TP4 Arquitectura web

Integrantes:

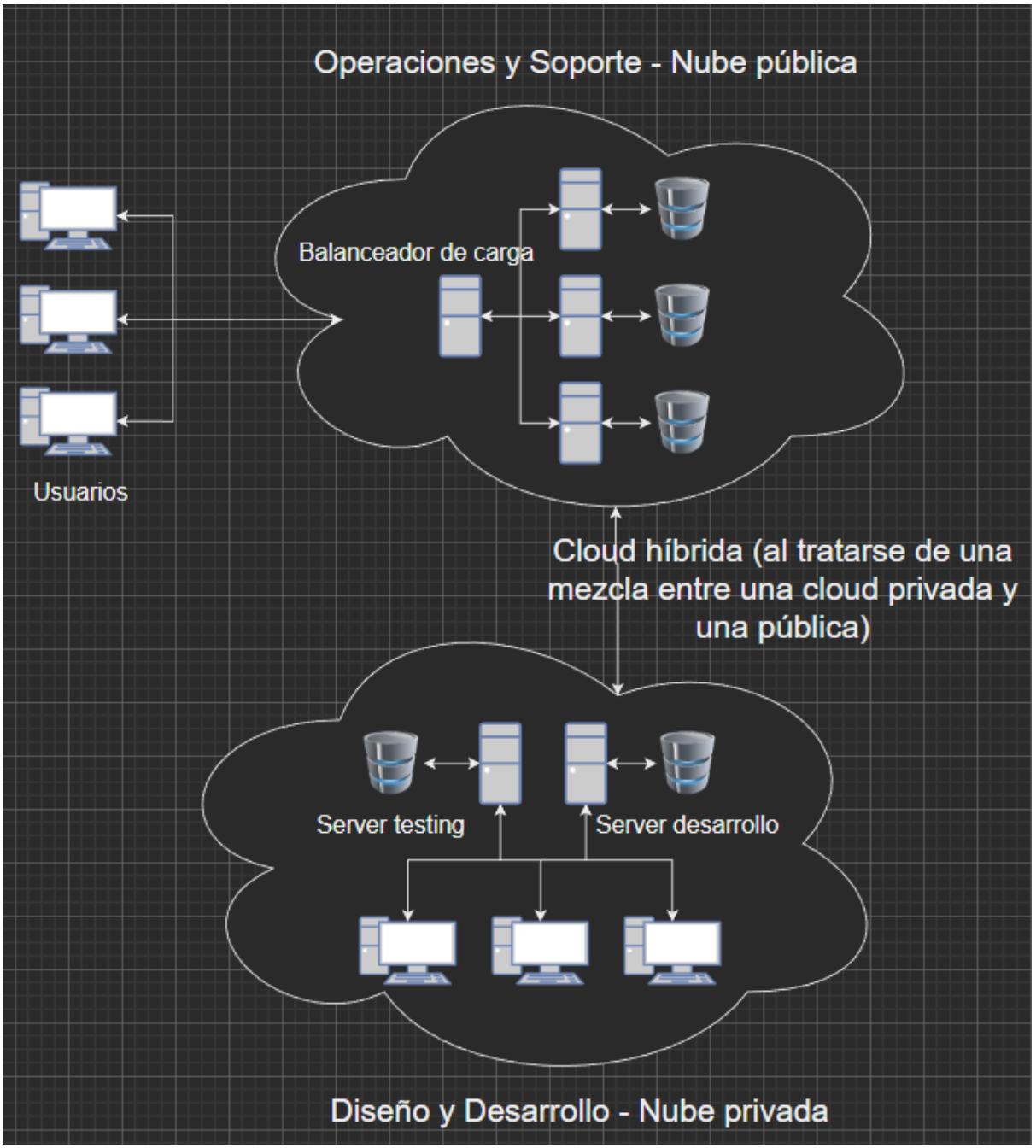
- Ezequiel Cinalli
- Micaela Cisneros
- German De Francesco
- Andrea Gherbi
- Lucas Guerrero

2)

Operaciones y soporte utilizaría una **cloud pública**, ya que sus recursos están disponibles a los usuarios que se encuentran fuera del firewall de la empresa. En este caso ya están utilizando un balanceador de carga para redireccionar el tráfico de los requests en los servidores de juego disponibles. Esto se seguiría manteniendo al migrar, pero con la posibilidad de generar más o menos instancias de servidores según la demanda.

Diseño y desarrollo utilizaría una **cloud privada**, ya que sus servidores no deberían estar disponibles al público en general, sino a dicho sector de la empresa. Para poder conectarse, tienen que hacerlo desde la misma red donde están alojados on-premise o utilizando una vpn para, a través de un túnel virtual, simular estar dentro de la misma red. Es decir, seguirían estando montados sobre su propio hardware pero es más eficiente para administrar/escalar sus recursos. Se puede escalar tanto como el hardware que tengan.

Es decir, estaríamos utilizando una **cloud híbrida**, una mezcla de cloud privada para las cosas que necesitan mayor seguridad y pública para otras que no tanto, quedando esos mundos unidos.



3)

Análisis de costos para el ambiente de Operaciones y Soporte.

Costos de servidores anual (solo hardware)

	Servidores Alquilados de una Cloud Pública	**Servidores On-Premise Alquilados**
CPU	Procesador 3 x 2 GHz	Procesador 3 x 2 GHz
Memoria	32 GB	32 GB
Almacenamiento	50 TB	50 TB
Costo por servidor	$0,50 la hora	$299 al mes
Cantidad de servidores	512	859
Costo total por año	**$2.242.560**	**$3.082.092**

Costos cloud pública vs on-premise (completo)

	Cloud pública (512 servidores)	On-premise (859 servidores)
Up-front costs (una vez)	**$**12.885	**$119.873,45**
Compra de hardware	$0	$0
Compra de software	$0	$111.120,24 ($129,36 por servidor)
Mano de obra	$12.885 ($15 por servidor)	$8.753,21 ($10,19 por servidor)
Ongoing costs (mensual)	**$236.803,08**	**$296.841**
Uso de hardware	$184.320 ($0,50 la hora por servidor)	$256.841 ($299 por servidor)
Uso de ancho de banda	$39.598,08 ($77,34 por mes por servidor)	$0
Costo de administración	$12.885 ($15 por mes por servidor)	$40.000 ($80.000 x 6 empleados por año)
Costo de seguro	$0	$0
Sunk cost	**$0**	**$0**
Integration cost	**$5.000**	**$0**

En base a los datos de las tablas resumimos que para mantener el funcionamiento On-Premise se necesitaría:

- Un capital inicial de **$119.873,45**
- Mensualmente se necesitan **$296.841**
- El desembolso total para el funcionamiento de un año sería de **$3.681.965,45**

Para mantener el funcionamiento en una Cloud pública se se necesitaría:

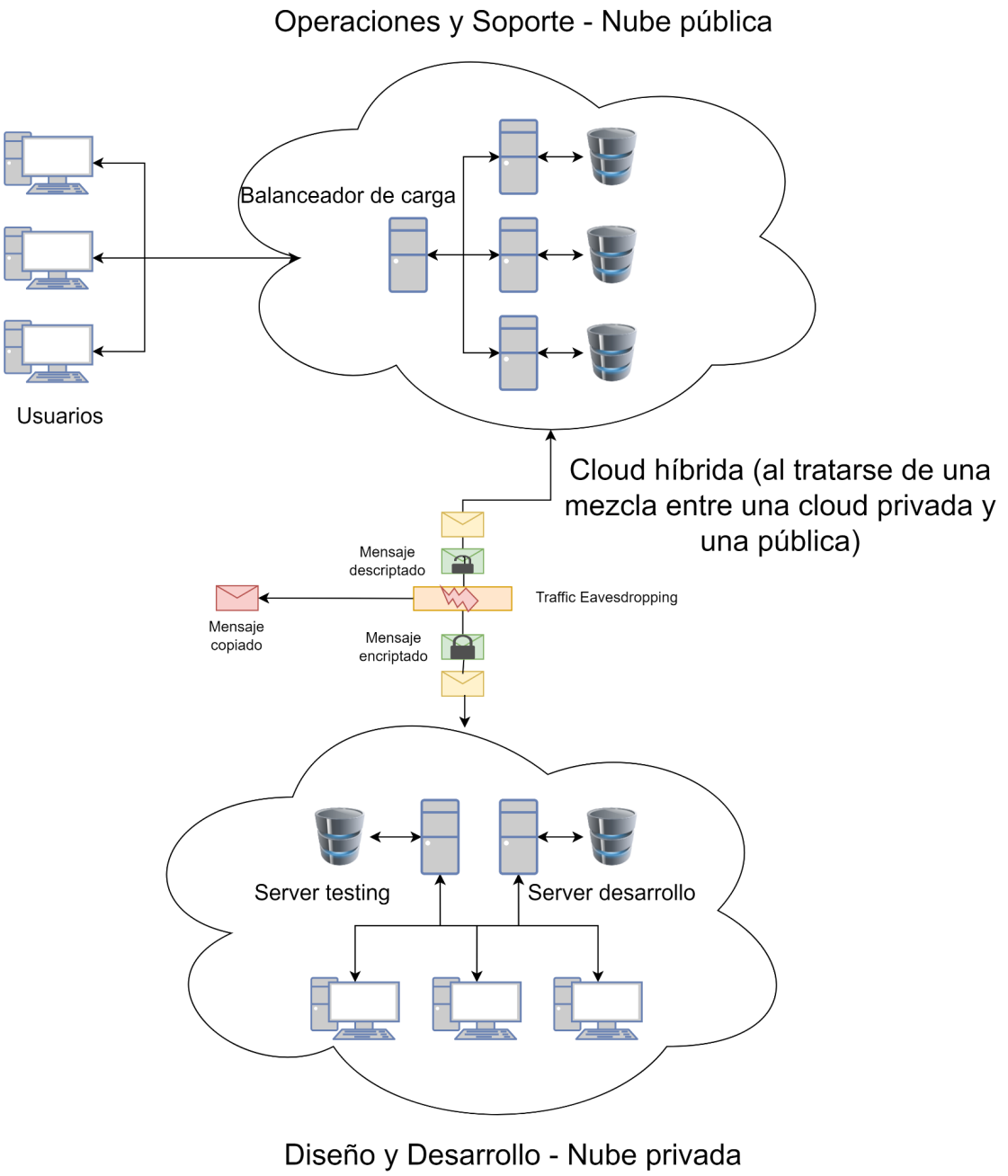
- Un capital inicial de **$17.885**
- Mensualmente se necesitan **$236.803,08**
- El desembolso total para el funcionamiento de un año sería de **$2.859.521,96**

Nuestra recomendación es migrar a la cloud pública debido al análisis del costo favorable, tanto del capital inicial inferior como del valor mensual. Además con cloud ganamos beneficios extras como alta disponibilidad, confiabilidad, performance, escalabilidad.

4)

- *Habrá un riesgo de intercambio de información sensible entre el ambiente on-premise de AGC y la cloud pública, como así también entre los servidores que se encontraran en el cloud.*

La primera amenaza hace referencia a **Traffic Eavesdropping**: esto es hacer sniffing, escuchar, interceptar (a veces además de escuchar, copia cosas). Es difícil de detectar porque no está rompiendo nada, sólo escuchando. Puede ser para robar o para recolectar datos para atacar posteriormente.

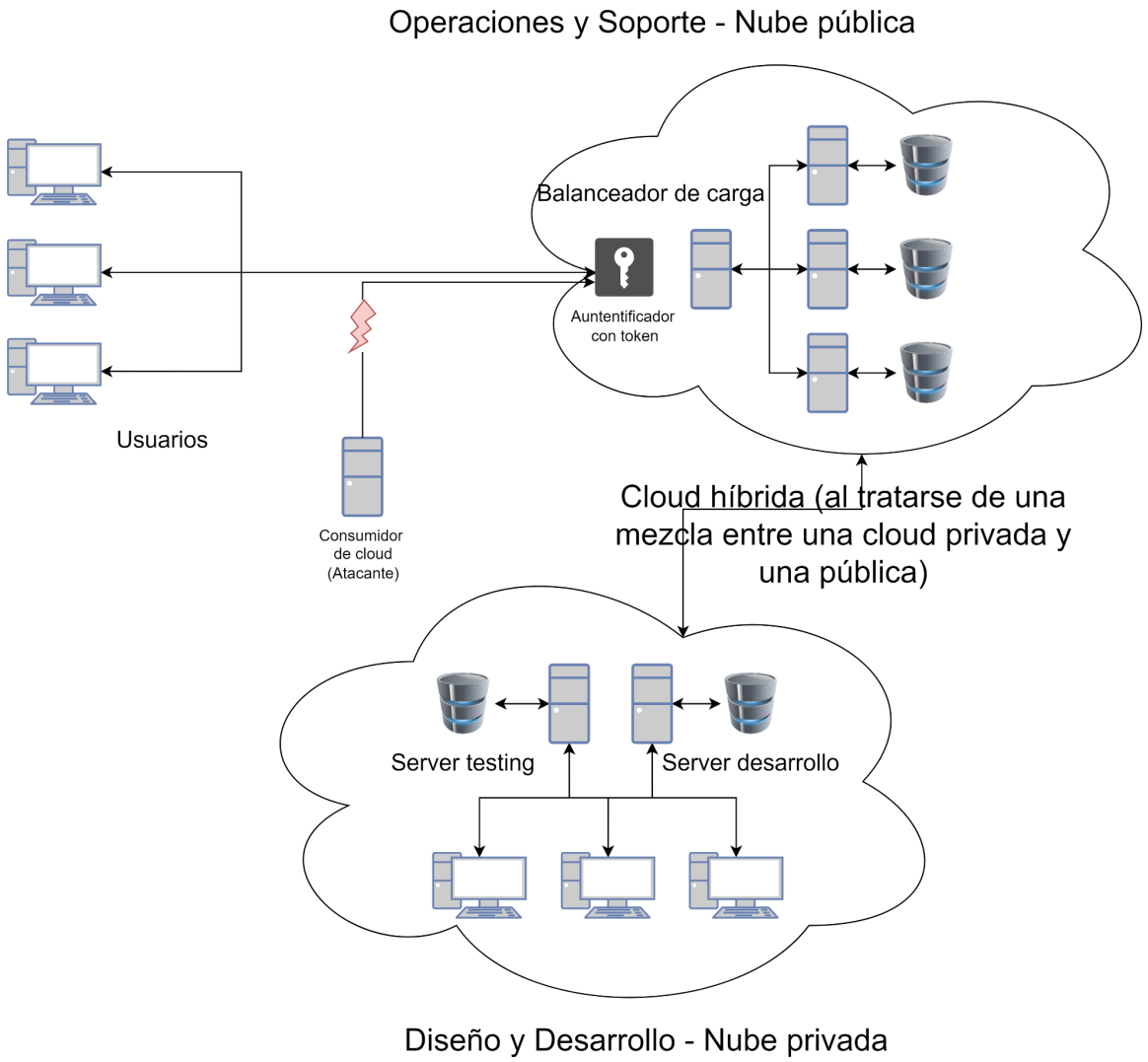


Posibles estrategias: encriptación, firma digital, infraestructura de clave pública.

- *Habrá un riesgo de que los “atacantes” ganen acceso no autorizado a los servidores con hosting en el cloud.*

La segunda amenaza hace referencia a **Autorización Insuficiente**: cualquier mecanismo que tenga que ver con

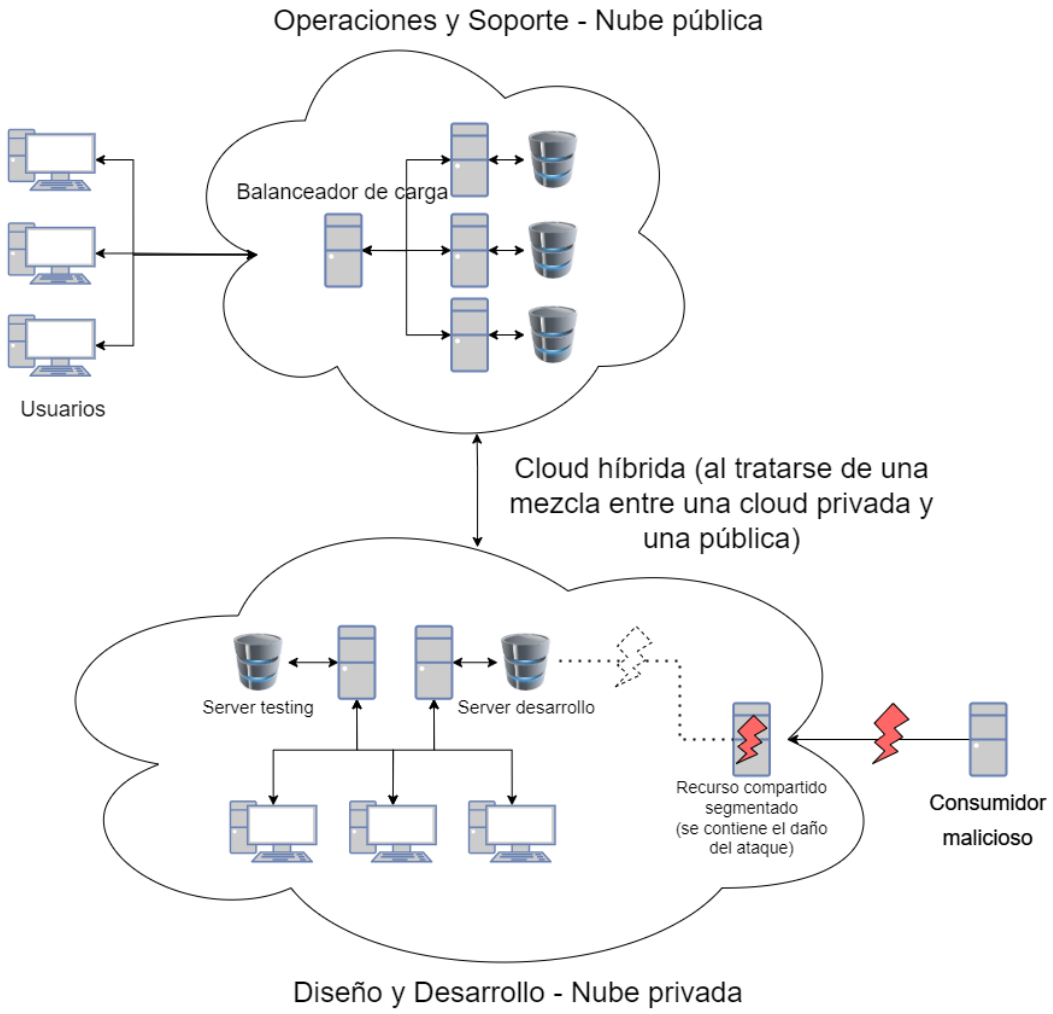
robar passwords o usuarios que tendrían que estar protegidos pero se dejaron las credenciales por defecto o no muy seguras.



Posibles soluciones: autenticación con token, que se tenga que regenerar.

- *Habrá un riesgo debido a que otros consumidores de cloud services de otras organizaciones que son consumidores del cloud compartirán los mismos recursos físicos que AGC en el cloud.*

La última amenaza hace referencia a **Superposición de Límites de Confianza**: se produce cuando el mismo recurso físico es compartido por diferentes consumidores. Un consumidor malicioso puede comprometer el recurso y a otros consumidores que comparten ese recurso.



Posible solución: segmentar/separar esos recursos para limitar el daño que pueda provocar el atacante.