguridad física.
    - Capa de Hardware: La empresa es responsable de su propio hardware, pero el proveedor de colocation proporciona el espacio físico, alimentación eléctrica y conectividad de red para estos equipos.

3. Hosting:
    - Propias:
        - Capa de Aplicación y Datos: La empresa es responsable de instalar, configurar y mantener sus propias aplicaciones y datos en la infraestructura proporcionada por el proveedor de hosting.
    - Proporcionadas por el proveedor de hosting:
        - Capa de Infraestructura Física: El proveedor de hosting es responsable de proporcionar y mantener la infraestructura física del datacenter, incluyendo alimentación, refrigeración y seguridad física.
        - Capa de Hardware: El proveedor de hosting proporciona y es responsable del hardware físico, incluyendo servidores y almacenamiento, sobre el cual se ejecutan las aplicaciones de los clientes.
4. Cloud Computing:
    - Propias:
        - Capa de Aplicación y Datos: La empresa es responsable de instalar, configurar y mantener sus propias aplicaciones y datos en la nube.

- Proporcionadas por el proveedor de la nube:
    - Capa de Infraestructura como Servicio (IaaS): El proveedor de la nube proporciona y es responsable de la infraestructura física subyacente, como servidores virtuales, almacenamiento y redes.
    - Capa de Plataforma como Servicio (PaaS): El proveedor de la nube ofrece una plataforma completa de desarrollo y ejecución que incluye sistemas operativos, middleware y herramientas de desarrollo.
    - Capa de Software como Servicio (SaaS): El proveedor de la nube ofrece aplicaciones completas como servicio, listas para usar y accesibles a través de internet, y es responsable de su mantenimiento y operación.

Dicho de otro modo, en un data center propio, la empresa es responsable de todas las capas del modelo, mientras que en los modelos de colocation, hosting y cloud, la responsabilidad se comparte entre la empresa u organización y el proveedor de servicios, dependiendo del nivel de servicio contratado.

Recomendaciones para la construcción de un Datacenter

Existen varias organizaciones independientes que establecen recomendaciones para la construcción de Datacenters. Si bien podría pensarse que esto solo podría ser de interés para las empresas donde se requiera instalar o reacondicionar un datacenter, es posible que desde el punto de vista de un usuario estas recomendaciones sean de utilidad cuando se esté evaluando contratar servicios externos en los modelos que detallamos anteriormente.

A continuación, indicamos algunas de estas recomendaciones:

ANSI/TIA-942

ANSI/TIA-942 es un estándar para la infraestructura de telecomunicaciones en centros de datos, que cubre aspectos como el diseño y la implementación de la infraestructura de telecomunicaciones, incluyendo cableado, espacios y redundancias.

El estándar define requisitos para el diseño y la construcción que ayudan a garantizar que un centro de datos sea capaz de alojar una infraestructura de TI que sea confiable y pueda manejar los cambios y crecimientos futuros. Algunas áreas clave que cubre el estándar incluyen:

- **Espacios del centro de datos**: Define los diferentes espacios dentro de un centro de datos, como salas de equipos, salas de telecomunicaciones y entrada de servicios.
- **Infraestructura del cableado**: Establece las prácticas de cableado estructurado que son importantes para la gestión y escalabilidad a largo plazo del centro de datos.
- **Sistemas de enfriamiento y ambientales**: Proporciona lineamientos sobre cómo manejar el entorno térmico dentro de un centro de datos.
- **Redundancia y resiliencia**: Ofrece criterios para la

redundancia de componentes críticos y la clasificación de data centers en categorías de redundancia, lo que ayuda a determinar el nivel de servicio y disponibilidad que se puede esperar de un data center.

El estándar es mantenido por la Telecommunications Industry Association (TIA), que es un grupo de comercio representando a los fabricantes y proveedores de equipos y servicios de alta tecnología de comunicaciones. La TIA trabaja con la industria y sus estándares son reconocidos a nivel mundial.

ANSI/BICSI 002-2019

ANSI/BICSI 002-2019 es otro estándar importante para data centers. BICSI es una asociación profesional que apoya la industria de las tecnologías de la información y las comunicaciones (ICT), que abarca la cadena de valor de voz, datos, electrónica de seguridad, sistemas de control y audio y video. El estándar ANSI/BICSI 002-2019 es una de las normativas más completas para el diseño y la implementación de centros de datos.

Resumimos a continuación los puntos clave del estándar ANSI/BICSI 002- 2019:

- **Diseño y Layout**: Proporciona lineamientos detallados sobre cómo diseñar la disposición de un data center, incluyendo la ubicación de salas críticas y la optimización del flujo de trabajo.
- **Infraestructura de Cableado**: Ofrece especificaciones para el sistema de cableado estructurado, incluyendo tanto el cableado de cobre como el de fibra óptica y su manejo.
- **Sistemas Eléctricos**: Cubre los requerimientos para la alimentación eléctrica, incluyendo la distribución de energía y las opciones de respaldo como generadores y UPS (sistema de alimentación ininterrumpida).
- **Sistemas Mecánicos**: Se enfoca en los sistemas de enfriamiento y ventilación, esenciales para mantener el

rendimiento y la fiabilidad del hardware crítico.

- **Redundancia y Fiabilidad**: Detalla los niveles de redundancia necesarios para los diferentes sistemas dentro del data center para asegurar la máxima disponibilidad y tiempo de actividad.
- **Seguridad y Protección contra Incendios**: Define las prácticas para la seguridad física y la protección contra incendios, incluyendo la detección y supresión de incendios.
- **Eficiencia Energética y Sostenibilidad**: Aborda cómo diseñar y operar un data center de manera energéticamente eficiente para minimizar el impacto ambiental.
- **Operaciones y Mantenimiento**: Ofrece recomendaciones para el mantenimiento continuo y las operaciones del datacenter, garantizando su operatividad y eficiencia a lo largo del tiempo.

El estándar BICSI 002 es una referencia clave para profesionales que buscan crear instalaciones de data center que no solo sean confiables y seguras, sino que también estén diseñadas para adaptarse a las tecnologías emergentes y las futuras demandas de expansión.

Uptime Institute Tier Standard

El Uptime Institute Tier Standard es un conjunto de criterios de diseño, construcción y operaciones que sirven para asegurar la infraestructura de un data center. Este estándar es ampliamente reconocido a nivel mundial y establece cuatro niveles de data centers, conocidos como Tier I, II, III y IV. Cada Tier refleja un nivel de servicio y una infraestructura de centro de datos, siendo Tier IV el más robusto y resiliente.

Aquí te presentamos un resumen de cada nivel:

Tier I: Básico. Un data center Tier I cuenta con una única ruta para la energía y el enfriamiento y no tiene componentes redundantes o de respaldo. Ofrece 99.671% de disponibilidad.

Tier II: Componentes redundantes. Un data center Tier II incluye componentes redundantes (como refrigeración y UPS) que ofrecen una mayor seguridad frente a fallos. La disponibilidad es del 99.741%.

Tier III: Mantenimiento concurrente. Un data center Tier III permite el mantenimiento y reemplazo de componentes sin interrumpir las operaciones. Ofrece 99.982% de disponibilidad y tiene múltiples rutas de energía y enfriamiento, aunque solo una está activa al mismo tiempo.

Tier IV: Tolerancia a fallos. Un data center Tier IV es completamente tolerante a fallos, con múltiples rutas de enfriamiento y energía activas y redundancia para todo. La disponibilidad esperada es del 99.995%.

Estas certificaciones ayudan a asegurar a los propietarios y operadores de los data centers, así como a los clientes, que la infraestructura cumple con los estándares necesarios para sus necesidades operativas y de negocio.

Cabe señalar que los porcentajes de disponibilidad en el estándar de Uptime Institute se refieren a la cantidad estimada de tiempo que un data center está operativo y disponible para su uso en el transcurso de un año. Estos son valores anuales y se basan en la premisa de que un año tiene 8,760 horas.

Aquí están los porcentajes de disponibilidad explicados en términos de tiempo de inactividad anual esperado:

Tier I: 99.671% de disponibilidad implica un tiempo de inactividad de aproximadamente 28.8 horas al año.

Tier II: 99.741% de disponibilidad se traduce en un tiempo de inactividad de aproximadamente 22 horas al año.

Tier III: 99.982% de disponibilidad significa que el tiempo de inactividad esperado es de alrededor de 1.6 horas al año.

Tier IV: 99.995% de disponibilidad equivale a un tiempo de

inactividad de solo 0.4 horas (24 minutos) al año.

Estos valores no son acumulativos y se restablecen cada año. Por lo tanto, los porcentajes son una medida de cuánto tiempo, en promedio, se espera que el centro de datos esté funcionando sin interrupciones en cualquier año dado. Esto no significa que un data center experimentará con seguridad la cantidad exacta de inactividad indicada; son promedios basados en las capacidades de diseño del datacenter y la probabilidad teórica de fallo.

Creemos importante señalar que las disponibilidades calculadas para los diferentes Tiers del Uptime Institute no incluyen las salidas de servicio programadas o el mantenimiento planeado. Estas cifras de disponibilidad se refieren a la inactividad no planeada que afecta la operación del datacenter.

El Uptime Institute define claramente que la certificación Tier refleja la redundancia y la capacidad de un data center para permanecer operativo durante interrupciones ***no planeadas***.

Por ejemplo, un data center Tier III está diseñado para permitir cualquier componente de la infraestructura crítica o la ruta de distribución a ser apagado o removido sin impactar la operación del computador crítico. Esto es parte de la idea de "mantenimiento concurrente" y no se considera una inactividad en términos de la disponibilidad del Tier.

Cabe señalar que el mantenimiento planeado es parte de las operaciones normales de cualquier data center y es esencial para su funcionamiento a largo plazo.

Los procedimientos y políticas de mantenimiento adecuados son importantes para garantizar que el centro de datos pueda operar según lo previsto y mantener su certificación Tier.

Asimismo, el Instituto ofrece un servicio de certificación cuyas etapas son:

1. **Certificación de Diseño de Documentos**: Evalúa si los documentos de diseño cumplen con los requisitos específicos

del Tier seleccionado.

2. **Certificación de Instalaciones Construidas**: Una vez que el data center está construido, se verifica que esté hecho de acuerdo con los diseños y puede cumplir con los requisitos del Tier correspondiente.
3. **Certificación de Operaciones Sustentables**: Esta certificación se enfoca en las operaciones y la gestión en curso del data center, asegurando que se sigan las mejores prácticas para mantener la certificación Tier.

Seguridad y Monitoreo

Los centros de procesamiento de datos, dado que albergan una gran cantidad de información crítica, más allá de las características de disponibilidad que hemos tratado. Es necesario también contemplar la debida protección contra accesos no autorizados, incendios, desastres naturales y condiciones ambientales adversas.

A continuación, exploraremos las mejores prácticas y tecnologías utilizadas para garantizar la seguridad física y el monitoreo ambiental en los datacenters.

Controles de acceso físico

Definición y Objetivo

Los controles de acceso físico son mecanismos y procedimientos diseñados para restringir y monitorizar la entrada a áreas sensibles dentro de un datacenter. Su objetivo es prevenir el acceso no autorizado, proteger la integridad de los datos y garantizar la seguridad del personal y los activos físicos.

Tipos de Controles de Acceso

- **Sistemas de tarjetas de acceso:** Utilizan tarjetas inteligentes que permiten la entrada a áreas específicas mediante lectores de tarjetas.

- Lectores biométricos: Verifican la identidad de una persona utilizando características físicas únicas como huellas dactilares, reconocimiento facial o escáneres de retina.

- Autenticación multifactor: Combina múltiples métodos de verificación (algo que el usuario sabe, algo que tiene y algo que es) para aumentar la seguridad.

Buenas Prácticas

- Zonas de acceso restringido: Delimitación clara de áreas con diferentes niveles de acceso según la función y la autorización del personal.

- Registros de entrada y salida: Mantenimiento de registros detallados de todas las personas que ingresan y salen del datacenter.

- Supervisión y auditoría continua: Monitoreo constante y auditorías regulares para asegurar el cumplimiento de las políticas de seguridad.

Protección contra incendios y otros desastres naturales

Sistemas de Protección contra Incendios

- Sistemas de detección de humo y calor: Sensores que detectan la presencia de humo o un aumento anormal de temperatura, activando alarmas y sistemas de supresión.

- Sistemas de extinción de incendios: Utilización de distintos medios como agua, gases inertes o químicos para extinguir incendios de manera eficiente y segura para los equipos electrónicos.

Prevención y Respuesta ante Desastres Naturales

- Evaluación de riesgos geológicos y climáticos: Análisis de la ubicación del datacenter para identificar riesgos como terremotos, inundaciones o tormentas.

- Planes de contingencia y recuperación: Desarrollo de estrategias y procedimientos para minimizar el impacto y asegurar una rápida recuperación en caso de desastres.

- Diseño estructural resistente: Construcción de instalaciones con características que soporten eventos naturales extremos.

Monitoreo Ambiental

Importancia del Monitoreo Ambiental

El monitoreo de las condiciones ambientales dentro de un datacenter es esencial para prevenir fallos en los equipos y garantizar un funcionamiento óptimo. Factores como la temperatura, la humedad y la calidad del aire pueden afectar significativamente el rendimiento y la vida útil de los equipos.

Parámetros Que Monitorear

- Temperatura y Humedad: Mantener estos parámetros dentro de rangos específicos para evitar el sobrecalentamiento y la condensación que pueden dañar los equipos.

- Calidad del aire y partículas: Monitorear la presencia de polvo y contaminantes que puedan obstruir o dañar los componentes electrónicos.

- Presencia de agua y otros líquidos: Detección de fugas o humedad que puedan causar cortocircuitos o corrosión.

Tecnologías de Monitoreo

- **Sensores y sistemas de alerta:** Instalación de sensores que proporcionan datos en tiempo real y alertas inmediatas en caso de desviaciones de los parámetros normales.

- **Integración con sistemas de gestión de infraestructura:** Uso de plataformas que centralizan la información de todos los sistemas de monitoreo para una gestión más eficiente.

- Monitoreo remoto y en tiempo real: Capacidades para supervisar el entorno del datacenter desde ubicaciones remotas, asegurando una respuesta rápida ante cualquier problema.

Conclusión

Implementar controles de acceso físico, sistemas de protección contra incendios y monitoreo ambiental es esencial para la seguridad y operatividad de un datacenter. Estas medidas no solo protegen la infraestructura y los datos críticos, sino que también aseguran la continuidad del negocio y la resiliencia ante posibles incidentes.