



GOBIERNO DE LA CIUDAD DE BUENOS AIRES

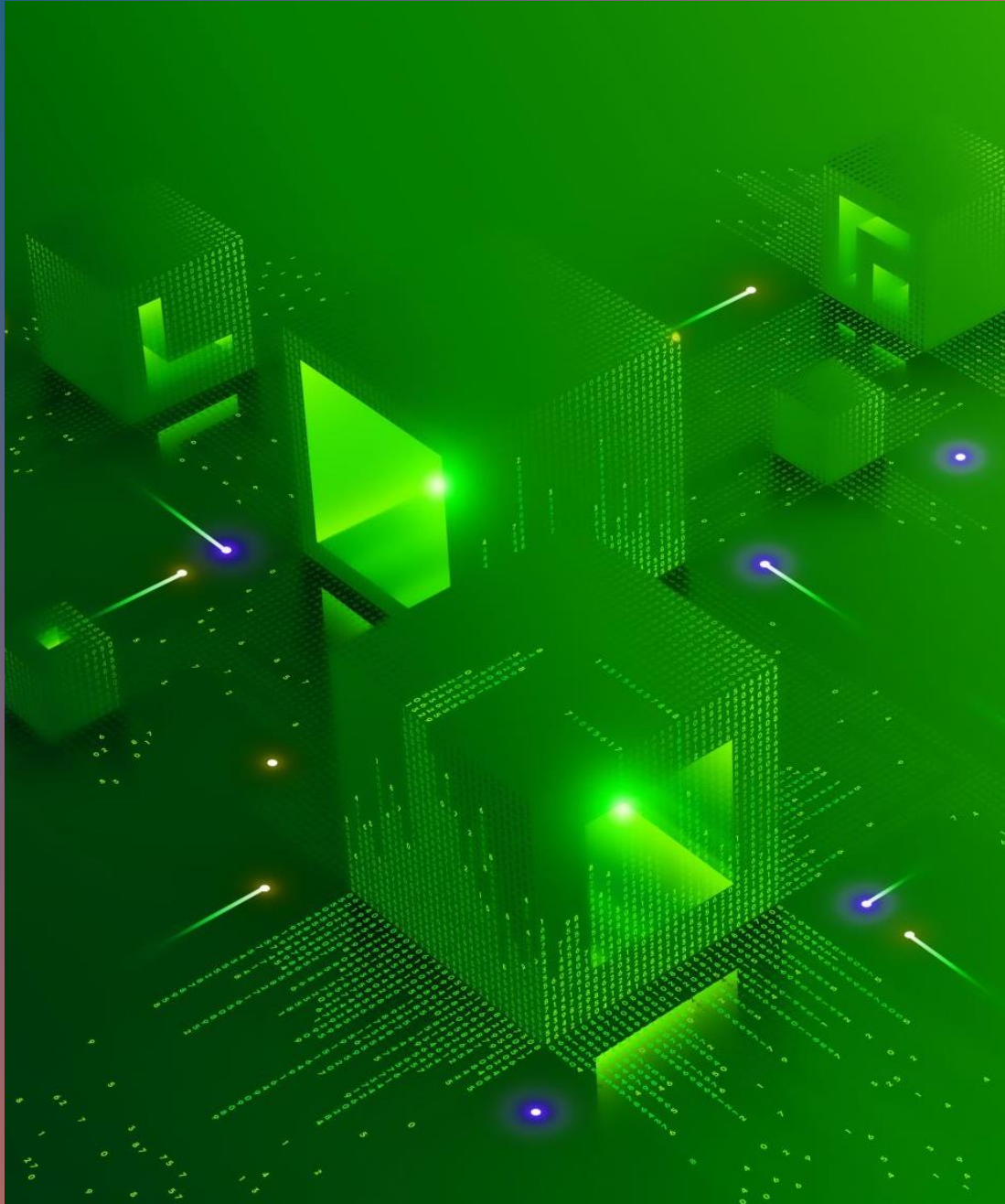
Ministerio de Educación

Dirección de Formación Técnico Superior

Instituto de Formación Técnico Superior N° 18

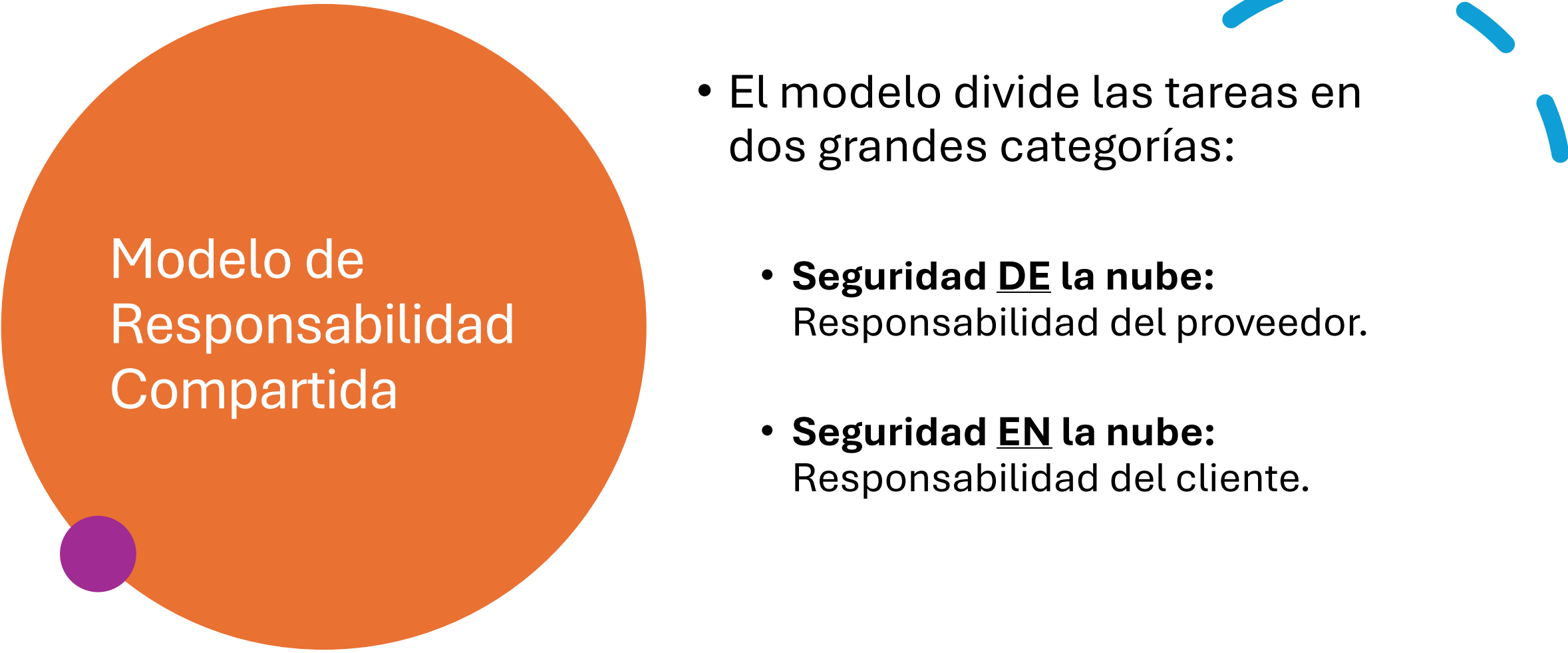
Mansilla 3643, (C1425BBW) Capital Federal

Arquitectura de sistemas en la Nube



- **Temas:**

- **Modelo de Responsabilidad Compartida**
- **Gestión de Identidad y Acceso (IAM)**
- **Seguridad de los Datos**
- **Matriz de Responsabilidades**



Modelo de Responsabilidad Compartida

- El modelo divide las tareas en dos grandes categorías:
 - **Seguridad DE la nube:**
Responsabilidad del proveedor.
 - **Seguridad EN la nube:**
Responsabilidad del cliente.

Alcance del Proveedor

- El proveedor se encarga de proteger la infraestructura global que ejecuta todos los servicios ofrecidos.
- Esto incluye:
 - **Infraestructura Física:** Seguridad de los centros de datos (guardias, cámaras, controles de acceso biométricos).
 - **Hardware:** Mantenimiento y sustitución de servidores, sistemas de almacenamiento y racks.
 - **Software de Virtualización:** La capa de abstracción (hypervisor) que permite que varios clientes compartan el mismo hardware físico de forma aislada.
 - **Red Global:** El cableado transoceánico, los puntos de presencia (Edge locations) y la conectividad entre regiones.



Alcance del Cliente

- El Cliente es responsable de lo que hay dentro de la infraestructura.
 - **Datos del Cliente:** Cifrado de datos (en reposo y en tránsito) y gestión de copias de seguridad.
 - **Gestión de Identidades y Accesos (IAM):** Quién tiene permiso para entrar a tu consola y qué pueden hacer.
 - **Configuración del Firewall:** Configuración de grupos de seguridad y listas de control de acceso a la red (NACLs).
 - **Sistema Operativo y Parches:** En modelos como IaaS, tú decides cuándo actualizar Windows o Linux.



La Responsabilidad según el Modelo de Servicio

Capa de Responsabilidad	On-Premise	IaaS (EC2, Azure VM)	PaaS (Lambda, App Service)	SaaS (Microsoft 365, Salesforce)
Datos y Contenido	Cliente	Cliente	Cliente	Cliente
Aplicación	Cliente	Cliente	Cliente	Proveedor
Runtime / S.O.	Cliente	Cliente	Proveedor	Proveedor
Virtualización	Cliente	Proveedor	Proveedor	Proveedor
Hardware / Red	Cliente	Proveedor	Proveedor	Proveedor



Ejemplos

- **En una máquina virtual**
- **Proveedor:** Garantiza que el servidor físico funcione y que la red llegue a la instancia.
- **Cliente:** Si deja el puerto 22 (SSH) abierto a todo el mundo y lo hackean, **es su responsabilidad**. El proveedor dio las herramientas para cerrarlo, pero no lo hizo.

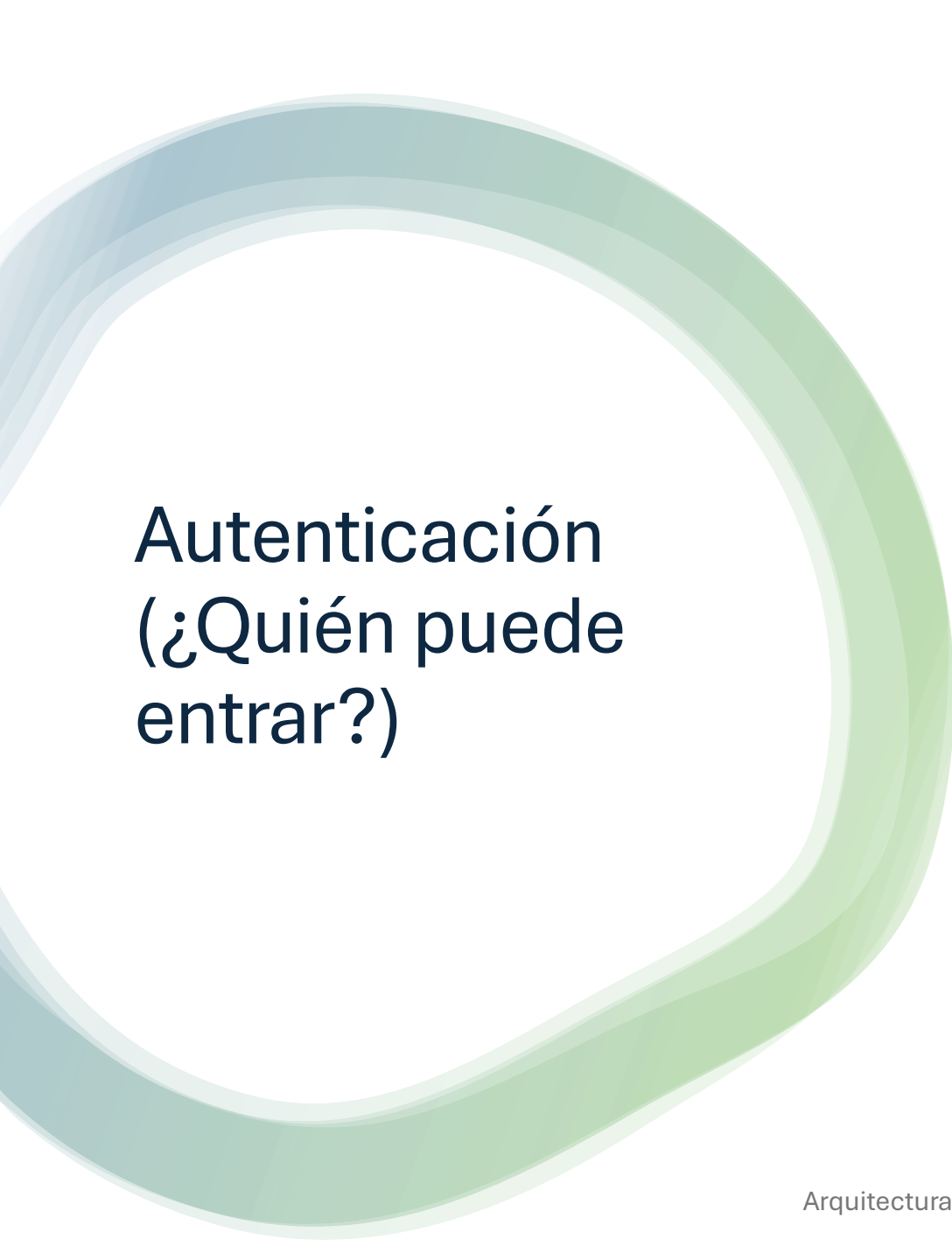
- **En una función sin servidor (PaaS / Serverless)**
 - **Proveedor:** Se encarga de actualizar el sistema operativo subyacente y de escalar el servidor según la demanda.
 - **Cliente:** Es responsable de que el **código** que escribio no tenga vulnerabilidades y de configurar correctamente quién puede invocar esa función.

- **Almacenamiento de Objetos (S3 / Blob Storage)**
- **Proveedor:** Asegura que los discos no fallen y que los datos no se pierdan físicamente (durabilidad).
- **Cliente:** Debe configurar el "bucket" como privado. Si el cliente lo pone "Público" por error y se filtran fotos confidenciales, el fallo es de configuración del cliente.



Gestión de Identidad y Acceso (IAM)

- esta función recae exclusivamente bajo la responsabilidad del cliente en todos los modelos de servicio (IaaS, PaaS y SaaS).
- el alcance de IAM basado en los conceptos de autenticación y autorización:
 - Autenticación
 - Autorización
 - Responsabilidad del Cliente en IAM



Autenticación (¿Quién puede entrar?)

- La autenticación se refiere al proceso de controlar quién tiene permiso para entrar a la consola de administración o a los recursos de la infraestructura.
- En el modelo de responsabilidad compartida, el cliente es el encargado de definir y gestionar estas identidades.
- Esto aplica incluso en servicios altamente administrados como **SaaS**, donde el cliente mantiene el control sobre quién accede a la aplicación y a los datos.

Autorización (¿Qué pueden hacer?)

- Una vez que una identidad ha sido autenticada, la autorización determina qué acciones específicas tiene permitido realizar y qué permisos posee.
 - **Configuración de permisos:** El cliente debe establecer qué puede hacer cada usuario o servicio dentro de la plataforma.
 - **Ejemplo en PaaS (Serverless):** El cliente es responsable de configurar correctamente quién o qué servicio tiene la capacidad de invocar una función específica (como AWS Lambda).
 - **Ejemplo en Almacenamiento:** Es responsabilidad del cliente configurar el acceso a los datos (por ejemplo, decidir si un "bucket" de almacenamiento es público o privado).

Responsabilidad del Cliente en IAM

- Independientemente de si se utiliza infraestructura básica o software como servicio, la gestión de accesos es una tarea crítica del usuario:
 - **Control Total:** El proveedor de la nube nunca supervisa los datos del cliente ni sus configuraciones de acceso para verificar si son seguras; esa tarea le corresponde íntegramente al cliente.
 - **Riesgos de Configuración:** Si un cliente deja accesos abiertos por error (como un puerto SSH o un almacenamiento público), las consecuencias de un posible ataque son su responsabilidad, ya que el proveedor solo entrega las herramientas para cerrar dichos accesos, pero no las ejecuta por el cliente.

Identidad

- una **identidad** se refiere al "quién" solicita acceso a los recursos de la nube. No se limita únicamente a personas físicas, sino que abarca cualquier entidad que necesite interactuar con la infraestructura.
- Bajo el modelo de responsabilidad compartida, el cliente es el único encargado de definir y gestionar estas identidades, que generalmente se dividen en dos grupos:
 - Usuarios Humanos
 - Servicios o Máquinas

Usuarios Humanos

- Son las personas que necesitan acceder a la consola de administración o a las aplicaciones para trabajar.
- **Ejemplo:** Un administrador de sistemas que entra a configurar un servidor o un desarrollador que sube código.

Servicios o Máquinas

- Son entidades no humanas, como aplicaciones, funciones o servicios automáticos, que requieren permisos para realizar tareas específicas dentro de la plataforma.
- **Ejemplo en PaaS:** Un servicio o aplicación que necesita tener la capacidad de invocar una función específica, como AWS Lambda.

Aspectos clave sobre la identidad en la nube:

- **Identificación única:** Cada identidad permite controlar de manera individual quién tiene permiso para entrar a la consola y qué acciones específicas puede realizar.
- **Responsabilidad absoluta:** El cliente es responsable de estas identidades en todos los modelos (IaaS, PaaS, SaaS). El proveedor nunca supervisa ni verifica si las configuraciones de acceso de estas identidades son seguras.
- **Propiedad:** El cliente es el dueño y responsable único de decidir quién accede a sus datos.



Seguridad de los Datos

- Independientemente del Tipo de servicio contratado (IaaS, PaaS o SaaS), El cliente es el dueño y responsable único de proteger la información. El proveedor jamás revisará los datos para ver si están protegidos; esa es una tarea que le corresponde íntegramente al cliente.

1 - Cifrado de Datos

- Se debe gestionar el cifrado para asegurar la confidencialidad de la información.
 - Cifrado en Reposo (At Rest)
 - Cifrado en Tránsito (In Transit)



Cifrado en Reposo (At Rest)

- Se refiere a proteger los datos mientras están guardados en discos, bases de datos o sistemas de almacenamiento.
- Se debe decidir qué algoritmos de cifrado usar y gestionar las claves de acceso.
- **Ejemplo en Almacenamiento (S3/Blob):** Aunque el proveedor asegura que el disco físico no falle, se debe configurar el "bucket" para que los objetos se cifren antes de escribirse en el disco.



Cifrado en Tránsito (In Transit)

- Se refiere a proteger los datos mientras viajan por la red, ya sea entre el usuario y la nube o entre diferentes servicios internos.
- Implementar protocolos seguros (como HTTPS/TLS) para que, si alguien intercepta el tráfico, no pueda leer el contenido.
- **Ejemplo en Redes:** Configurar correctamente los grupos de seguridad y firewalls para permitir solo conexiones cifradas.



2 - Gestión de Copias de Seguridad (Backups)

- No basta con cifrar; la disponibilidad también es parte de la seguridad de los datos.
- El cliente es responsable de definir las políticas de respaldo y la frecuencia de las copias de seguridad.
- Si se borra accidentalmente una base de datos o se sufre un ataque de ransomware que cifra los archivos, el proveedor no es responsable de recuperar esa información.

3 - Normativas de Cumplimiento(Compliance)

- El cumplimiento es un esfuerzo compartido donde se dividen las certificaciones:
- **Alcance del Proveedor:** Se encarga del cumplimiento de la **infraestructura física** y el **hardware**. Ellos obtienen certificaciones (como ISO 27001 o PCI-DSS) para sus centros de datos y la capa de virtualización.
- **Alcance del Cliente:** Es responsable de que el uso que le da a los datos cumpla con las leyes locales o de industria (como GDPR para privacidad o HIPAA para salud).
 - **Ejemplo:** El proveedor puede tener un centro de datos certificado, pero si se guardan números de tarjetas de crédito sin cifrar y sin control de acceso, el cliente esta incumpliendo la normativa.

Resumen de Roles en Seguridad de Datos

Concepto	Responsabilidad del Proveedor	Responsabilidad del Cliente
Cifrado	Ofrecer herramientas y hardware de seguridad.	Aplicar el cifrado en reposo y en tránsito.
Backups	Durabilidad física de los discos.	Configurar y probar los respaldos.
Privacidad	Aislamiento físico y lógico de clientes.	Configurar quién accede a qué (IAM).

Ejemplo



Amazon S3 (Object Storage)



Base de Datos (IaaS o PaaS)

Amazon S3 (Object Storage)

- En este servicio, la línea de responsabilidad entre lo que hace el proveedor y el cliente es muy clara:
- **Lo que hace el proveedor (Seguridad DE la nube):**
 - Garantiza la **durabilidad física**: asegura que los discos donde se guardan los archivos no fallen y que los datos no se pierdan por un problema de hardware.
 - Mantiene el aislamiento lógico para que otros clientes no puedan ver todas las carpetas de otros clientes(buckets).
 - Ofrece las **herramientas de cifrado** (como KMS).
- **Lo que hace el cliente (Seguridad EN la nube):**
 - **Cifrado en Reposo**: Debe entrar a la configuración del "bucket" y activar el cifrado para que cada archivo se encripte antes de tocar el disco físico. Decide si usa claves gestionadas por el proveedor o si gestiona sus propias claves de acceso.
 - **Cifrado en Tránsito**: Se debe configurar políticas que obliguen a usar **HTTPS/TLS**; conexiones por HTTP (sin cifrar) hay riesgo de interceptación
 - **Privacidad**: Se debe configurar el bucket como **privado**. Si se deja "Público" se filtran datos.

Base de Datos (IaaS o PaaS)

- Aquí la responsabilidad varía según se instala una base de datos (IaaS) o se usa un servicio administrado (PaaS):
- **Protección de Datos Sensibles:**
 - Aunque el centro de datos del proveedor tenga certificaciones de seguridad (como ISO o PCI-DSS), si se guardan datos críticos como **números de tarjetas de crédito** sin cifrarlos dentro de la tabla, el cliente es quien incumple la normativa.
 - El cliente es responsable de aplicar el **mínimo privilegio** mediante IAM para que solo las aplicaciones autorizadas lean esos datos.
- **Disponibilidad y Backups:**
 - El proveedor da la herramienta para hacer copias de seguridad, pero el cliente **define la frecuencia** y las políticas de respaldo.
 - Si hay un ataque de **ransomware** que cifra tus tablas o se borra la base de datos por error, el proveedor no podrá recuperar tu información si no se configuro los backups correctamente.

Acción de Seguridad	¿Quién la ejecuta?	Herramienta/Concepto
Garantizar que el disco no se rompa	Proveedor	Mantenimiento de Hardware
Activar el candado en el bucket (S3)	Cliente	Configuración de Cifrado
Decidir quién puede leer la DB	Cliente	Gestión de IAM
Cumplir con leyes de privacidad (GDPR)	Cliente	Uso responsable y cifrado



Matriz de Responsabilidades (RACI)

- Es una herramienta para asignar funciones claras entre proveedor y cliente. Se puede usar el modelo RACI (Responsable, Aprobador, Consultado, Informado).

Dinámica de la Matriz según el Servicio

- La matriz no es estática; la responsabilidad es dinámica y se desplaza dependiendo de qué tan administrado sea el servicio que se contrate. A continuación, se detalla cómo se distribuyen las tareas en los modelos principales:

Capa de Responsabilidad	IaaS (Ej: EC2)	PaaS (Ej: Lambda)	SaaS (Ej: Salesforce)
Datos y Contenido	Cliente	Cliente	Cliente
Aplicación	Cliente	Cliente	Proveedor
Runtime / S.O.	Cliente	Proveedor	Proveedor
Virtualización	Proveedor	Proveedor	Proveedor
Hardware y Red	Proveedor	Proveedor	Proveedor

Matriz RACI: Caso SaaS (Software as a Service)

Capa / Actividad	Cliente	Proveedor	Descripción de la Tarea
Datos y Contenido	R/A		El cliente es el único responsable de la seguridad de su información.
Gestión de Accesos (IAM)	R/A		Controlar quién entra a la aplicación y qué permisos tiene asignados.
Aplicación		R/A	Mantener el software libre de errores y actualizar sus funciones operativas.
Runtime / S.O.		R/A	Gestión de parches del sistema operativo y ejecución técnica del software.
Infraestructura Física		R/A	Seguridad de los centros de datos, mantenimiento de hardware y red global.

Matriz RACI: Caso PaaS (Platform as a Service)

Capa / Actividad	Cliente	Proveedor	Descripción de la Tarea
Datos y Contenido	R/A		Cifrado de los datos y gestión de las copias de seguridad (backups).
Aplicación (Código)	R/A		Asegurar que el código escrito por el desarrollador no tenga vulnerabilidades.
Configuración de Acceso	R/A		Configurar correctamente qué servicios o personas pueden invocar las funciones.
Runtime / S.O.		R/A	Actualizar el sistema operativo subyacente y el entorno de ejecución del código.
Escalabilidad y Hardware		R/A	Escalar los servidores según la demanda y mantener toda la infraestructura física.

- 
- **R - Responsable (Responsible):** Es quien ejecuta la tarea. Es la entidad (cliente o proveedor) que realiza el trabajo para completar la actividad específica.
 - **A - Rendidor de Cuentas (Accountable):** Es el responsable último de que la tarea se complete correctamente. Es quien "es el dueño" del resultado y debe asegurar que se cumplan los estándares.

Componente	Proveedor	TI	Negocio	Seguridad
Software	R	-	-	C
Infraestructura	R	-	-	C
Usuarios y Roles	-	R	R	C/I
Cumplimiento	C	C	C	R

- * R : Responsable
- * A : Aprobador
- * C : Consultado
- * I : Informado