



**Universidad Autónoma de Baja California**  
Facultad de Ingeniería Mexicali  
Ingeniería en Computación

---

**Reporte de Actividad:  
Conocer un Centro de Datos**

---

**Materia:**

Redes de Computadoras

**Unidad: 1 Semana: 1**

**Profesor:**

Mtro. Emmanuel Zúñiga Torres

**EQUIPO 05:**

---

Moya Monreal Erick Anselmo — 1110604  
Rodríguez Maldonado Irving Alejandro — 1182794

Mexicali, Baja California  
31 de enero de 2026

## Lista de contenido

<b>1. Introducción</b>	<b>2</b>
<b>2. Desarrollo</b>	<b>4</b>
2.1. Características Físicas del Centro de Datos . . . . .	4
2.2. Infraestructura, Respaldo y Manejo de Eventualidades . . . . .	4
2.3. Ventilación, Refrigeración y Disposición Física . . . . .	5
2.4. Seguridad en Capas y Estándares Aplicables . . . . .	5
2.5. Control de la Información y Protección de Datos . . . . .	7
2.6. Modelos de Cómputo en la Nube y Rentabilidad . . . . .	7
<b>3. Conclusiones</b>	<b>9</b>
<b>Referencias</b>	<b>10</b>

## 1. Introducción

Para la realización de este taller se utilizaron los recursos electrónicos proporcionados por el profesor a través de la plataforma Classroom. Dichos recursos se organizaron en tres ejes temáticos principales: Centros de Datos, Estándares en Centros de Datos y Tipos de Cómputo en la Nube.

Durante la sesión de clase se visualizaron los materiales audiovisuales, mientras se realizaba la toma de notas enfocada en los aspectos más relevantes. El profesor destacó una serie de criterios clave que debían considerarse para el análisis y desarrollo del presente reporte, entre los cuales se incluyen:

1. Acceso exterior y disposición de la seguridad perimetral, así como su estructuración por capas.
2. Planes de respuesta ante emergencias y eventualidades.
3. Accesos interiores y medidas de seguridad para áreas restringidas del centro de datos.
4. Distribución de la infraestructura y organización de los servidores.
5. Seguridad de la información.
6. Volúmenes de hardware, ancho de banda y medios de transmisión, principalmente fibra óptica.
7. Distribución geográfica de los centros de datos a nivel global.
8. Procesos de destrucción física de datos y manejo de residuos.
9. Sistemas de refrigeración, considerando las variaciones climáticas.
10. Sistemas de alimentación eléctrica y mecanismos de respaldo.
11. Niveles de acceso y personal autorizado.
12. Protección de los datos mediante técnicas de encriptación.
13. Certificaciones que cumplen los centros de datos.
14. Sostenibilidad financiera de la operación.

Posteriormente, se analizó una imagen esquemática representativa de un centro de datos típico, identificando sus principales componentes y relacionándolos con los elementos observados en los recursos audiovisuales revisados.

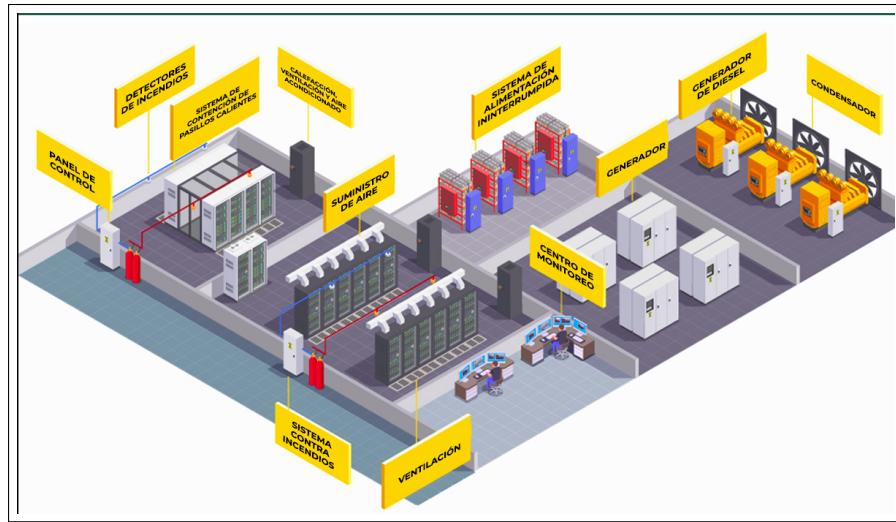


Figura 1: Esquema de un Centro de Datos típico.

Asimismo, se estudiaron los diferentes estándares que regulan la construcción y operación de los centros de datos, haciendo énfasis en su preparación ante fallos, emergencias y escenarios críticos. Finalmente, se discutieron los distintos tipos de cómputo en la nube, junto con sus ventajas, desventajas, modelos de servicio y despliegue más comunes, así como la rentabilidad de los centros de datos desde la perspectiva empresarial y su viabilidad económica para cualquier negocio o empresa.

## 2. Desarrollo

### 2.1. Características Físicas del Centro de Datos

Los centros de datos analizados se caracterizan por una infraestructura física diseñada para operar de forma continua, segura y tolerante a fallos [2, 3]. La ubicación del sitio, la disposición del perímetro y la segmentación de áreas internas responden a criterios de seguridad, eficiencia operativa y control de riesgos.

El perímetro exterior cuenta con barreras físicas, señalización, vigilancia permanente y sistemas de detección, lo que permite prevenir accesos no autorizados desde el primer nivel. Internamente, el diseño del centro de datos separa claramente las áreas administrativas, técnicas y críticas, restringiendo progresivamente el acceso conforme se avanza hacia el piso de datos.

La disposición física de los servidores se organiza en racks de alta densidad, alineados para optimizar el flujo de aire frío y caliente, reduciendo puntos de sobrecalentamiento y mejorando la eficiencia energética del recinto.



Figura 2: Visualización de racks de alta densidad y cableado de fibra óptica en un centro de datos de Google.

### 2.2. Infraestructura, Respaldo y Manejo de Eventualidades

La infraestructura tecnológica está compuesta por miles de servidores personalizados, sistemas de almacenamiento distribuido y redes de alta velocidad basadas principalmente en fibra óptica. El ancho de banda disponible es un elemento crítico, permitiendo la transmisión masiva de datos a escala global con latencias mínimas.

Para garantizar la continuidad operativa ante fallos, los centros de datos implementan múltiples niveles de respaldo. En el suministro eléctrico se utilizan sistemas UPS, bancos de baterías y generadores de emergencia que permiten mantener la operación incluso ante interrupciones prolongadas del servicio eléctrico externo.

El manejo de eventualidades y emergencias incluye planes de continuidad del negocio y recuperación ante desastres, los cuales contemplan fallos eléctricos, incendios, inundaciones, sismos y otras inclemencias. Estos planes se apoyan en estándares internacionales que definen los niveles de redundancia, disponibilidad y tolerancia a fallos que debe cumplir un centro de datos moderno.

### 2.3. Ventilación, Refrigeración y Disposición Física

La ventilación y la refrigeración son elementos esenciales debido a la alta densidad de hardware y la generación constante de calor. Los sistemas de enfriamiento varían según el clima de la región, empleando desde enfriamiento por aire exterior hasta circuitos de agua y torres de evaporación.

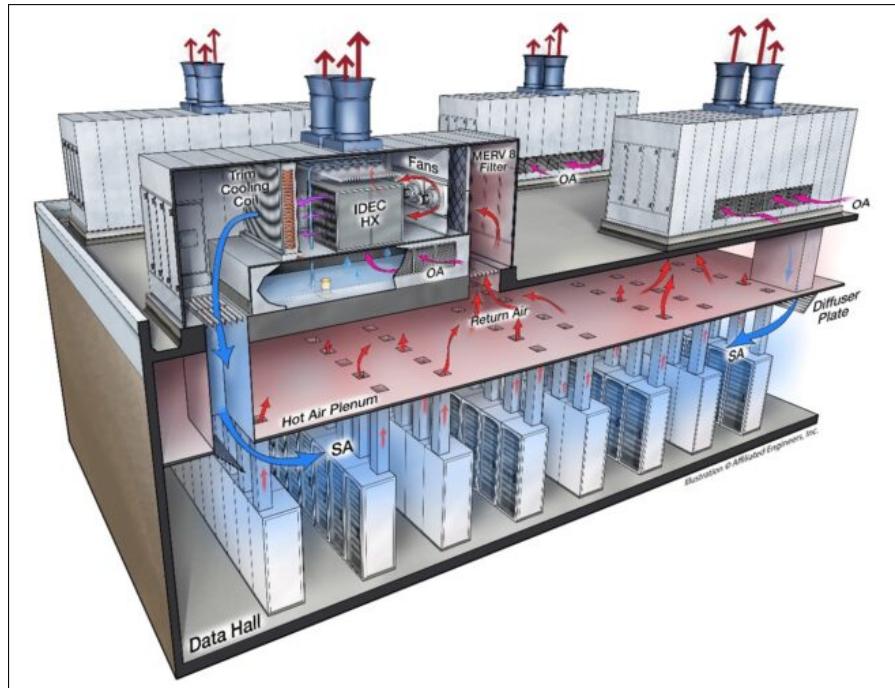


Figura 3: Esquema de sistemas de enfriamiento en un centro de datos.

La disposición física de los equipos sigue el principio de pasillos fríos y calientes, permitiendo dirigir el flujo de aire de manera eficiente y reducir el consumo energético. Estos sistemas están monitoreados constantemente para detectar variaciones de temperatura y responder de forma automática ante cualquier anomalía.

### 2.4. Seguridad en Capas y Estándares Aplicables

La seguridad del centro de datos se estructura mediante un enfoque de seguridad en capas [1], donde cada nivel añade un control adicional que limita el acceso únicamente al personal autorizado. Este modelo reduce significativamente la probabilidad de intrusión y errores humanos.

Los estándares más relevantes en este contexto incluyen aquellos relacionados con la infraestructura, la seguridad de la información y la continuidad del servicio, los cuales establecen lineamientos claros para la respuesta ante emergencias, incendios y fallos críticos. La certificación bajo estos estándares garantiza que el centro de datos cumpla con prácticas reconocidas a nivel internacional.

Capa de Seguridad	Descripción
Perímetro	Vallas, vigilancia física y control de accesos externos.
Acceso al edificio	Controles de identidad y sistemas biométricos.
Áreas internas	Segmentación de zonas y acceso restringido.
Piso de datos	Acceso exclusivo a personal técnico autorizado.
Destrucción de medios	Eliminación física segura de dispositivos de almacenamiento.

Tabla 1: Ejemplo de estructura de seguridad en capas en un centro de datos.

A continuación, se muestra la relación entre las capas de seguridad física observadas y algunos de los estándares internacionales que regulan su implementación.

Capa de Seguridad	Estándar Asociado
Perímetro	ISO/IEC 22237, ANSI/TIA-942
Acceso al edificio	ISO/IEC 27001
Áreas internas	Uptime Institute Tier Standard
Piso de datos	ISO/IEC 27001
Protección contra incendios	NFPA 75 / NFPA 76

Tabla 2: Relación entre capas de seguridad física y estándares aplicables.

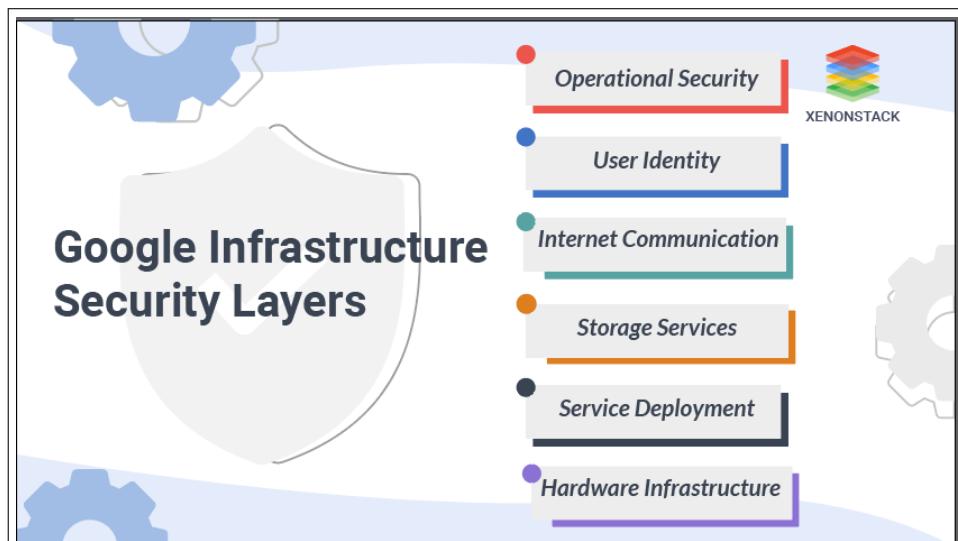


Figura 4: Ejemplo de seguridad en capas en un centro de datos.

## 2.5. Control de la Información y Protección de Datos

El control de la información es un aspecto crítico en la operación de los centros de datos, ya que estos manejan grandes volúmenes de información sensible perteneciente a usuarios y organizaciones. Para garantizar la privacidad, los datos se protegen mediante técnicas de encriptación tanto en tránsito como en reposo.

El acceso a la información está estrictamente regulado mediante políticas de autorización y monitoreo continuo. En caso de que los dispositivos de almacenamiento lleguen al final de su vida útil o presenten fallos, se aplican procesos de destrucción física controlada, asegurando que la información no pueda ser recuperada.

Estas medidas permiten resguardar la confidencialidad, integridad y disponibilidad de los datos, cumpliendo con los requisitos legales, técnicos y éticos asociados al manejo de la información digital.



Figura 5: Proceso de trituración física de discos duros para la eliminación segura de datos residuales.

## 2.6. Modelos de Cómputo en la Nube y Rentabilidad

Finalmente, se analizaron los modelos de cómputo en la nube, particularmente el enfoque *Everything as a Service* (XaaS) [5], que permite a las organizaciones acceder a recursos tecnológicos bajo demanda. Estos modelos reducen costos de inversión inicial, delegan la gestión de infraestructura al proveedor y mejoran la escalabilidad de los servicios.

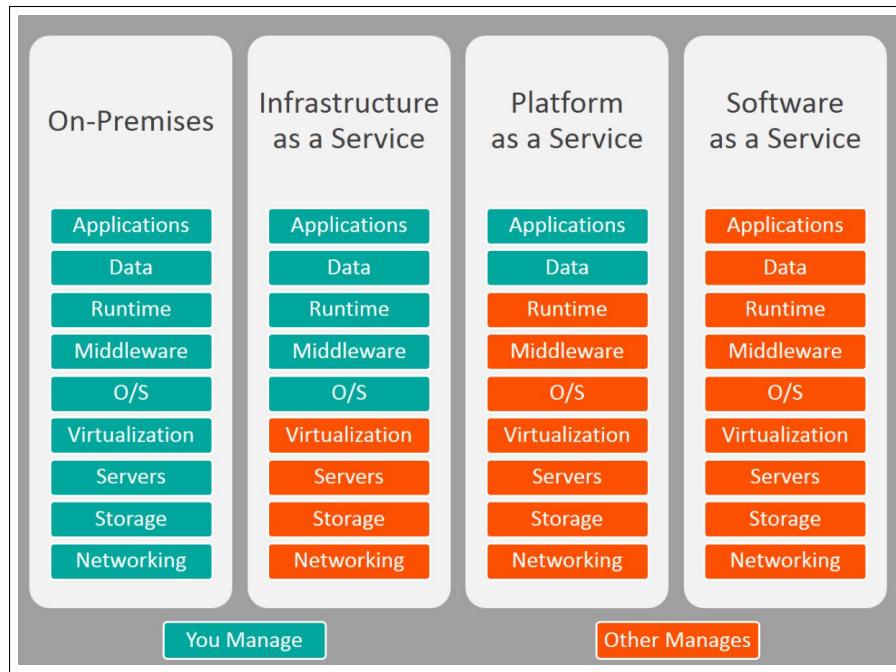


Figura 6: Modelos de servicio en la computación en la nube.

Desde una perspectiva empresarial, la rentabilidad de los centros de datos se fundamenta en la optimización de recursos, la automatización de procesos y la capacidad de ofrecer servicios confiables a gran escala, convirtiéndose en un elemento clave para la competitividad de cualquier negocio o empresa.

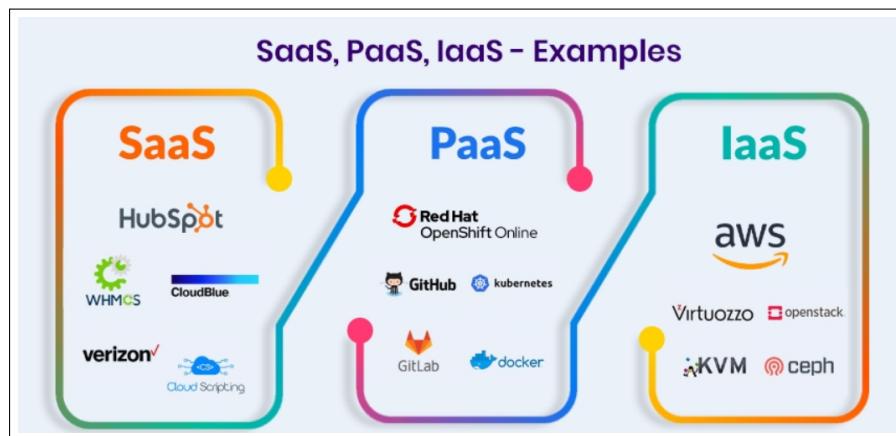


Figura 7: Ejemplos de servicios de computación en la nube.

### 3. Conclusiones

El análisis de los centros de datos permitió comprender que estos no son únicamente espacios destinados al almacenamiento de información, sino infraestructuras altamente controladas, diseñadas para operar de manera continua y segura bajo cualquier circunstancia. Uno de los aspectos que más destaca es el nivel de seguridad implementado, tanto en el acceso exterior como en las áreas internas, donde el ingreso se restringe de forma progresiva hasta limitar el acceso al piso de datos a un porcentaje mínimo del personal autorizado.

Otro punto relevante es la forma en que se protege la información. La destrucción física de los dispositivos de almacenamiento, como los discos duros, evidencia la importancia que se le da a evitar cualquier recuperación de datos una vez que estos dejan de ser utilizables. Este proceso, junto con el manejo adecuado de residuos y reciclaje de materiales, refleja una preocupación no solo por la seguridad de la información, sino también por el impacto ambiental de la operación.

Asimismo, resulta evidente la importancia de los sistemas de respaldo y de los planes de respuesta ante emergencias. La presencia de múltiples fuentes de alimentación, sistemas de respaldo energético y mecanismos de recuperación ante fallos permite que los centros de datos continúen operando incluso ante eventos críticos como cortes eléctricos o desastres naturales. Esto demuestra que la confiabilidad del servicio depende en gran medida de la preparación previa ante escenarios adversos.

En conjunto, el recorrido y análisis de un centro de datos permitió identificar que su diseño, operación y mantenimiento están orientados a garantizar la disponibilidad constante de los servicios, la protección de la información y la minimización de riesgos. Estos elementos, que no siempre son visibles para el usuario final, resultan fundamentales para el funcionamiento de los servicios digitales que forman parte de la vida cotidiana.

## Referencias

- [1] Google Cloud. *Data Center Security: 6 Layers Deep*. [Archivo de video]. Recuperado de: <https://youtu.be/kd33UVZhnAA>
- [2] Google Cloud. *Google Data Center 360° Tour*. [Archivo de video]. Recuperado de: <https://youtu.be/zDAYZU4A3w0>
- [3] Google Data Centers. *Infraestructura y Seguridad Global*. Recuperado de: <https://datacenters.google/intl/es-419/>
- [4] Telmex. *Centros de Datos de Clase Mundial*. [Archivo de video]. Recuperado de: [https://www.youtube.com/watch?v=jsrv4eiT\\_ro](https://www.youtube.com/watch?v=jsrv4eiT_ro)
- [5] Red Hat. *Cloud Computing: Public, Private and Hybrid*. Recuperado de: <https://www.redhat.com/es/topics/cloud-computing/>
- [6] Google. *Sustainability in Data Centers*. Recuperado de: <https://datacenters.google/efficiency/>