INTR. A LA NUBE PÚBLICA

TEMA 2: Infraestructura global y seguridad básica

DESARROLLO DE APLICACIONES MULTIPLATAFORMA y WEB

DANIEL LILLO

PEQUEÑO REPASO

El usuario no conoce ni gestiona la infraestructura física que soporta los servicios, recursos y datos alojados. Existen:

- Modelos de servicio (IaaS, PaaS, SaaS...)
- Modelos de despliegue (pública, privada, híbrida...).

PEQUEÑO REPASO

La nube está formada por centros de datos interconectados por todo el mundo.

Cada centro de datos alberga servidores, sistemas de refrigeración, energía y red.

Se agrupan por zonas y regiones para mejorar la **disponibilidad** y la **latencia**.

ESTRUCTURA GLOBAL

Los **centros de datos** son la infraestructura física con servidores y sistemas de energía y red.

Las **regiones** son un conjunto de **zonas de disponibilidad** cercanas geográficamente. Cada **zona** dispone de varios **centros de datos**.

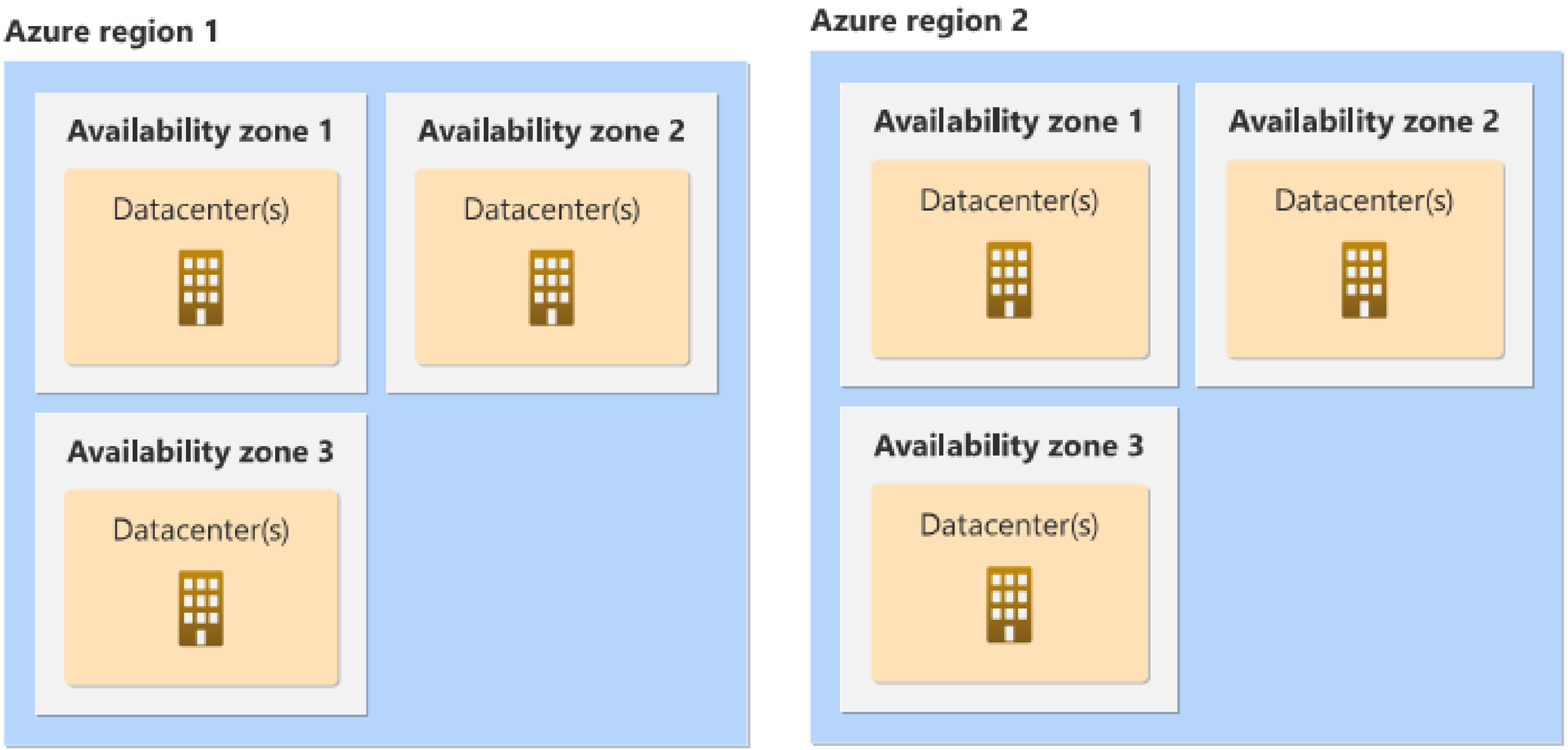
¿Qué es una zona de disponibilidad (AZ)?

ZONAS DE DISPONIBILIDAD

Las **zonas de disponibilidad** (AZ) son uno o varios centros de datos conectados dentro de una misma región.

Se sitúan a una distancia prudencial para que una caída de red o un desastre natural no afecte a todas las zonas de disponibilidad de una misma región.

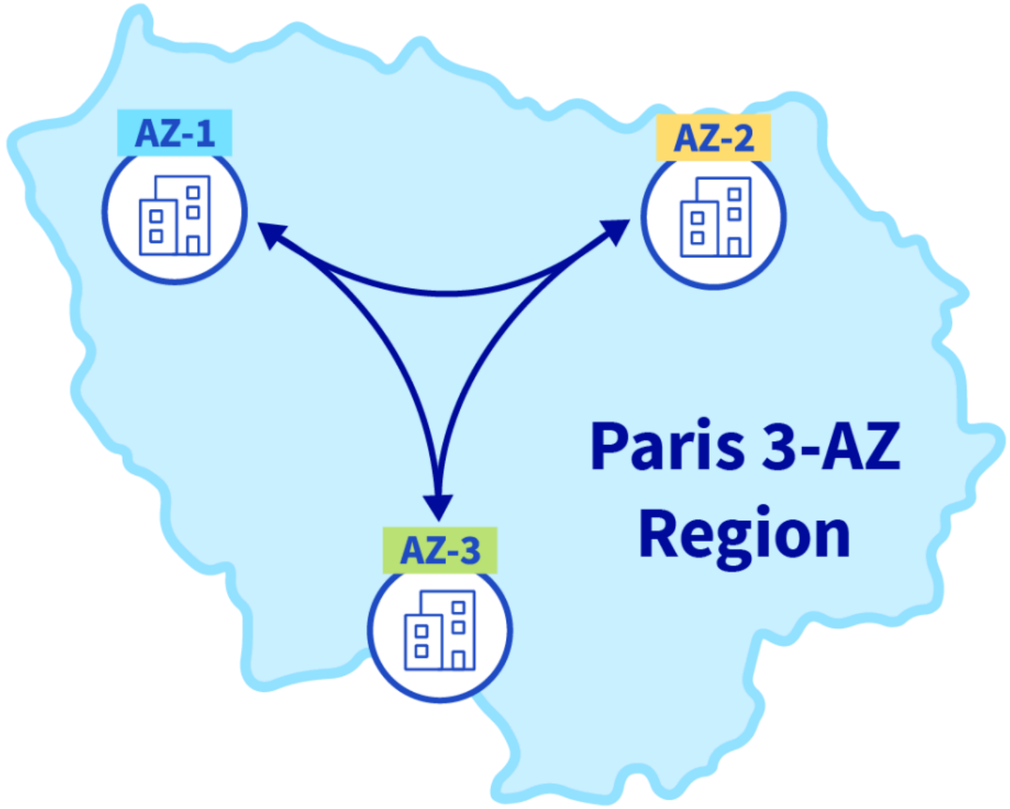
Las AZ están conectadas entre sí por una red privada de fibra, lo que mejora la fiabilidad y la disponibilidad.


Azure region 1
Availability zone 1
Datacenter(s)
Availability zone 2
Datacenter(s)
Availability zone 3
Datacenter(s)
Azure region 2
Availability zone 1
Datacenter(s)
Availability zone 2
Datacenter(s)
Availability zone 3
Datacenter(s)

ZONAS DE DISPONIBILIDAD

Estas AZ permiten cambiar el flujo de tráfico entre ellas para mantener activa la región.

Si se cae la instancia “a”, todo el flujo pasa a la instancia “b”.



ELECCIÓN DE LA REGIÓN

A la hora de elegir la región, debemos tener en cuenta los siguientes apartados:

1. Que la región elegida cumpla nuestros requisitos legales. Por ejemplo, los datos del gobierno de EE.UU. deben estar, por ley, alojados en EE.UU.

2. Desplegar en la región de donde provengan la mayoría de los clientes.

ELECCIÓN DE LA REGIÓN

3. No todos los servicios se encuentran en todas las regiones, por lo que deberemos elegir la región también en función de si se encuentra en ella el servicio o servicios que nos interesan.

4. Precio. No todas las regiones cobran lo mismo por diversos servicios. Por ejemplo, el almacenamiento en S3 en AWS es más caro en Sao Paulo respecto a otras regiones.

PARTE PRÁCTICA DEL TEMA

Os vais a dividir por parejas, a cada una se le asignará un proveedor de los siguientes:

- AWS
- Azure
- Google Cloud
- Oracle Cloud

Debéis visitar el **mapa de regiones** situado en su página oficial y responder en un documento las siguientes preguntas.

PARTE PRÁCTICA DEL TEMA

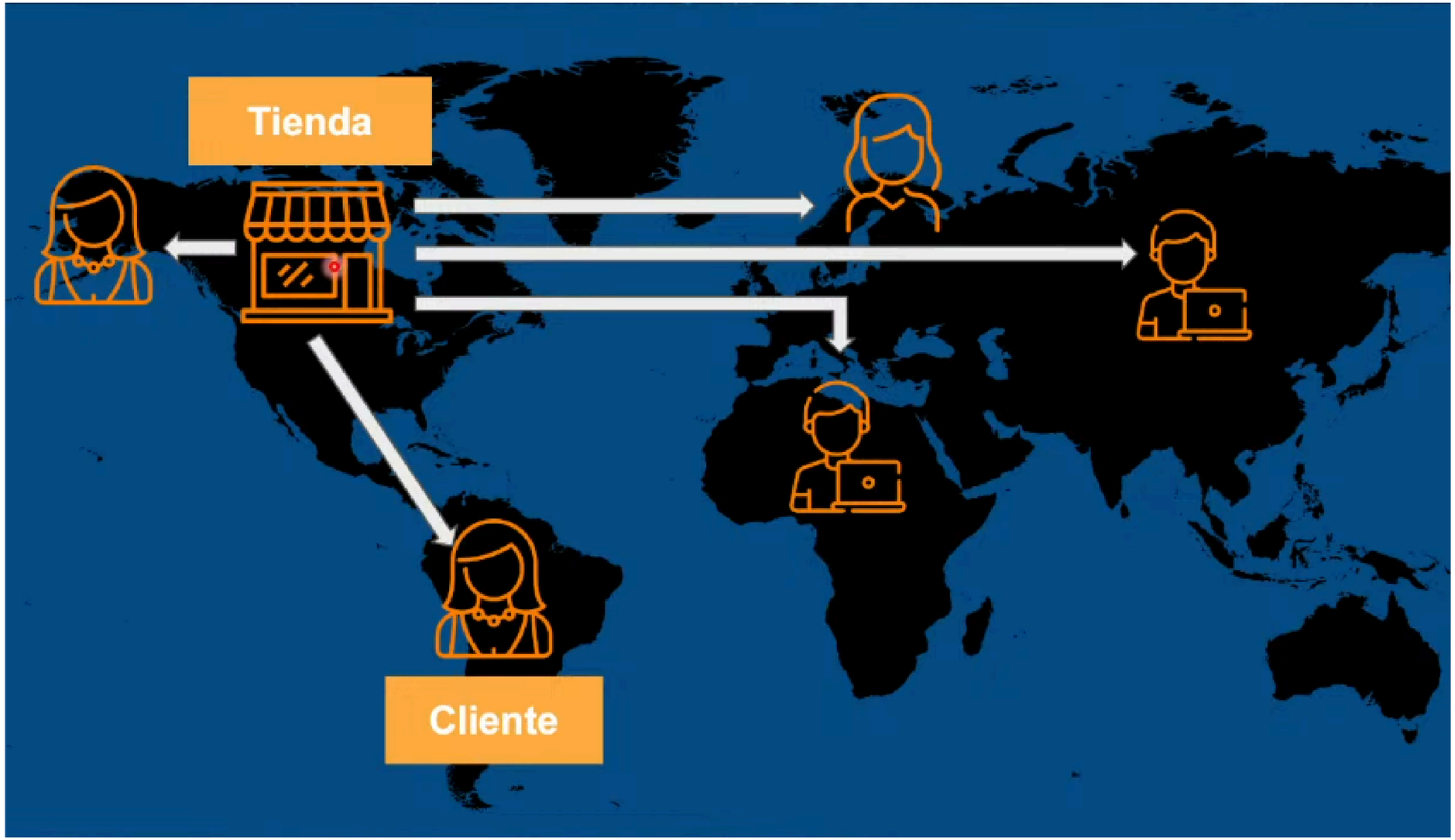
- ¿Cuántas regiones activas tiene el proveedor? Nombra tres regiones futuras.
- ¿Cuál es la más cercana a España? ¿Cuántas regiones existen en la zona oeste de Europa?
- ¿En qué continente hay menos regiones? ¿Por qué?
- ¿Cuál es la zona más abundante de regiones?
- ¿Existe alguna región aislada? ¿Cuál? ¿Por qué?

EL CONCEPTO DE CDN

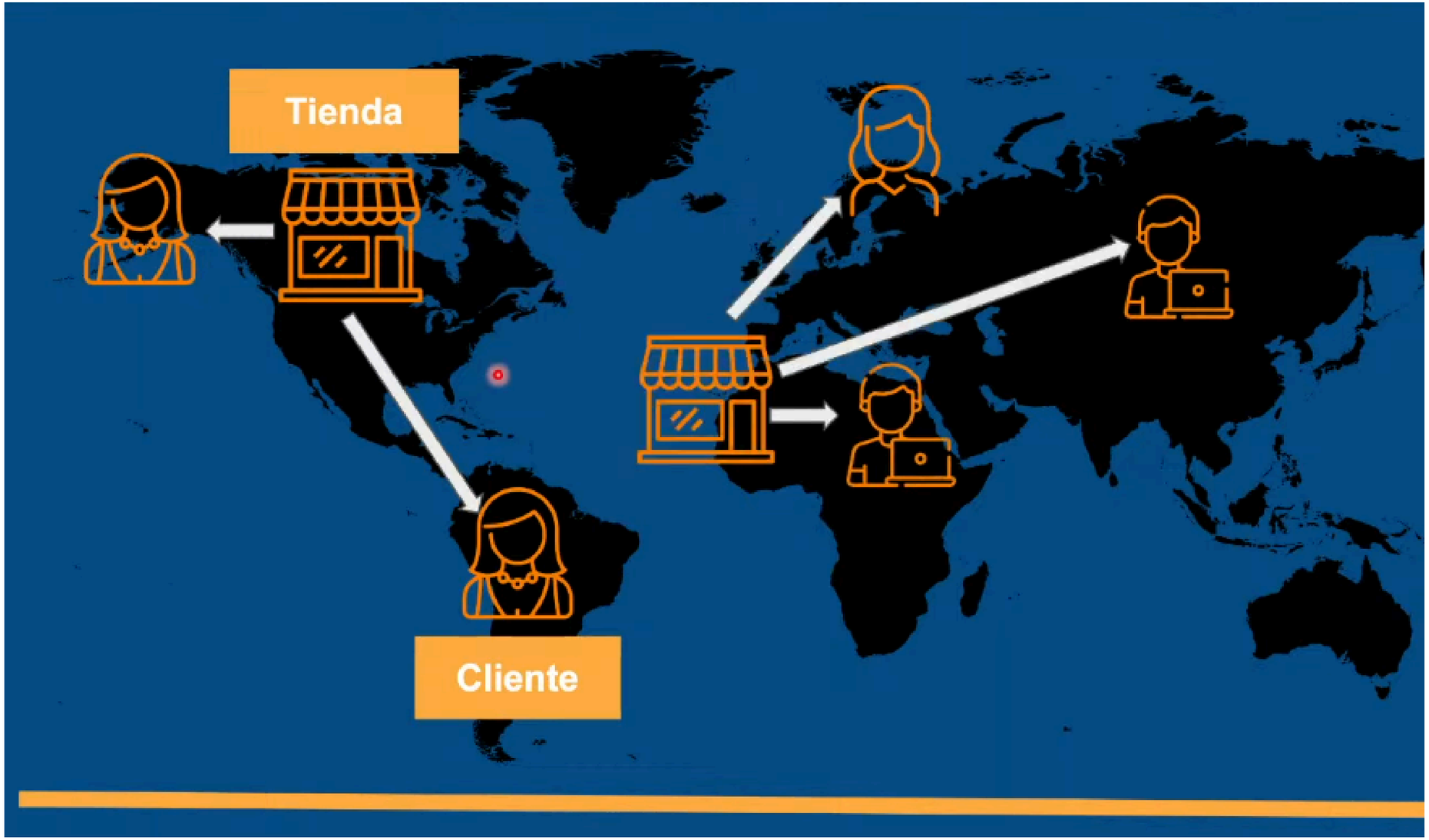
Un CDN (Content Delivery Network o Red de Entrega de Contenido) es una red de servidores interconectados que acelera la carga de las páginas web para las aplicaciones que tienen un uso intensivo de datos.

Los datos deben viajar por Internet desde el servidor al usuario. Si el usuario se encuentra lejos, la **latencia** será muy alta, por lo que el contenido del sitio se almacena en servidores de CDN ubicados más cerca de los usuarios.

EL CONCEPTO DE CDN



EL CONCEPTO DE CDN



EL CONCEPTO DE CDN

Las ventajas de las CDN son:

EL CONCEPTO DE CDN

Las ventajas de las CDN son:

- Reducir el tiempo que las páginas tardan en cargar
- Reducir los costos del ancho de banda
- Aumentar la disponibilidad del contenido
- Mejorar la seguridad del sitio web

PARTE PRÁCTICA DEL TEMA

¿Qué función realizan y para qué sirven los siguientes conceptos de Amazon Web Services?

- CloudFront
- Edge Location
- AWS Outpost

CLOUDFRONT

Amazon CloudFront sirve para agilizar la distribución de contenido web estático y dinámico (.html, .css, .js, imágenes) al usuario.

CloudFront entrega el contenido a estos usuarios a través de una red mundial de centros de datos llamados **Edge Locations**.

La solicitud del usuario se redirige a la Edge Location que ofrece la menor latencia.

CLOUDFRONT

Su funcionamiento es tal que así:

Si el contenido ya se encuentra en la Edge Location con menor latencia, se le entrega al usuario.

En caso contrario, CloudFront lo recupera de aquello que se haya definido como origen del contenido.

AWS OUTPOSTS

AWS Outposts se trata de un servicio que extiende los servicios y el almacenamiento de AWS para ser utilizados en centros de datos On-Premise.

Con estos racks de servidores, la empresa puede ejecutar algunos servicios de AWS en local.

NECESIDADES DE LA NUBE

Se me ha ocurrido montar una aplicación/web del estilo de YouTube en la que habrá clases online de cualquier asignatura y cualquier profesor que quiera proporcionarlas. El modelo de negocio es irrelevante.

¿Qué necesito para crear mi aplicación?

NECESIDADES DE LA NUBE

Respecto a la aplicación/empresa de la que se realizó la práctica anterior, responde a las siguientes preguntas:

- ¿Qué tipo de datos maneja? (archivos, texto, vídeos, usuarios...).
- ¿Qué datos deben estar siempre disponibles?
- ¿Qué datos pueden almacenarse sin acceso inmediato?

PROVEEDORES CLOUD

La nube es un ecosistema de servicios, por lo que los proveedores no venden servidores, sino estos **servicios**.

ACTIVIDAD

Accede a la documentación de un proveedor (por ejemplo, AWS) e identifica al menos 8 categorías de servicios.

Haz una tabla clasificando estas categorías en categorías de servicios principales y categorías de servicios complementarias.

Justifica brevemente por qué encasillas a cada una en cada tabla.

ALMACENAMIENTO

En la nube, almacenar datos implica **decisiones de arquitectura**.

No todo el almacenamiento ofrece la misma latencia, la misma durabilidad o el mismo coste.

¿Qué puede implicar elegir mal?

ALMACENAMIENTO

En la nube, almacenar datos implica **decisiones de arquitectura**.

No todo el almacenamiento ofrece la misma latencia, la misma durabilidad o el mismo coste.

Elegir mal puede implicar un alto sobrecoste para la empresa, bajo rendimiento relativo o riesgos de disponibilidad. **El almacenamiento condiciona toda la arquitectura**.

ALMACENAMIENTO

¿Cuáles son las tecnologías de almacenamiento en la nube según su contenido?

¿Se categorizan por “qué guardan” o por otros motivos?

ALMACENAMIENTO

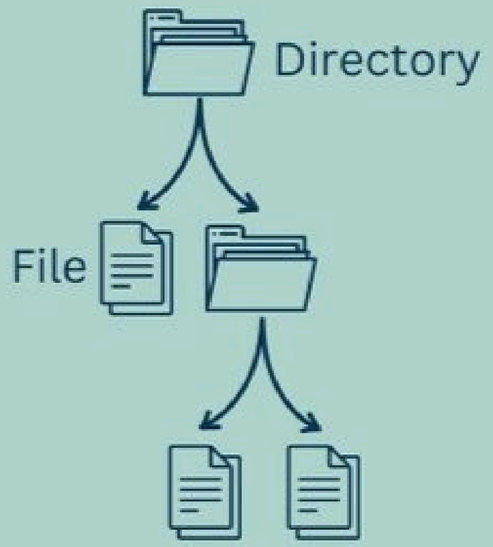
Según su contenido:

- Almacenamiento en bloques.
- Almacenamiento de objetos.
- Almacenamiento de archivos.

Se diferencian en cómo se accede a la información, la latencia ofrecida y qué tipo de aplicaciones soportan, entre otras cosas.

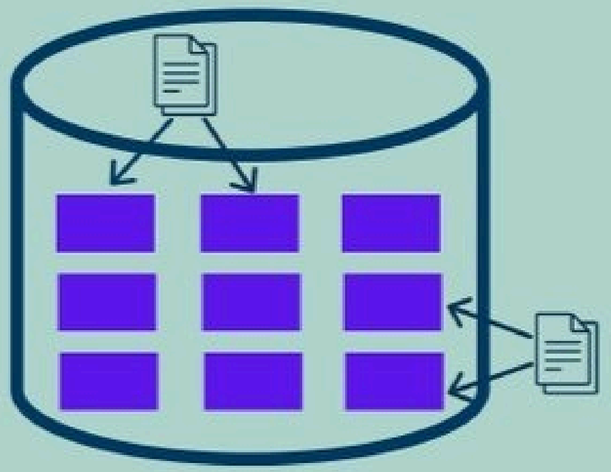
ALMACENAMIENTO

File Storage



Stores data as a hierarchy of files within directories.

Block Storage



Fixed-size of blocks at specific location on memory.

Object Storage

Flexible container size.

ALMACENAMIENTO

Elegir todo lo relacionado con el almacenamiento se trata de un **compromiso técnico**.

Esta elección se debe realizar según diversos factores como pueden ser el tipo de dato, la frecuencia con la que accedemos a esos datos, la necesidad de concurrencia, el coste...

ACTIVIDAD (PARTE 1)

Visita la documentación de AWS y nombra las principales diferencias y características de los tres tipos de almacenamiento que hemos nombrado.

A continuación, identifica qué tipo de almacenamiento utilizarías para:

- Contenido multimedia.
- Datos temporales.
- Archivos compartidos.

ACTIVIDAD (PARTE 1 Y 2)

Visita la documentación de AWS y nombra las principales diferencias y características de los tres tipos de almacenamiento que hemos nombrado.

Identifica qué tipo de almacenamiento utilizarías para:

- Contenido multimedia.
- Datos temporales.
- Archivos compartidos.

Justifica cada decisión desde el punto de vista técnico, de coste y de rendimiento.

BASES DE DATOS

Las empresas tienen diferentes opciones a la hora de administrar sus bases de datos en la nube.

Los estilos de gestión de bases de datos se pueden generalizar en cuatro categorías:

- Autogestionadas
- Automatizadas
- Gestionadas
- Autónomas

BBDD AUTOGESTIONADAS

En este modelo, una organización ejecuta su base de datos en la nube, pero gestiona la propia base de datos utilizando recursos internos y **sin que el proveedor de servicios en la nube integre ninguna automatización**.

Esto ofrece algunos de los beneficios estándar de ubicar una base de datos en la nube (incluidas una flexibilidad y agilidad mejoradas), pero la organización aún conserva la responsabilidad y el control sobre la gestión de las bases de datos.

BBDD AUTOMATIZADAS

Las empresas utilizan APIs de servicios en la nube para bases de datos a fin de colaborar con operaciones de ciclo de vida, pero mantienen el acceso a los servidores de la base de datos y controlan la configuración de las mismas y los sistemas operativos.

Los servicios de base de datos automatizados son limitados y, por lo general, no incluyen actividades planificadas, como el mantenimiento.

BBDD GESTIONADAS

Similar al de las bases de datos en la nube automatizadas, con la excepción de que el proveedor de servicios en la nube no permite que los consumidores accedan a los servidores que alojan la base de datos.

Los ajustes se limitan a las configuraciones en la nube suministradas por estos proveedores, ya que los usuarios finales **no pueden instalar su propio software**.

La BD gestionada es un ejemplo del modelo compartido.

BBDD AUTÓNOMAS

La automatización y el aprendizaje automático eliminan el trabajo humano relacionado con la gestión de la base de datos y el ajuste del rendimiento.

Algunos de los servicios son para la actividad comercial, como las operaciones sin tiempo de inactividad para tareas (previstas y no previstas) de bases de datos y ciclo de vida de servicios.

ACTIVIDAD

Compara las BBDD gestionadas y autogestionadas en los siguientes aspectos:

- Dónde se ejecuta la propia BD.
- Quién se encarga de la instalación y configuración.
- Quién se encarga del mantenimiento.
- Cómo funcionan los backups.
- Cuál es más escalable.
- Cuál supone más coste.

ACTIVIDAD

Aspecto	BD Autogestionada	BD Gestionada
Dónde se ejecuta	En una máquina virtual / en servidores on-premise	Como servicio del proveedor
Instalación y configuración	A cargo del cliente	Automatizada por el proveedor
Mantenimiento y parches	Responsabilidad del cliente	Responsabilidad del proveedor
Backups	Manuales o scripts propios	Automáticos e integrados
Escalabilidad	Manual y limitada	Más sencilla y menos limitada
Coste	Menor coste directo	Mayor coste, menos carga operativa

RESPONS. COMPARTIDA

Cuando hablamos del concepto de nube, la seguridad y el mantenimiento se reparten entre proveedor y cliente.

Como ya hemos visto, en una BD autogestionada, el cliente gestiona casi todo lo relacionado con el sistema y la BD. En una gestionada, el proveedor asume gran parte de la operación, siendo el cliente aún responsable del uso correcto y de los datos.

La nube **no elimina** la responsabilidad del cliente.

RESPONS. COMPARTIDA

Aplicar parches de seguridad del motor MySQL.

Decidir quién puede acceder a la BD.

Restaurar una copia de seguridad y hacer comprobaciones.

RESPONS. COMPARTIDA

Aplicar parches de seguridad del motor MySQL.
Autogestionada: Cliente
Gestionada: Proveedor

Decidir quién puede acceder a la BD.
Autogestionada: Cliente
Gestionada: Cliente

Restaurar una copia de seguridad y hacer comprobaciones.
Autogestionada: Cliente
Gestionada: Cliente

SEGURIDAD EN LA NUBE

Crear recursos en la nube es fácil y rápido, al igual que también lo es cometer errores.

Un error de configuración puede exponer datos, generar sobrecostes y permitir accesos no autorizados.

Muchos incidentes dentro de las empresas **no son ataques**, sino **malas configuraciones**.

SEGURIDAD EN LA NUBE

¿De qué hablamos cuando tratamos el tema de seguridad en la nube?

Se basa en:

- Acceso (qué puedes hacer).
- Protección de datos (qué se expone y qué se cifra).
- Identidad (quién eres).

La **seguridad IAM** es la clave en los servicios cloud.

SEGURIDAD EN LA NUBE

Para los servicios de las empresas en la nube, ¿cuál de los siguientes es el mayor riesgo?

- Virus o malware
- Ataques DDoS
- Permisos mal asignados
- Errores humanos

SEGURIDAD EN LA NUBE

Para los servicios de las empresas en la nube, ¿cuál de los siguientes es el mayor riesgo?

- Virus o malware
- Ataques DDoS
- Permisos mal asignados
- Errores humanos

Los errores humanos y los permisos mal asignados son los mayores riesgos en estos servicios. Pueden provocar filtraciones de datos, infracciones normativas y pérdidas.

GESTIÓN DE PERMISOS

Los aspectos esenciales para una gestión eficaz de los permisos son:

- **Principio de privilegio mínimo**, ofreciendo a los usuarios solo el acceso que necesitan.
- **Modelos de acceso**, ya sea basado en roles o basado en atributos.
- **Autenticación multifactor**.
- **Auditorías periódicas**, identificando permisos no utilizados o excesivos para evitar vulnerabilidades.
- **Herramientas de automatización** que simplifiquen la gestión de permisos a escala.

GESTIÓN DE PERMISOS

El principio del privilegio mínimo trata de otorgar a los usuarios el acceso **justo** para realizar su trabajo.

Este principio ayuda a reducir la superficie de ataque si una cuenta de usuario se ve comprometida.

Además, reduce riesgos de seguridad interna al reducir las posibilidades de uso indebido accidental o intencional.

ACTIVIDAD

Encuentra el significado de las siglas RBAC y ABAC cuando hablamos de permisos en la nube.

Defínelos y enumera diversas similitudes y diferencias en cuanto a, por ejemplo, mantenimiento, escalabilidad y complejidad.

GESTIÓN DE PERMISOS

Para implementar el principio de privilegio mínimo se necesita un modelo de control de acceso adecuado.

Aquí entran el control de acceso basado en roles (**RBAC**) y control de acceso basado en atributos (**ABAC**).

RBAC agrupa los permisos en roles predefinidos y los usuarios heredan los permisos según su rol asignado.

ABAC determina el acceso según atributos, como la hora del día, la ubicación o el tipo de dispositivo utilizado.

Aspecto	RBAC	ABAC
Complejidad	Simple y directo	Más complejo pero muy adaptable
Mejor para	Organizaciones estables con roles claros	Entornos con necesidades de acceso cambiantes
Escalabilidad	Puede resultar difícil de gestionar con demasiados roles.	Maneja la complejidad de manera más efectiva
Mantenimiento	Más fácil de mantener en configuraciones estables	Requiere ajustes continuos de política
Granularidad	Limitado a permisos basados en roles	Ofrece un control preciso y sensible al contexto.

IAM EN ENTORNOS REALES

En los entornos reales en la nube existen muchos equipos, usuarios, proyectos y entornos. Gestionar y revisar los permisos suele ser complejo.

La mayoría de errores vienen por no saber gestionar el crecimiento:

- Acumulación de permisos
- Cuentas que nadie usa pero siguen existiendo
- Permisos temporales que se vuelven permanentes

IAM EN ENTORNOS REALES

La gestión de identidades y accesos (IAM) no es solo para las personas. Los servicios también se comunican entre sí.

Una aplicación con demasiados permisos es un riesgo de seguridad, así como lo es utilizar credenciales de usuario para acceder a las mismas.

Las aplicaciones deberían usar roles y no usuarios con contraseña. Las credenciales robadas son el principal vector inicial de ataque.

IAM EN ENTORNOS REALES

Unos permisos mal asignados pueden permitir sobrecostes.

ERRORES HUMANOS

El factor más crítico.

Dejar los activos en la nube sin protección, hacer click en un enlace de phising...

La mejor forma de combatir el riesgo de error humano no es solo mediante IAM, sino también mediante la adopción de una **formación periódica**.