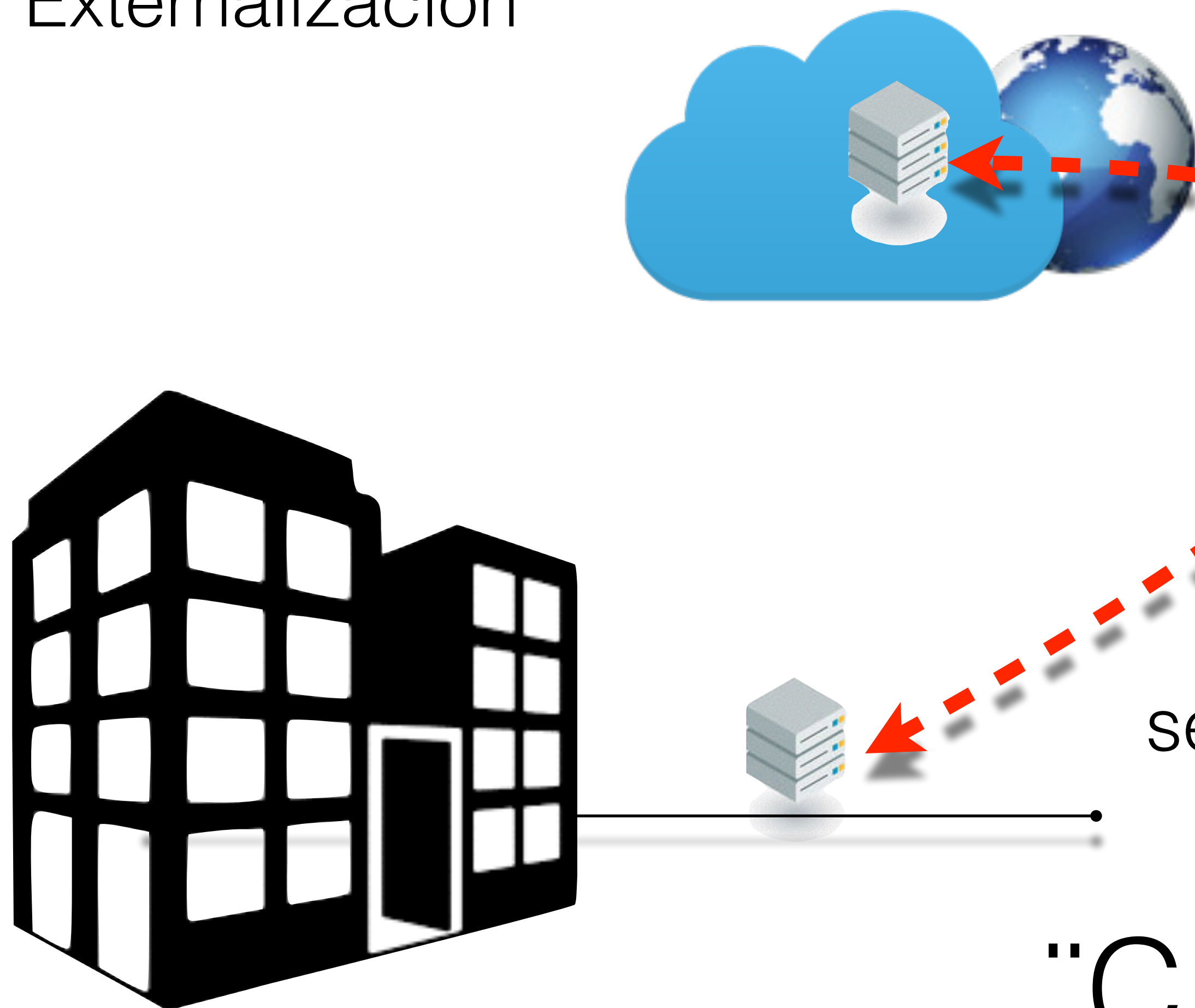


Pedro Xabier Alaña





pedroxabi  **sarenet** 

Dpto. comercial

0 Externalización



Los motivos están claros:

- Soporte 
- Focalización en el negocio 
- Envejecimiento de la infraestructura 
- Flexibilidad 

¿ Qué criterios sigo para elegir la empresa que albergue mis servidores ?

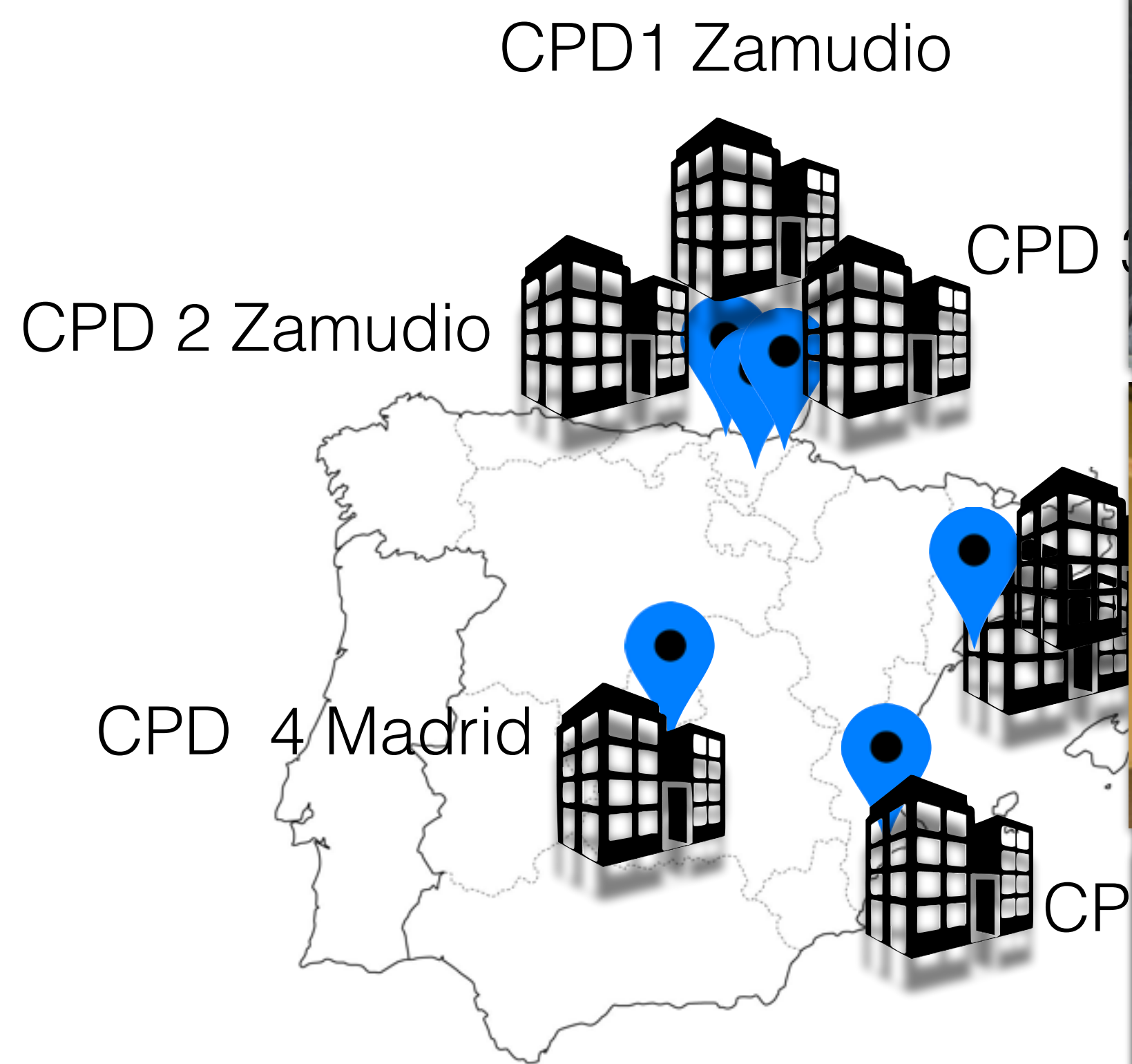
“Cloud de proximidad”



- Dónde alojaremos tus datos y cómo es un DC
- Cómo garantizamos energía y frío a los servidores
- Cómo es un nodo de la nube
- Cómo están conectados los centros de datos
- Cómo puedes conectarte a los centros de datos

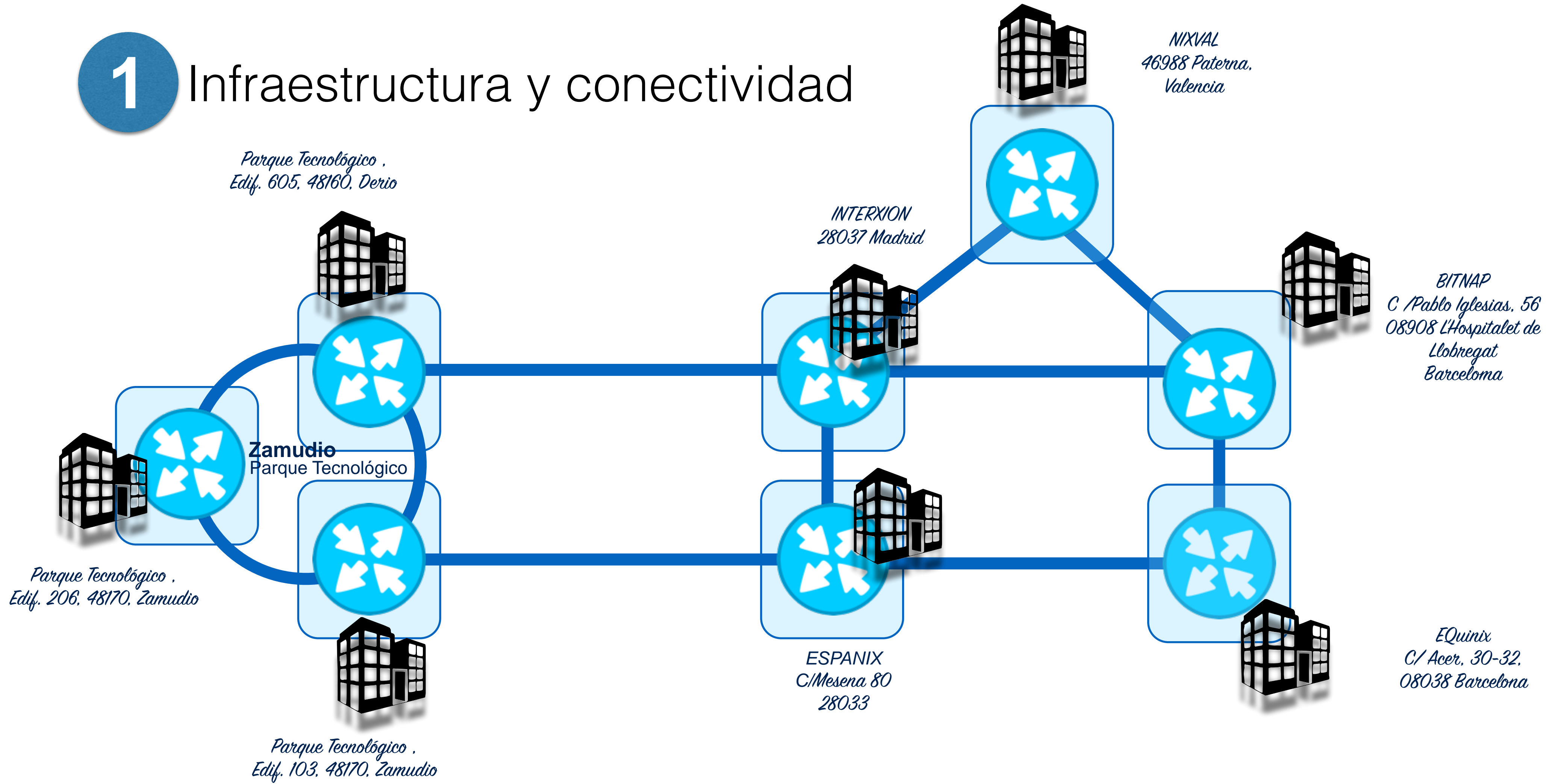
Infraestructura

1 Infraestructura y conectividad



INTELEON (Zamudio, Spain)
CPD Zamudio 1 P88,
Plano Tecnológico, Edificio 3
39.519745, -0.466933 }
40000 m² de superficie
España

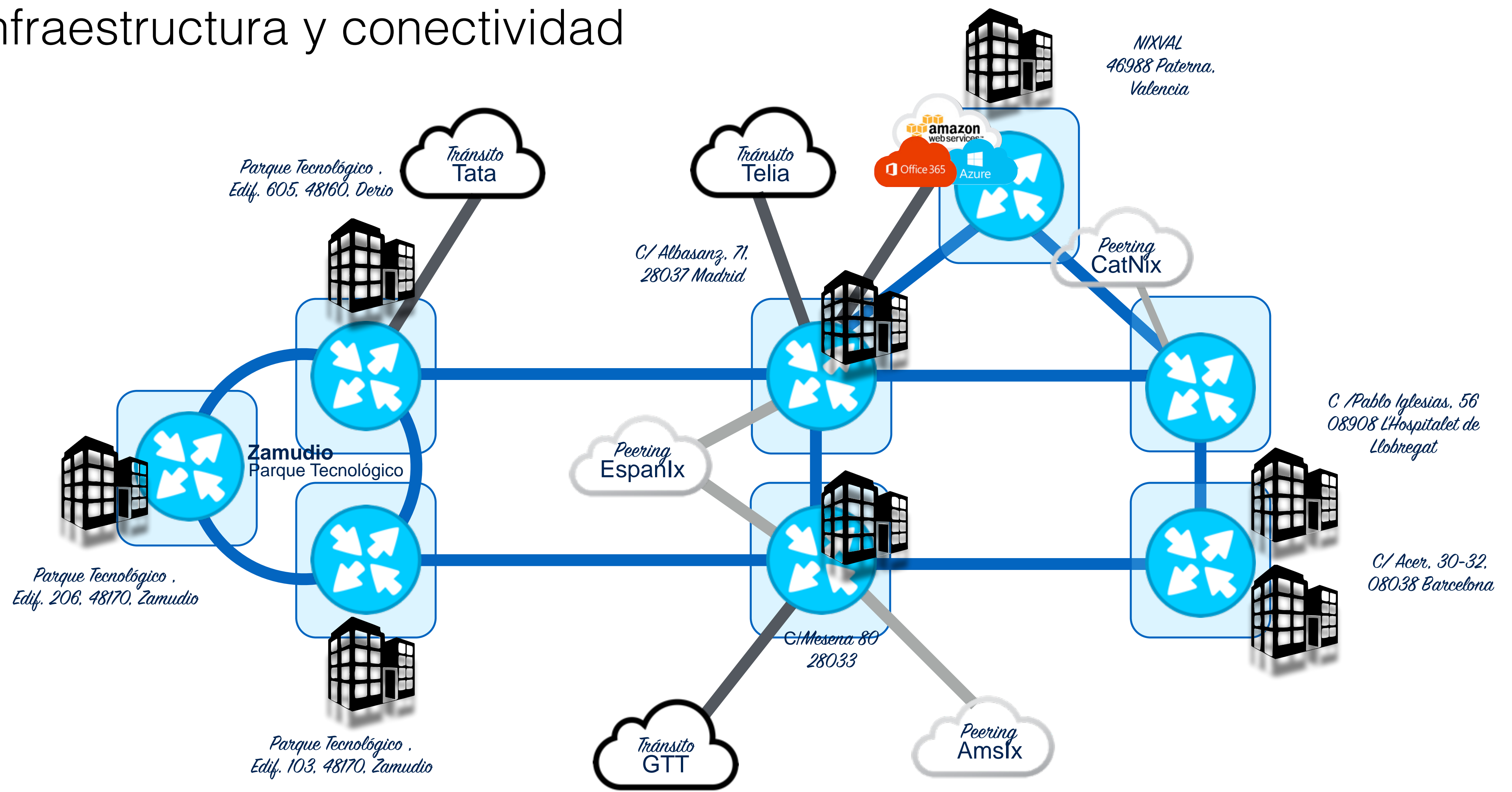
1 Infraestructura y conectividad



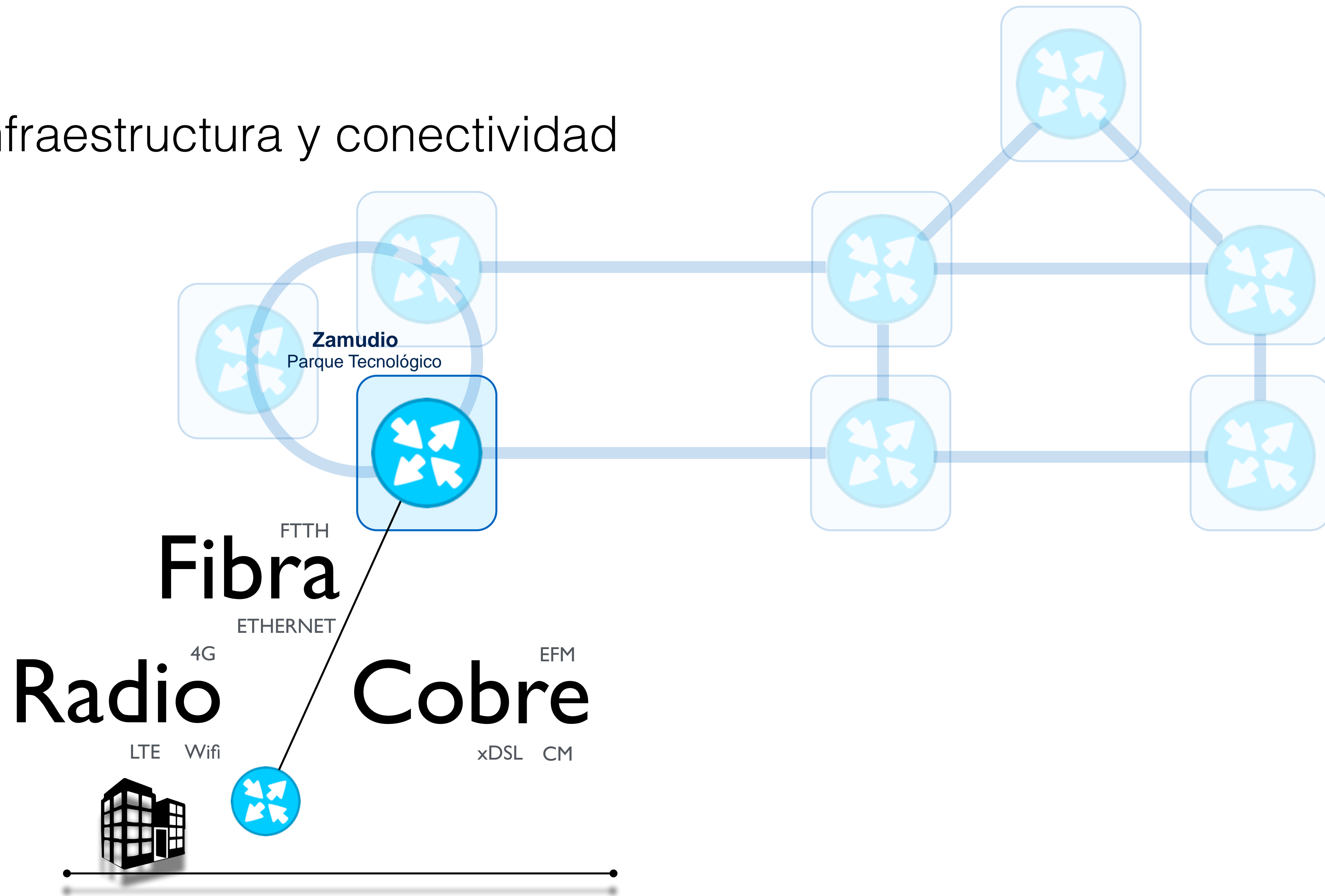
1 Infraestructura y conectividad



1 Infraestructura y conectividad



1 Infraestructura y conectividad

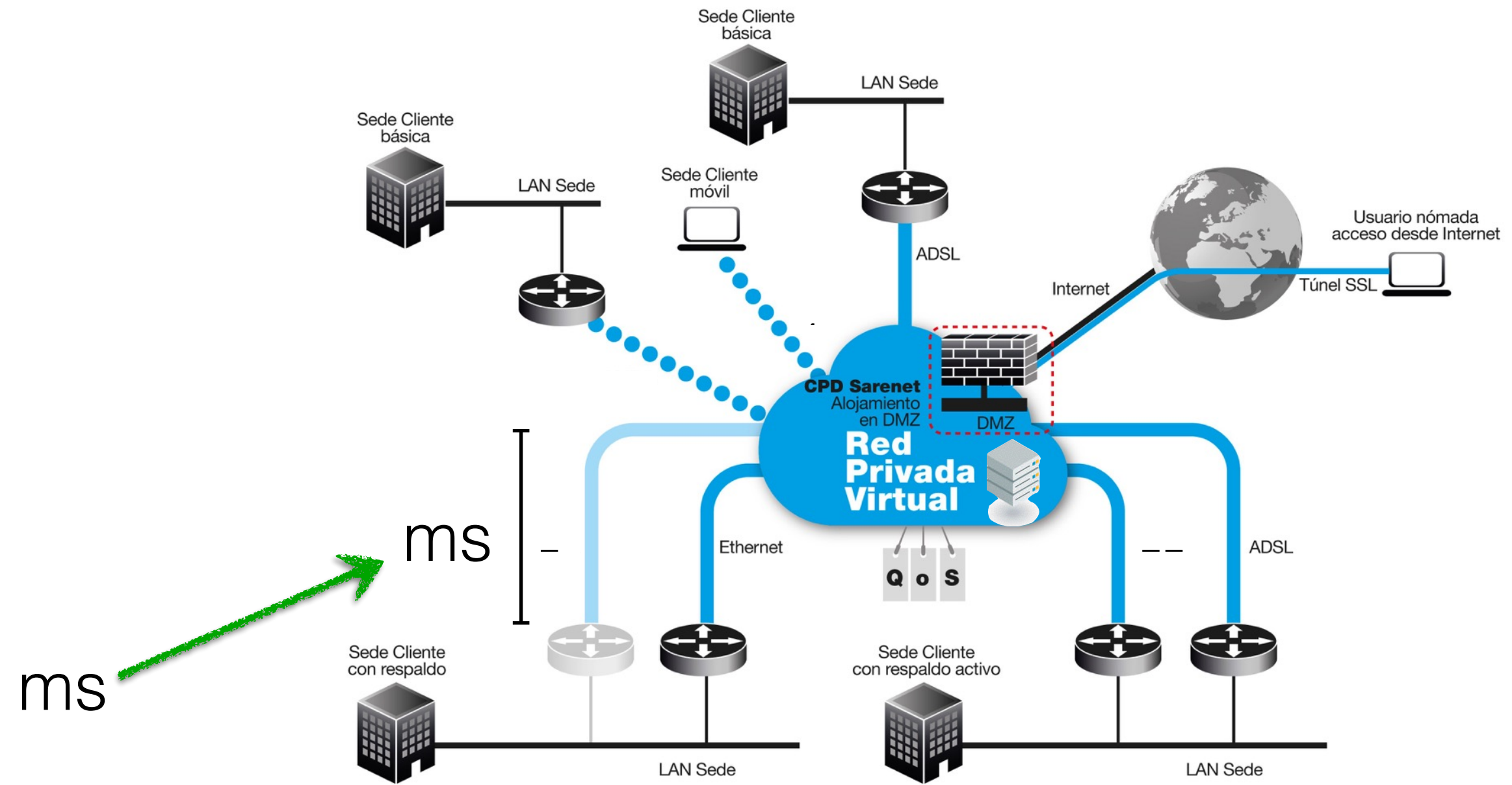
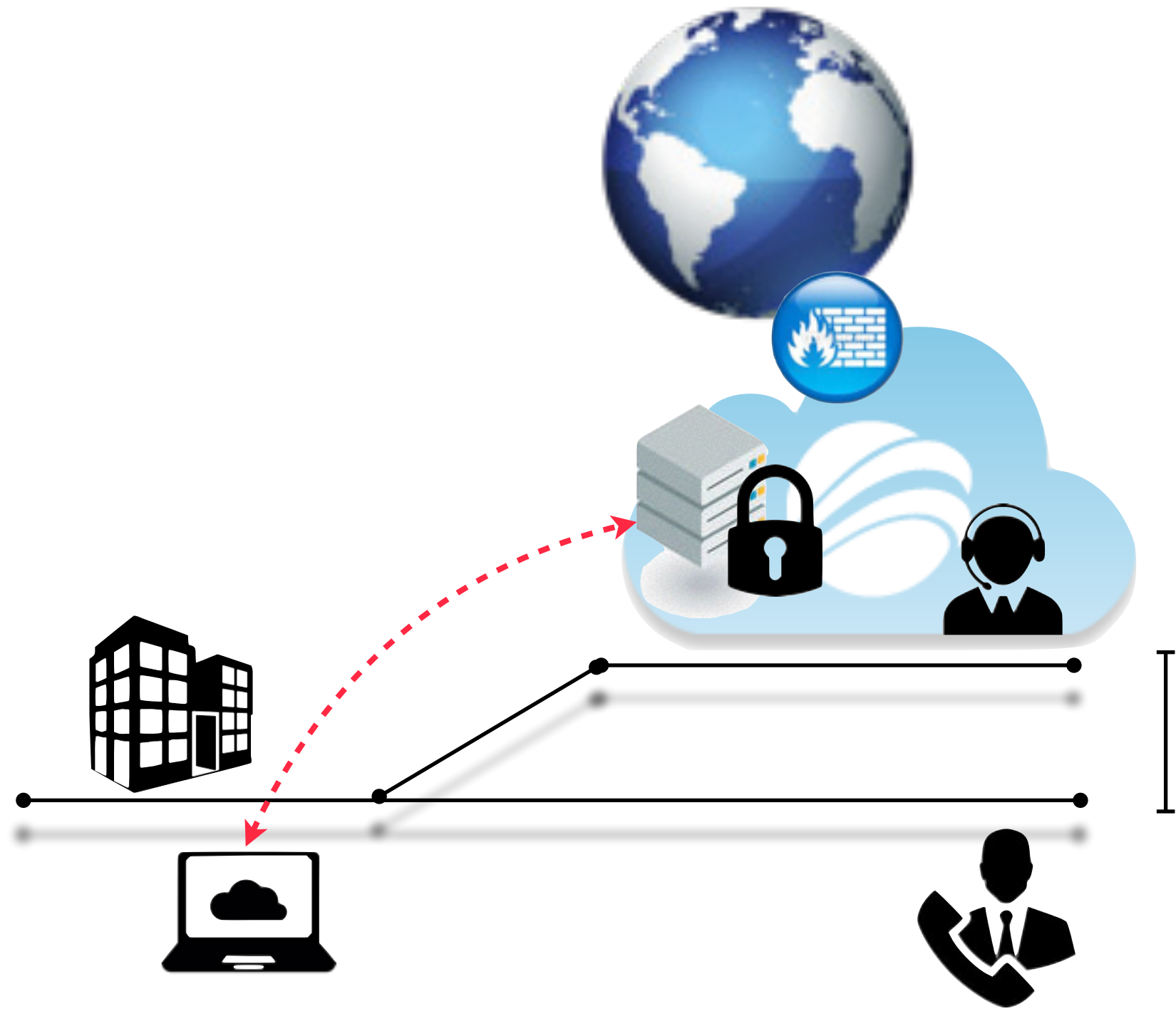




- Por qué son bajas las latencias de acceso
- Qué ventaja supone tener bajas latencias

Bajas
latencias

2 Bajas latencias

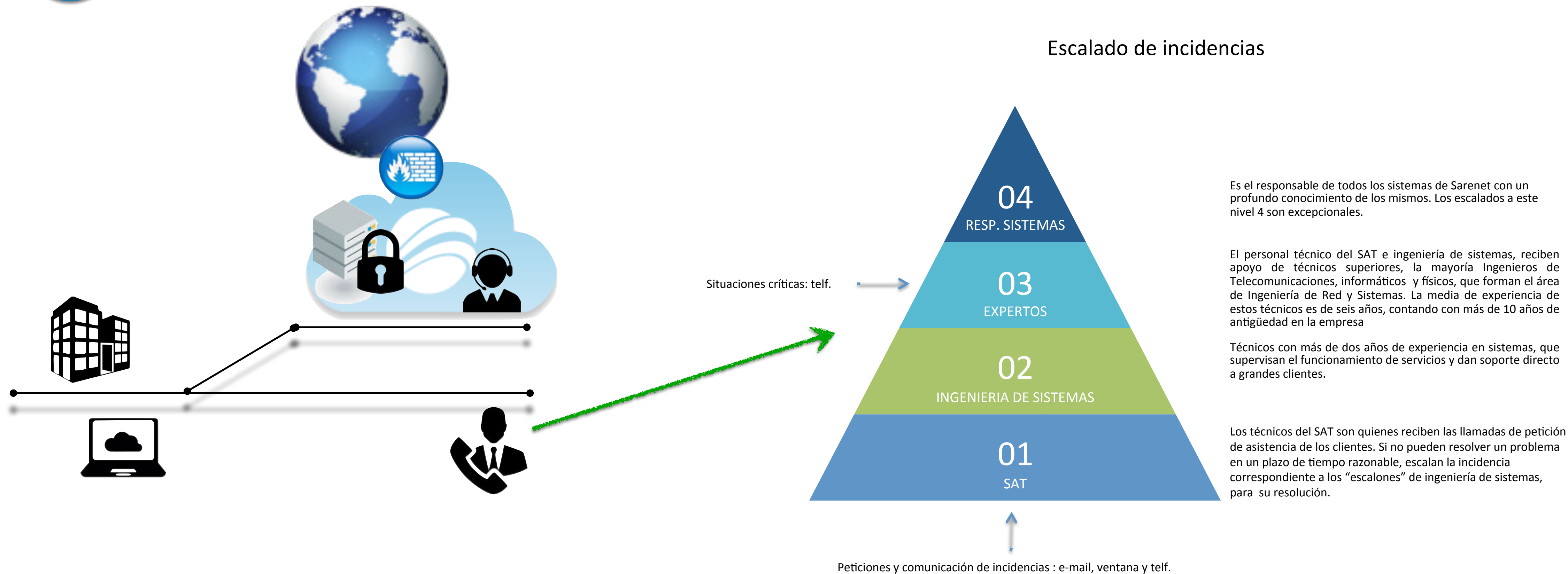




- Qué debes esperar del soporte técnico
 - Escalado claro de las incidencias
 - Alejado del DIY
 - Que les puedas poner caras, nombres y apellidos

Soporte
cercano

3 Soporte cercano y experto



Soporte cercano <—> lejos de DIY



3 Soporte cercano y experto

3 Soporte cercano y experto

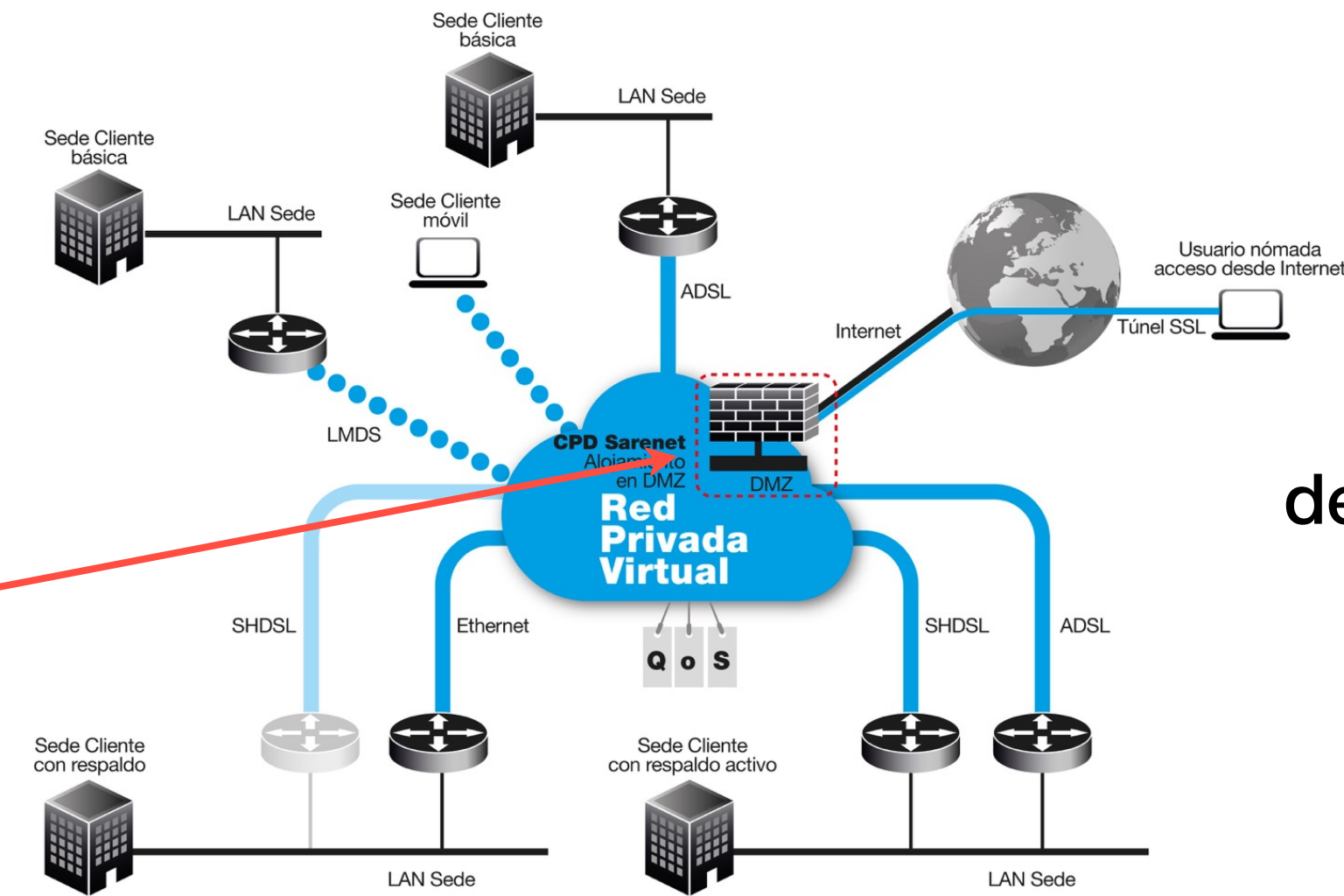
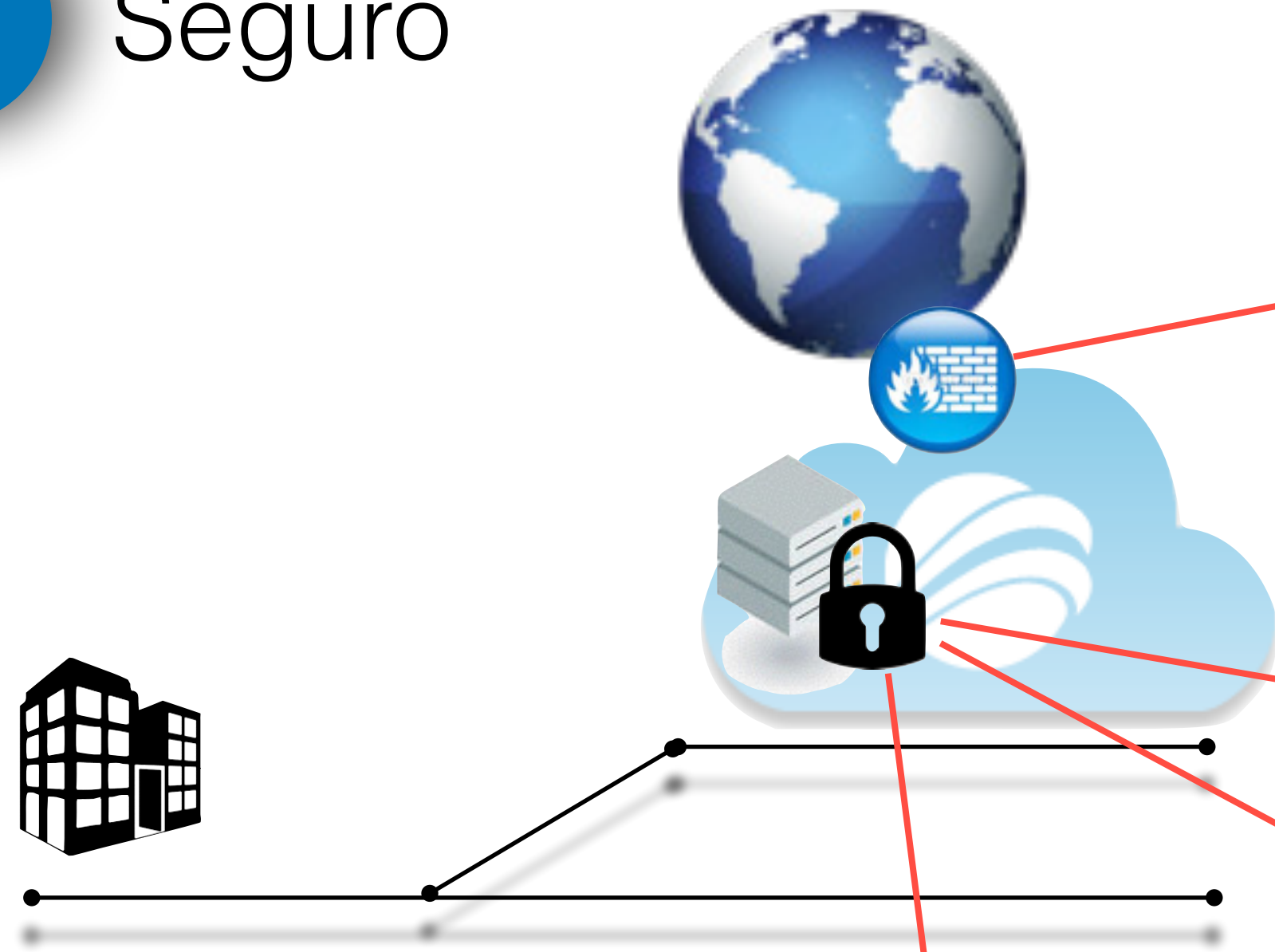
Baja rotación
en el
personal

4

- Qué niveles de seguridad ofrecemos
 - Red, perimetral
 - Cortafuegos de aplicaciones
 - Auditorías evolutivas
 - Mitigación frente ataques DDoS

Niveles de
seguridad

4 Seguro



Cortafuegos de última generación

Auditorías evolutivas

Cortafuegos de aplicaciones



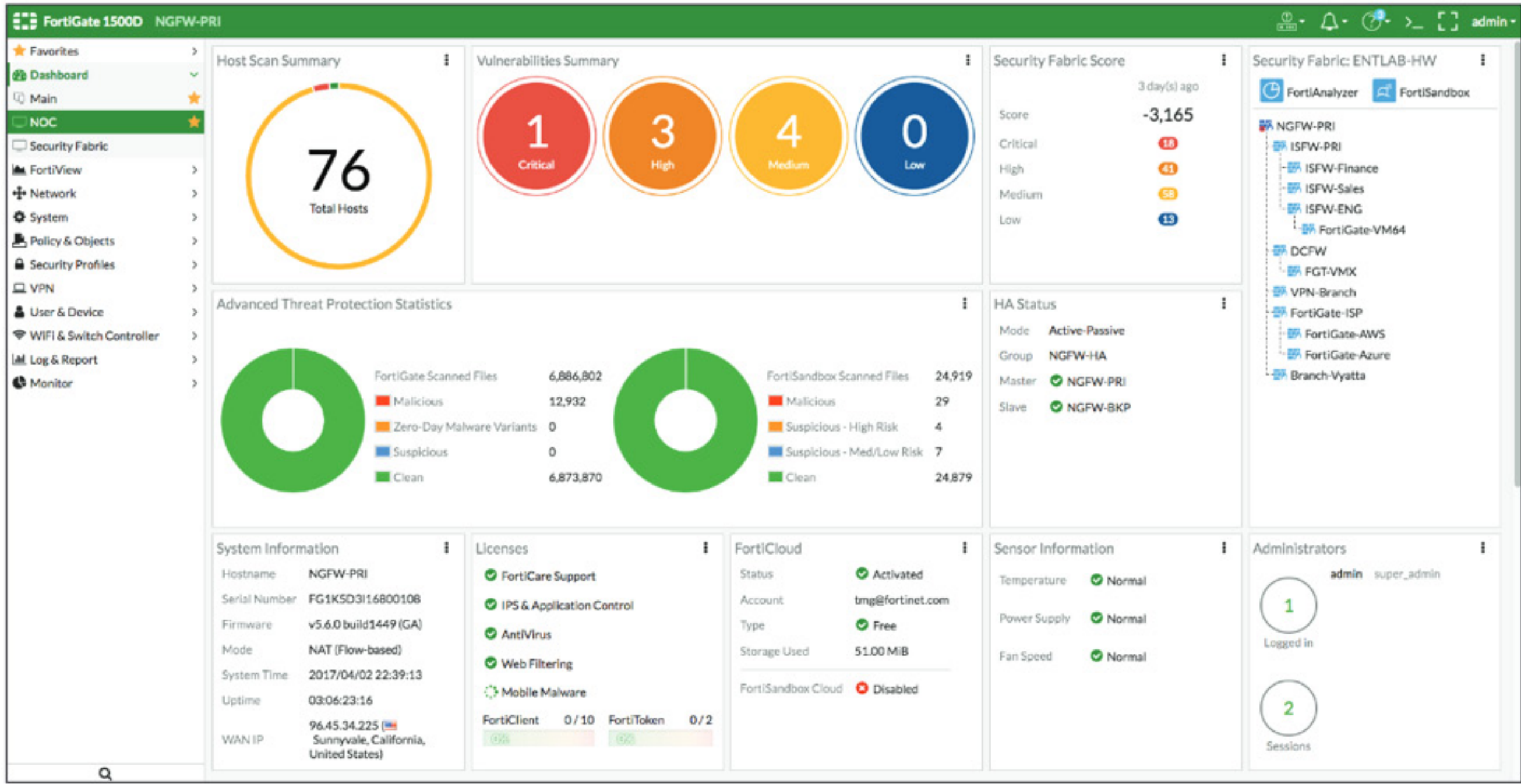
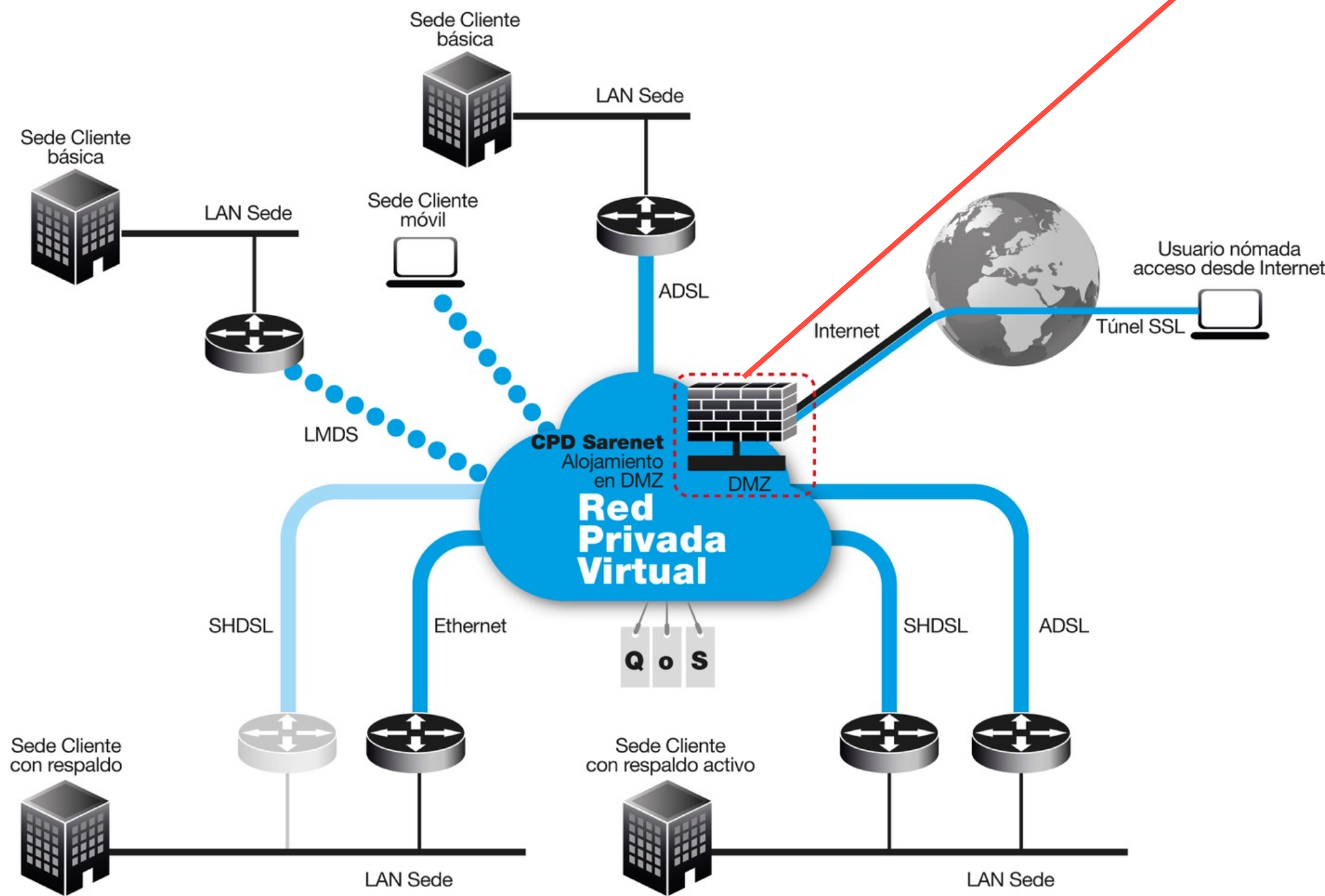
Mitigación de ataques DDoS

4

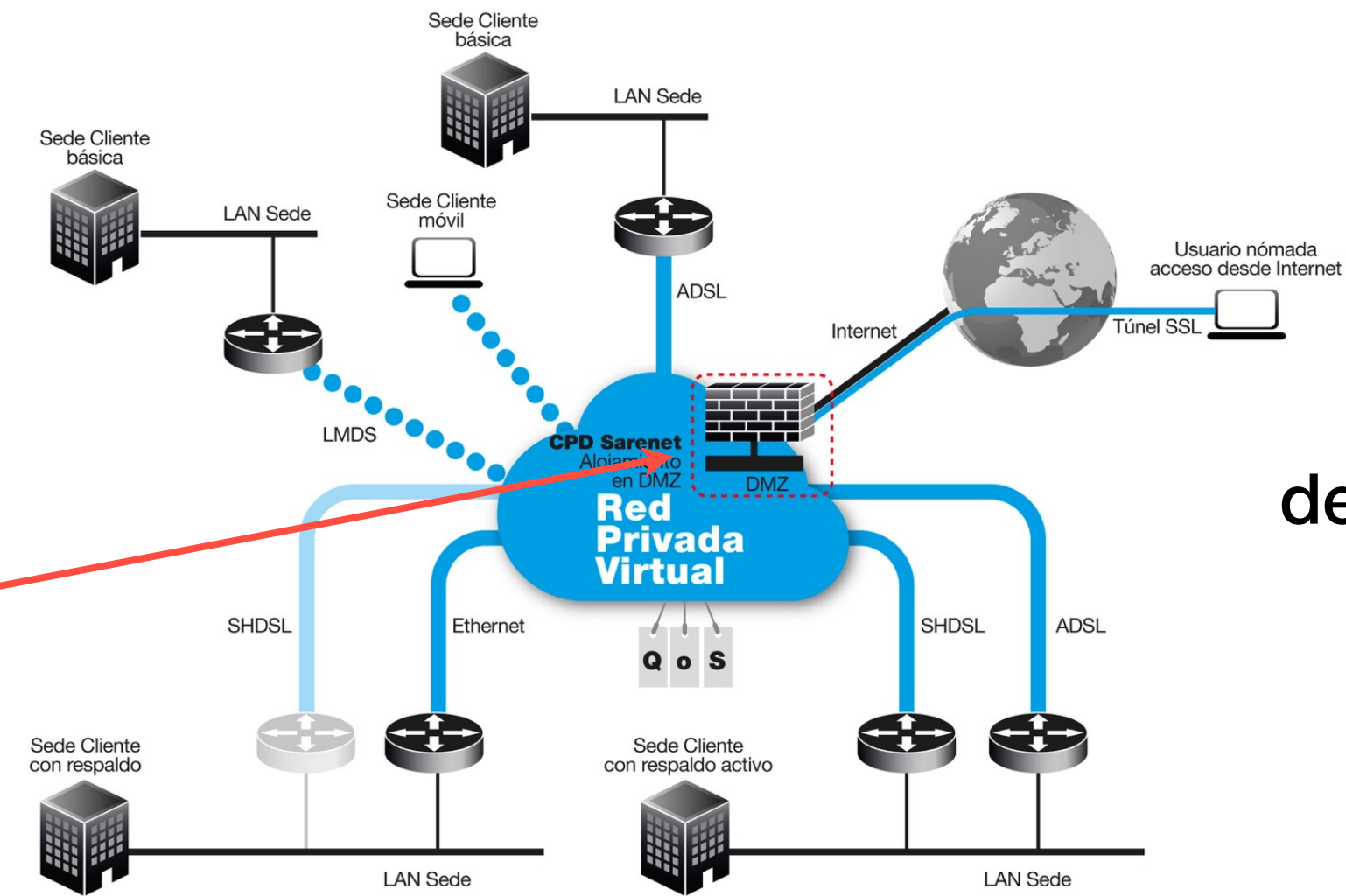
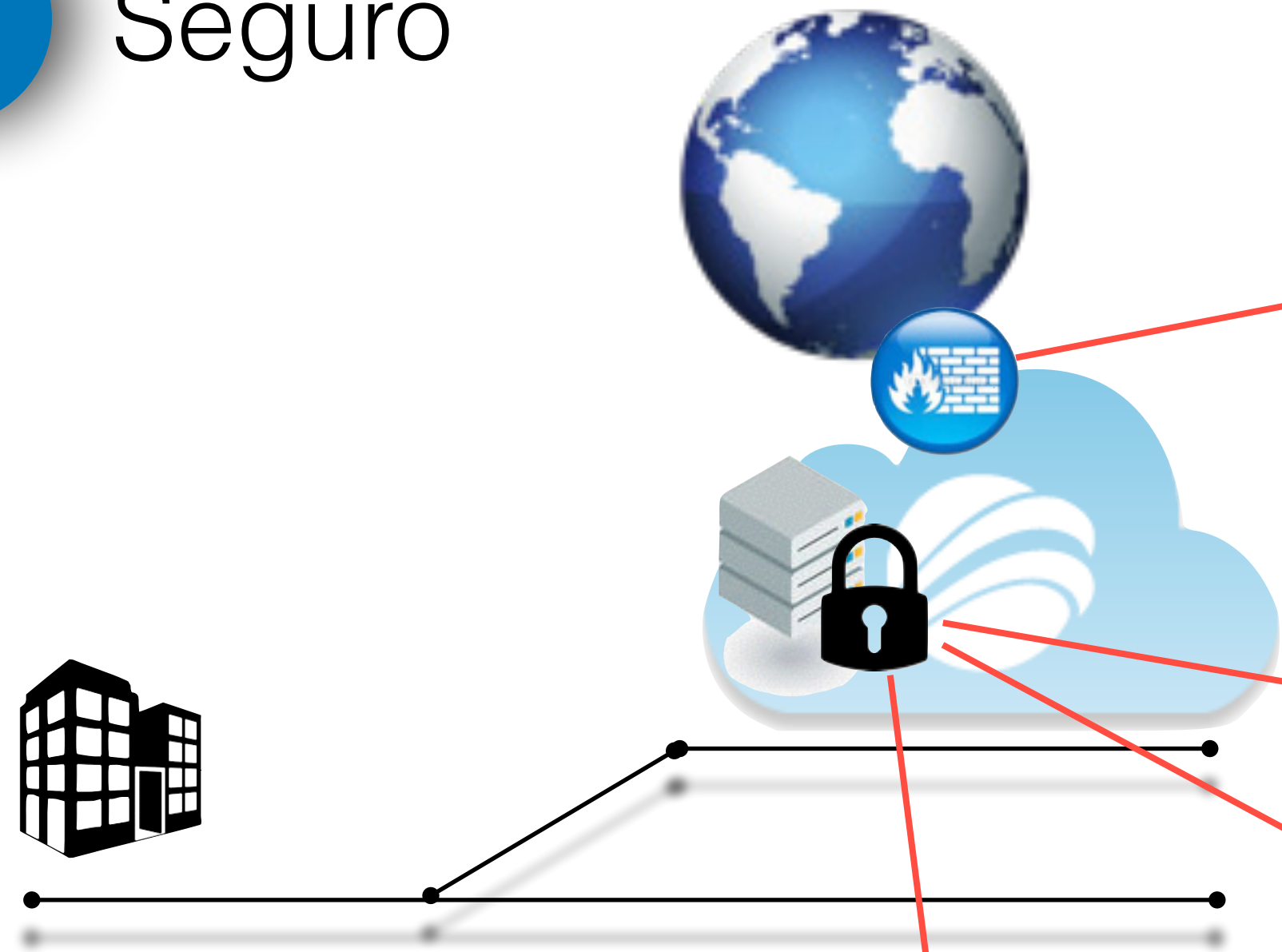
Seguro : Cortafuegos de última generación

MSSP GOLD PARTNER

SARENET
Zamudio, VIZCAYA, 48170, SPAIN
Phone: +34 94 420 94 70
<http://www.sarenet.es/internet/seguridad-gestionada/>



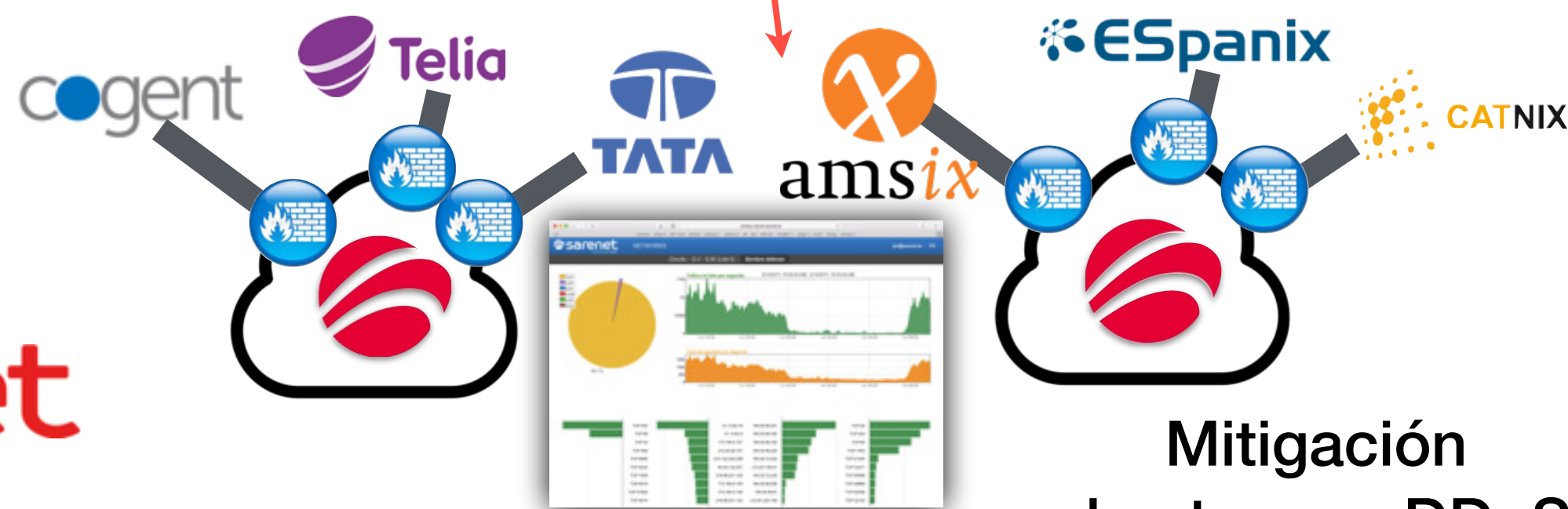
4 Seguro



Cortafuegos de última generación

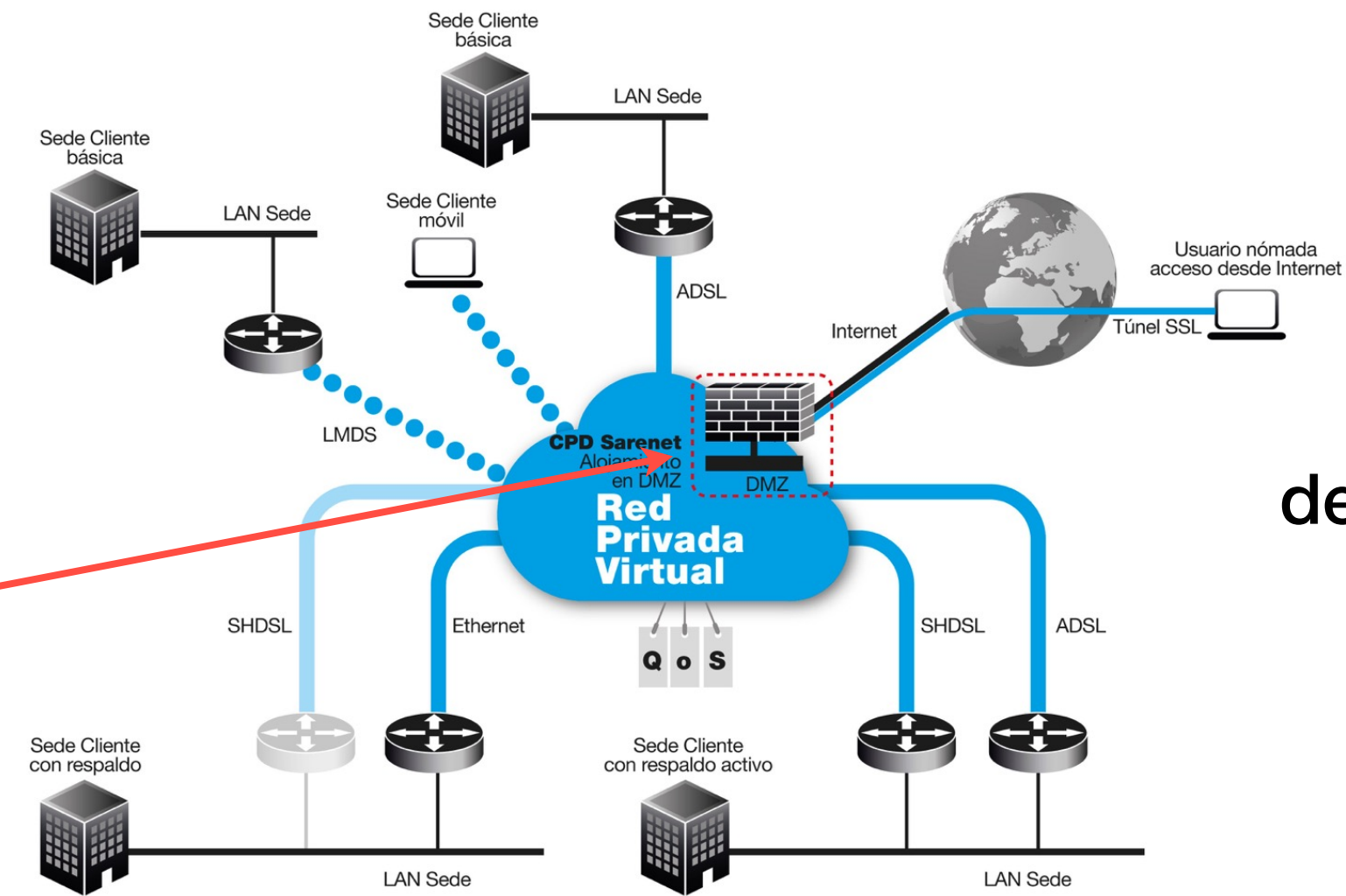
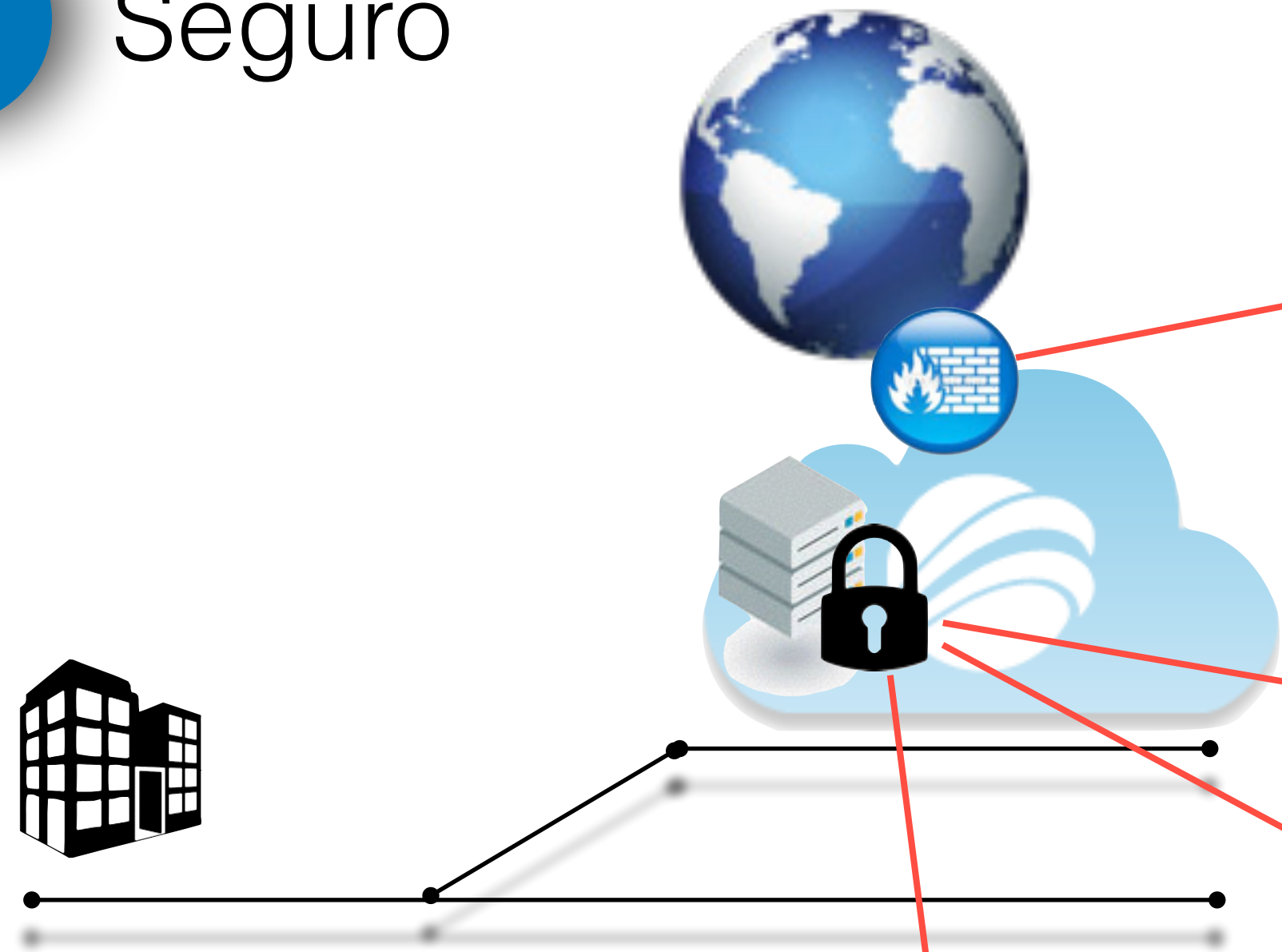
Auditorías evolutivas

Cortafuegos de aplicaciones



Mitigación de ataques DDoS

4 Seguro



Cortafuegos de última generación

Auditorías evolutivas

Cortafuegos de aplicaciones



4 Seguro : Cortafuegos de aplicaciones

FrontalPro



Cortafuegos de aplicaciones

+
Balanceador
+
Caché

Web Firewall / Webs / Bloqueos / Bloqueo

Datos

Fecha y hora	29 de octubre de 2013 a las 15:50
Método	GET
Host	wwwfront.sarenet.es
URI	/noticias/2002/02/11/interes-seguridad-crecido-tras-acontecimientos.html
IP Origen	192.148.167.11
User-Agent	Wget/1.12 (darwin10.7.1)
Razón (Ver regla)	

Mensaje

```
rule 803afad38 [id "970003"][file "/usr/local/etc/nginx/modsecurity/wwwfront2.sarenet.es-modsecurity.conf"][line "3145"] - Execution error - PCRE limits exceeded (-8): (null).
```

[+ Ver](#)



IPs bloqueadas

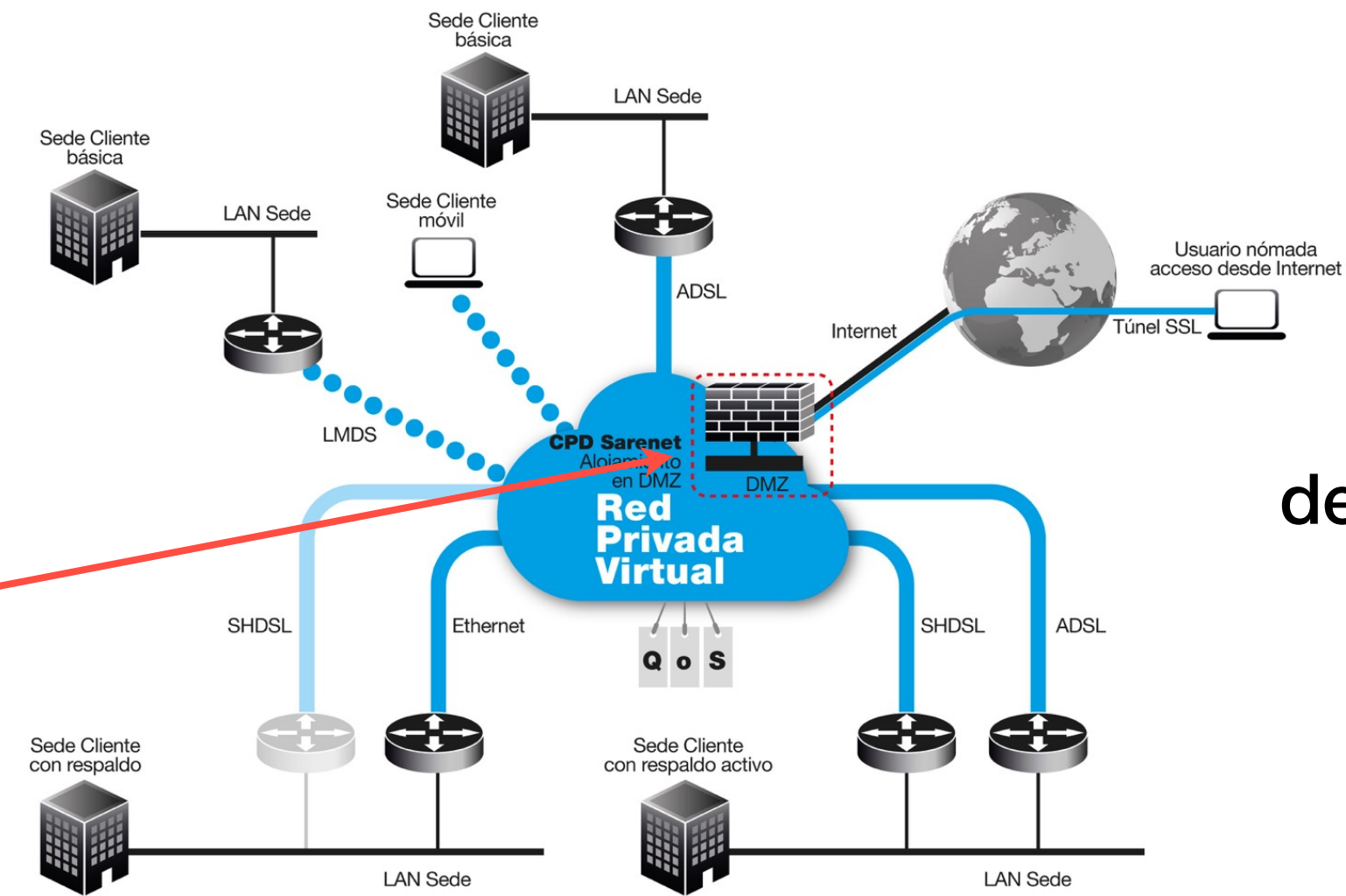
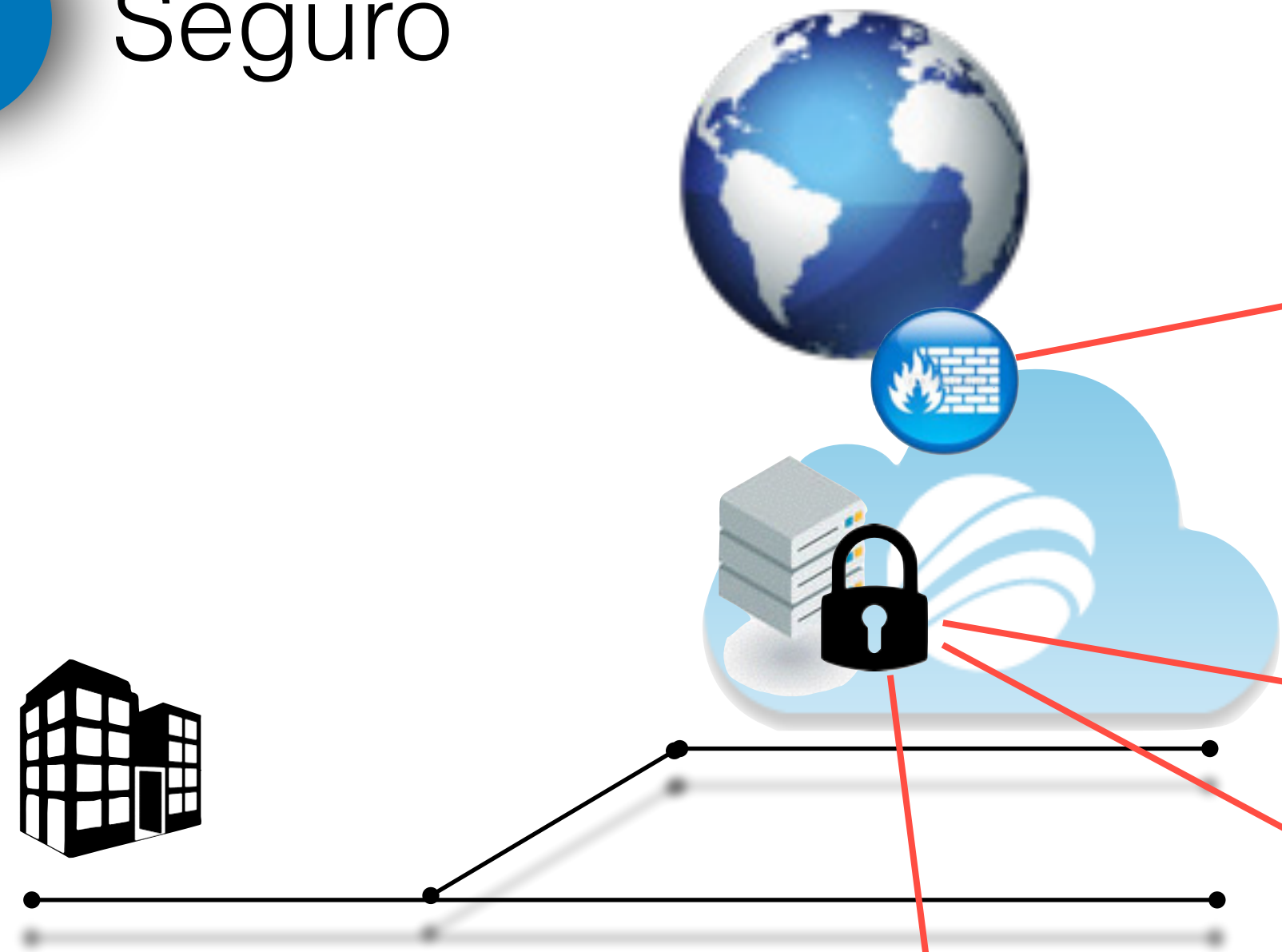
192.148.167.11	Spain
193.225.190.254	Hungary
193.239.186.196	Netherlands
123.167.5.45	China
213.197.216.236	Netherlands
198.20.69.74	N/A
194.30.0.16	Spain
176.31.107.115	France
222.103.190.147	Korea, Republic of

Web Firewall / Webs / Bloqueos

[Actualizar](#) [Buscar](#)

Fecha	IP Ataque	Host	URI	Método	Acciones
29 de octubre de 2013 a las 15:50	192.148.167.11	wwwfront.sarenet.es	/prensa/medios/eweek/interes-seguridad-crecido-tras-acontecimientos-2684.html	GET	Ver
29 de octubre de 2013 a las 15:50	192.148.167.11	wwwfront.sarenet.es	/noticias/2002/02/11/interes-seguridad-crecido-tras-acontecimientos.html	GET	Ver
29 de octubre de 2013 a las 15:29	192.148.167.11	wwwfront.sarenet.es	/prensa/medios/eweek/interes-seguridad-crecido-tras-acontecimientos-2684.html	GET	Ver

4 Seguro



Cortafuegos de última generación

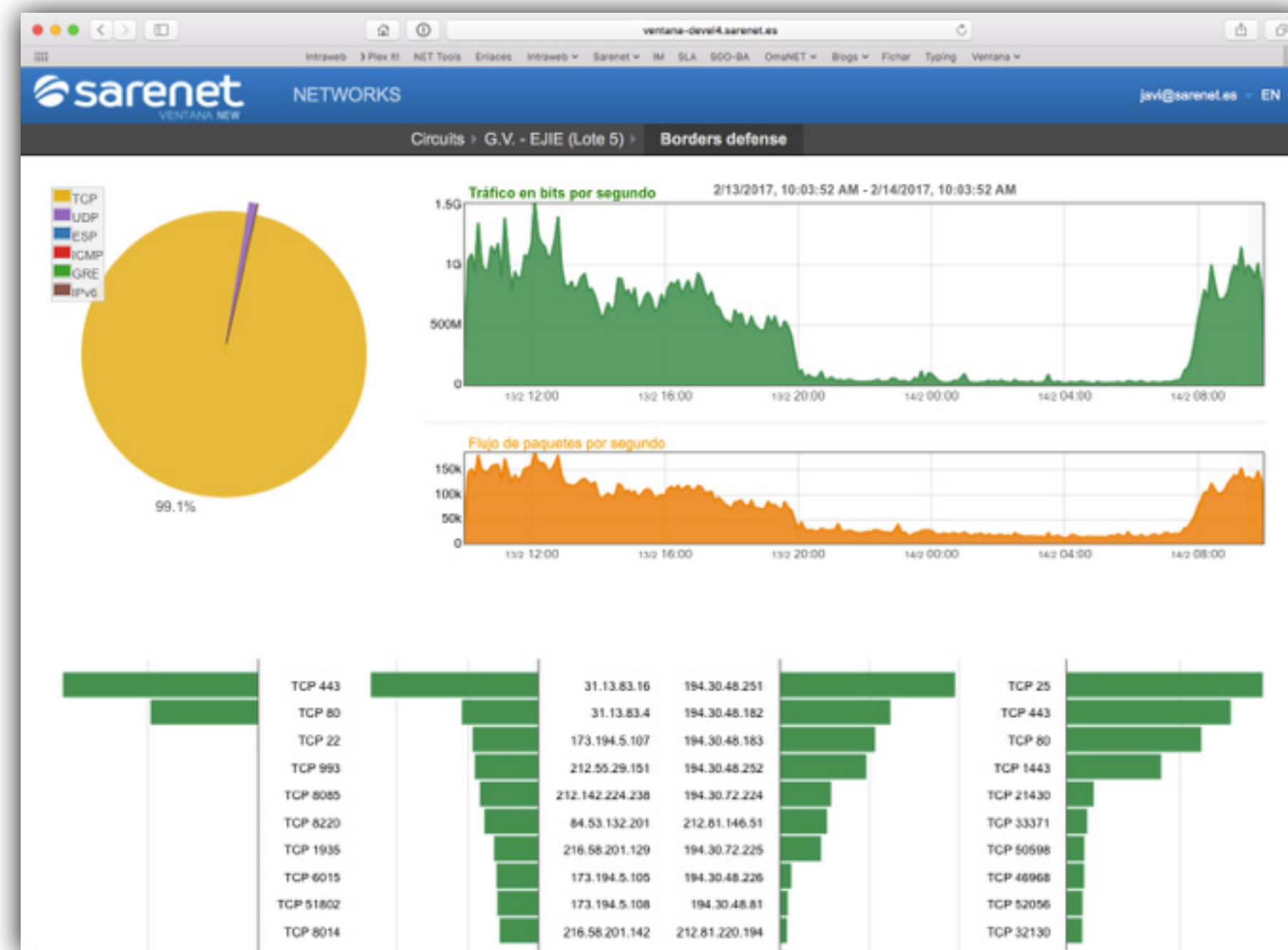
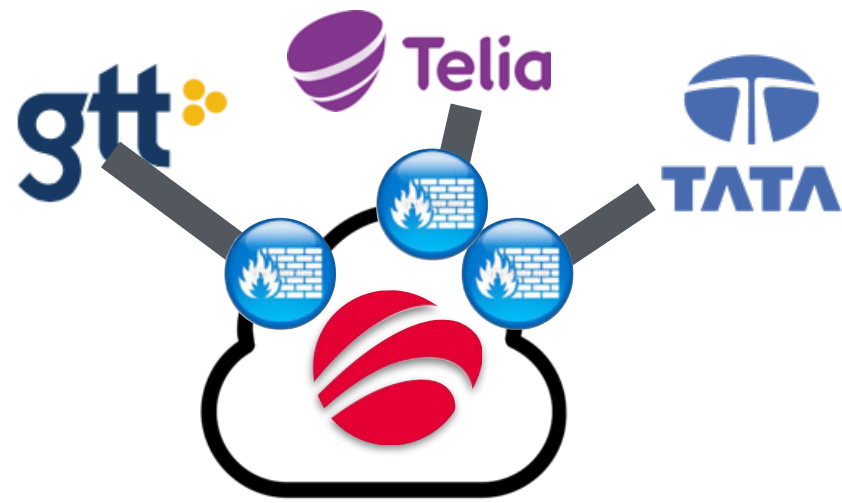
Auditorías evolutivas

Cortafuegos de aplicaciones



Mitigación de ataques DDoS

4 Seguro: Anti-DDoS





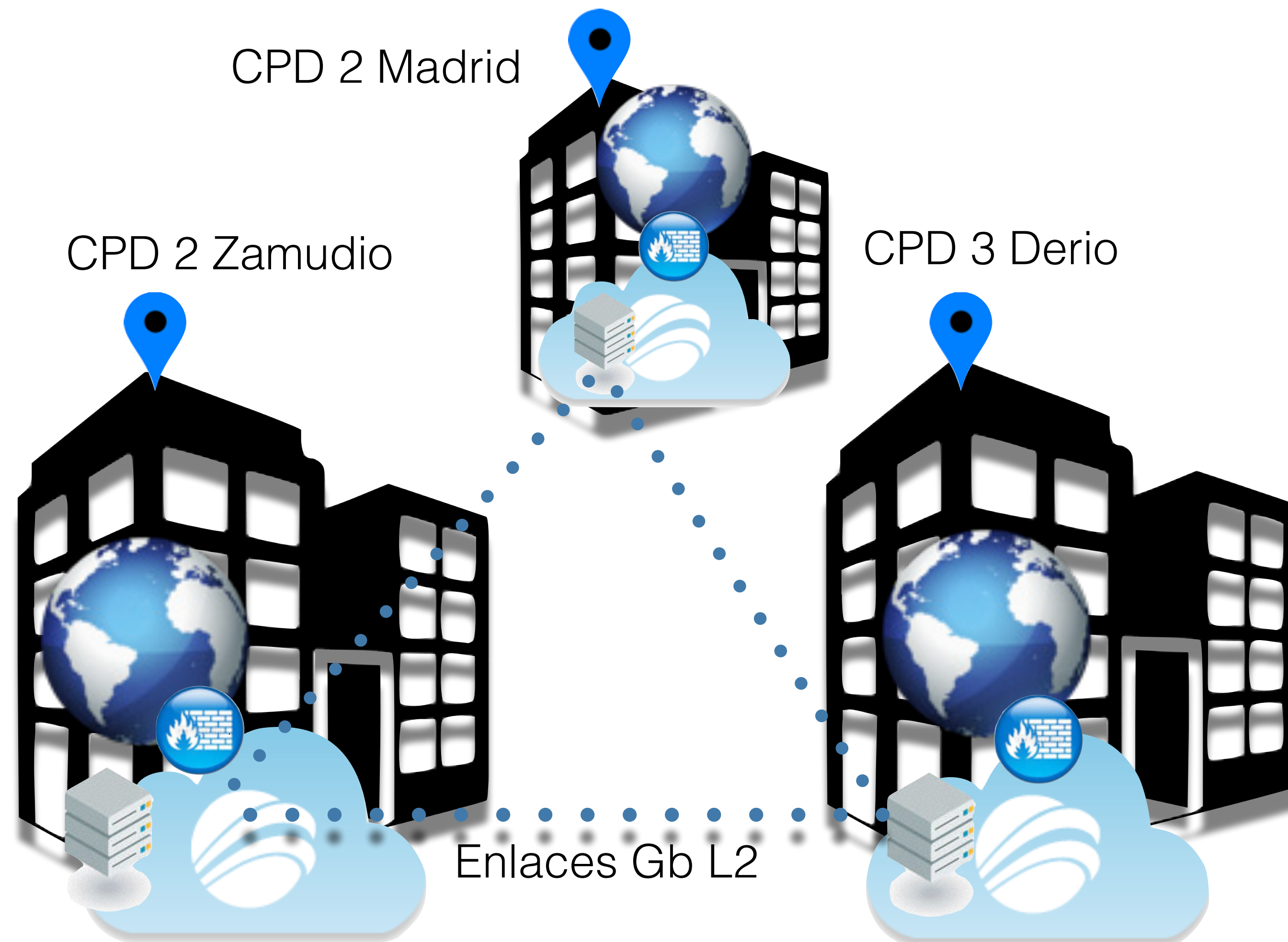
- Cómo montar un plan DR aprovechando los data centers : redundancia flexible
- Cómo se puede extender el concepto de cloud híbrida
 - CPD extendido : Máquinas físicas y Virtuales
 - Accesos seguros a otros hosters
 - Podemos ser la extensión de tu infraestructura

Arquitecturas
flexibles

5

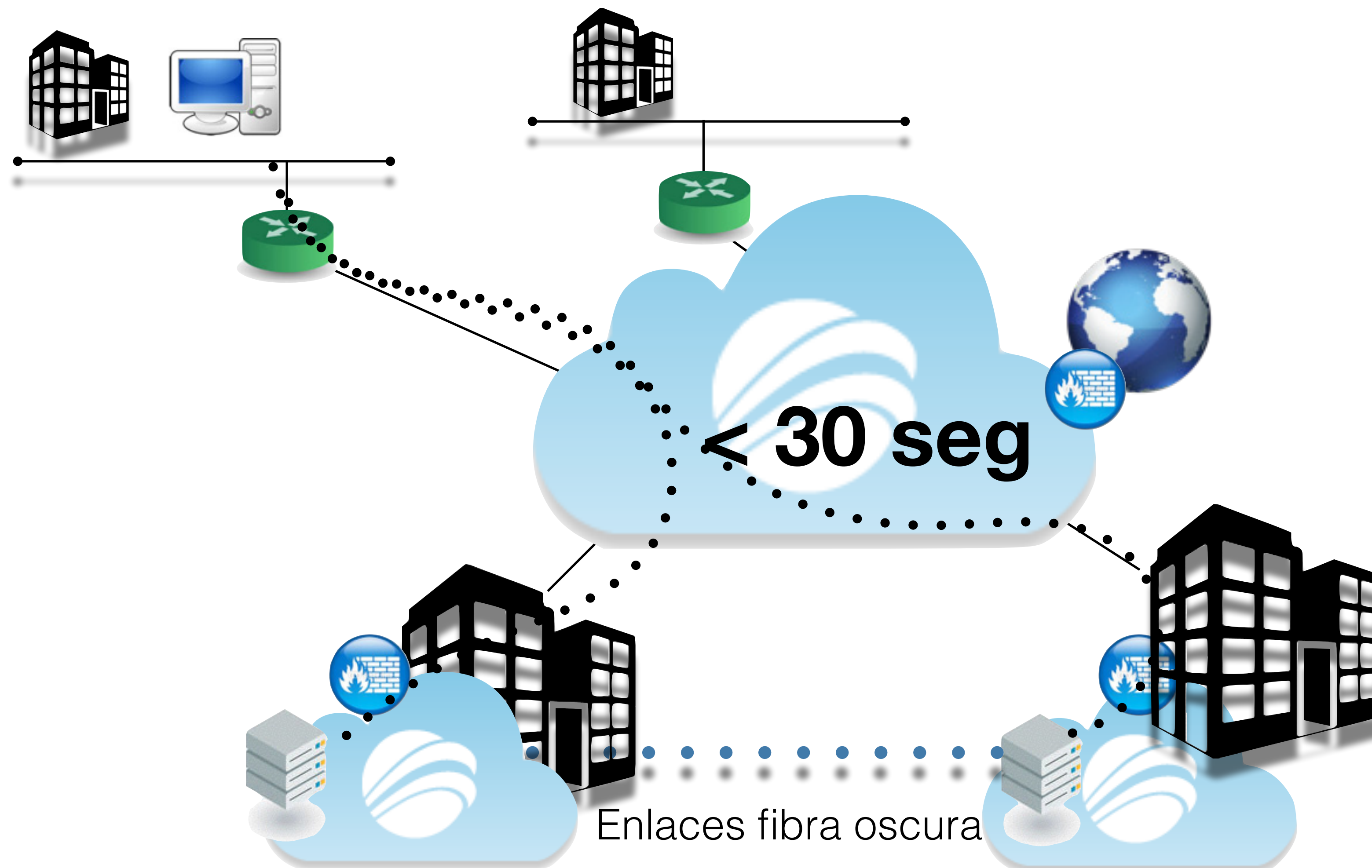
Flexible

Redundancia flexible

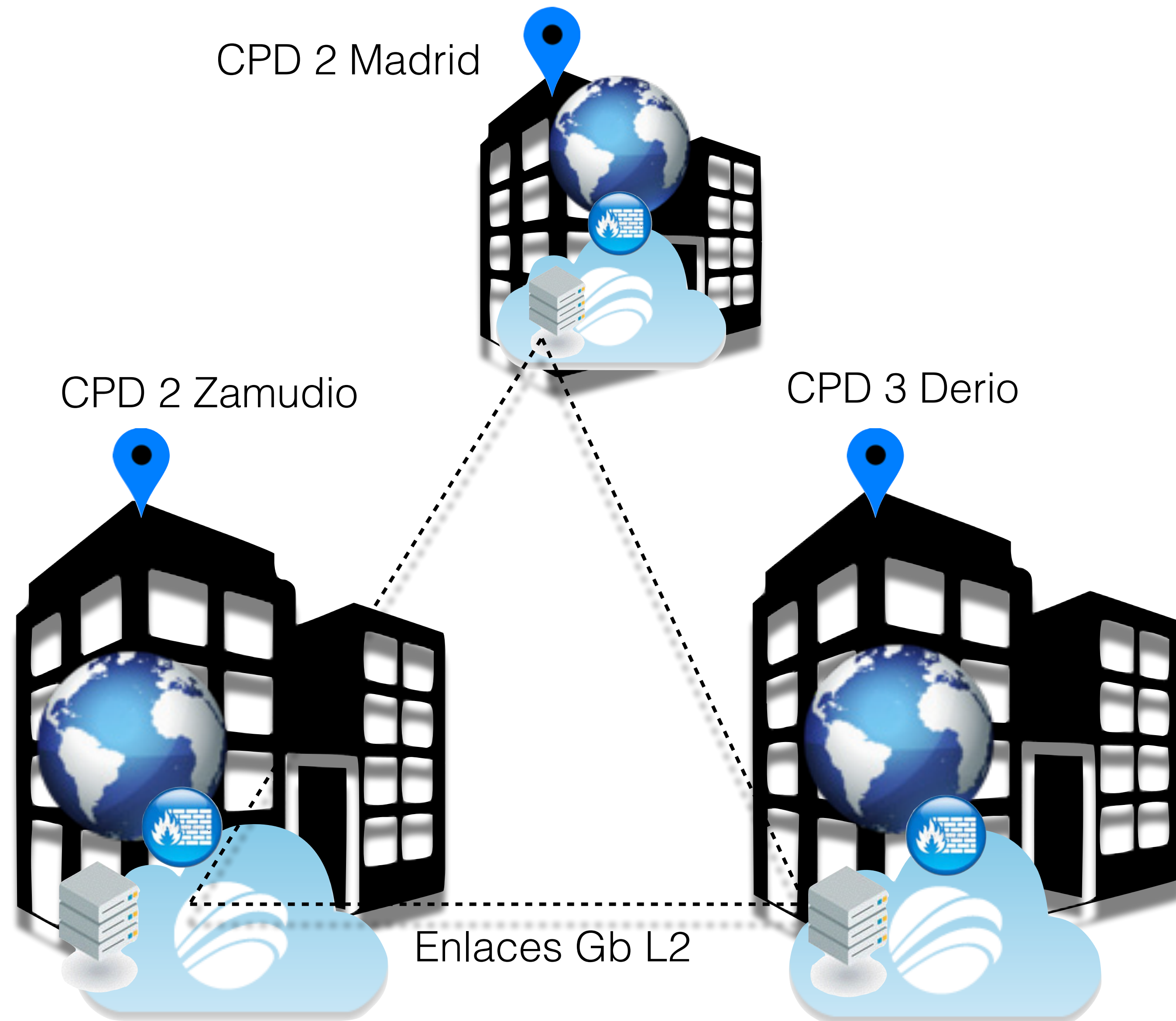


5

Flexible Redundancia flexible

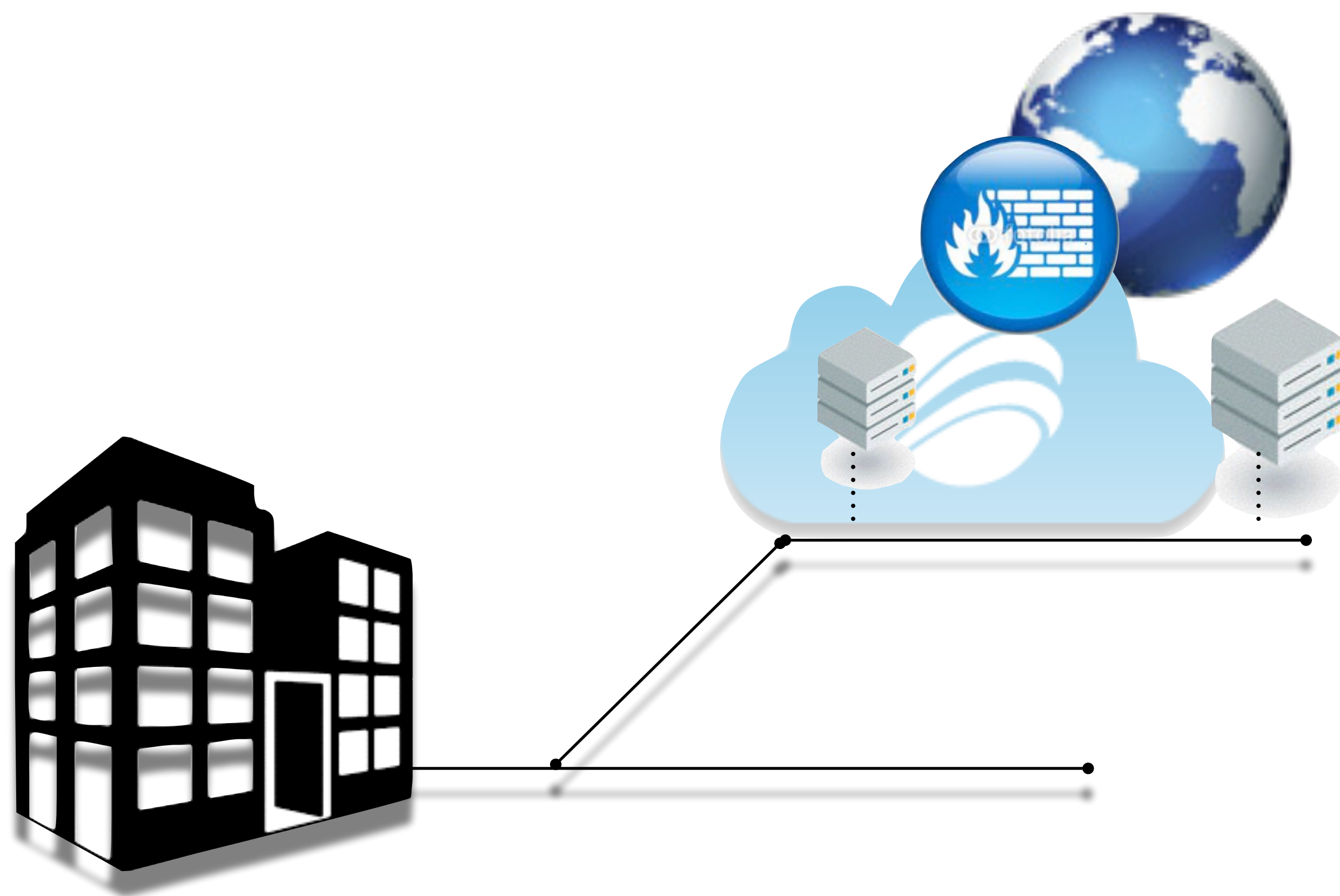


5 Flexible



5 Flexible

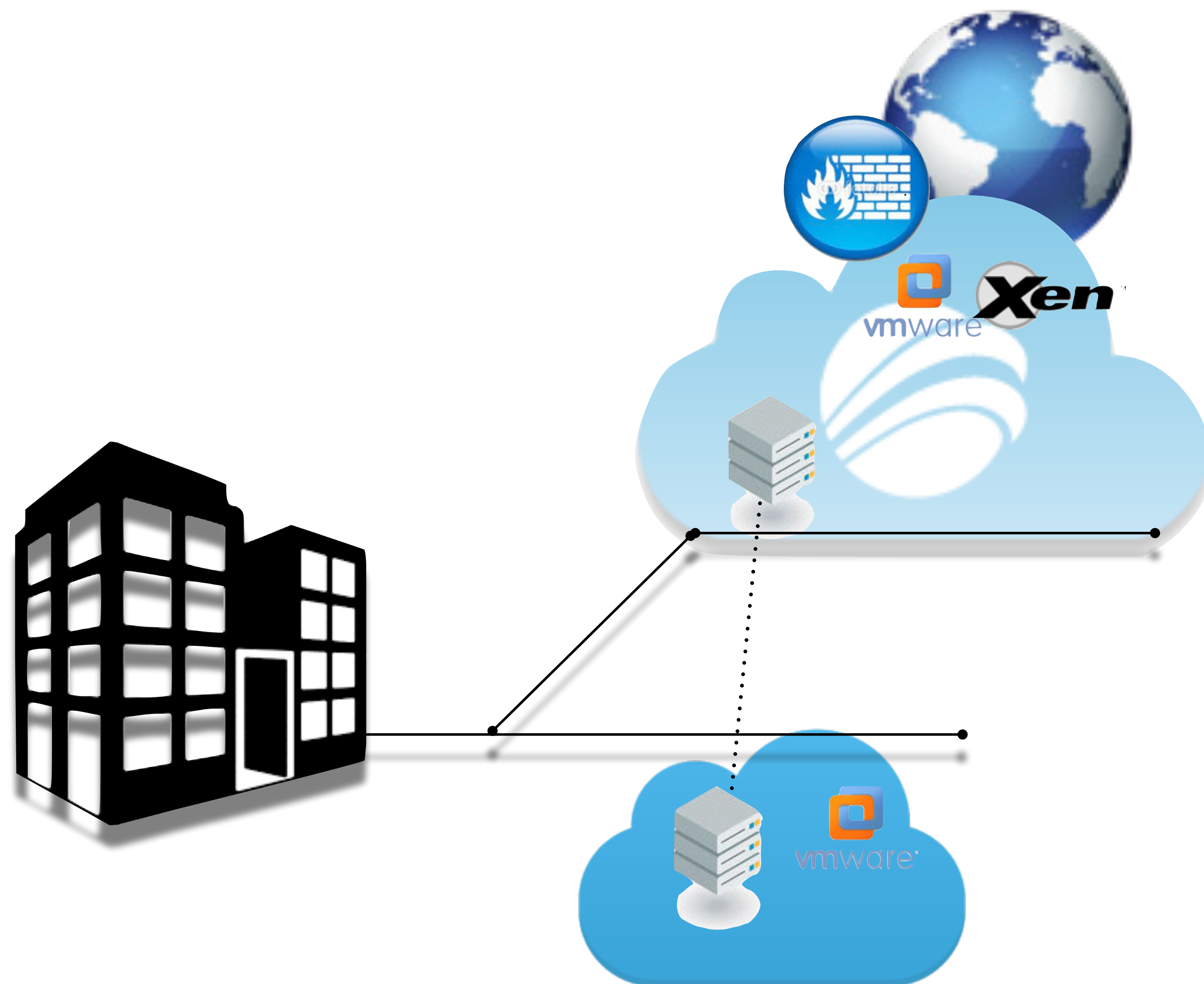
Cloud Híbrida



VLAN con
máquinas virtuales
y físicas

5 Flexible

Cloud Híbrida

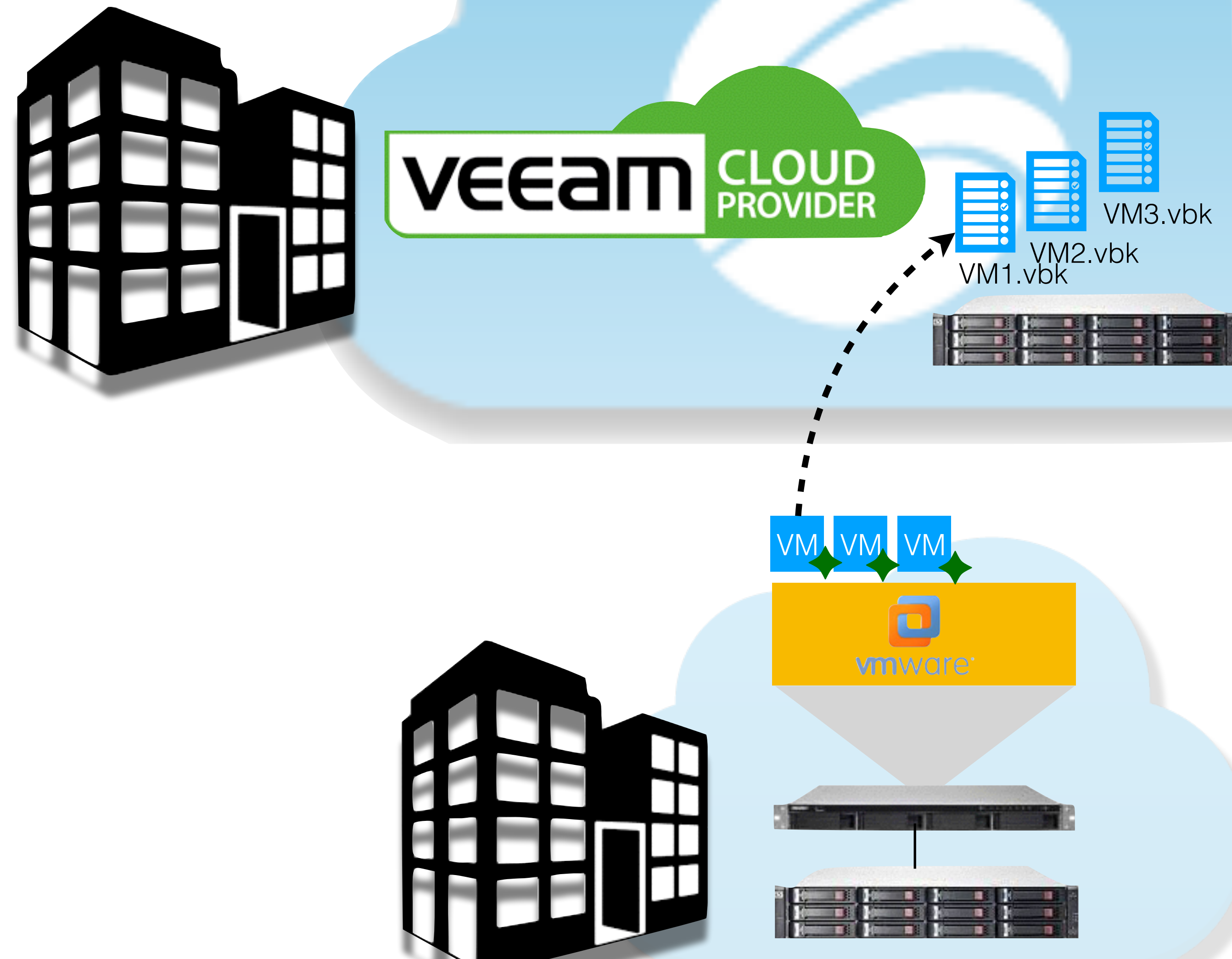


Extensión de la infraestructura del cliente las máquinas virtuales se cargan como imágenes

5 Flexible

Cloud + Veeam

Copias



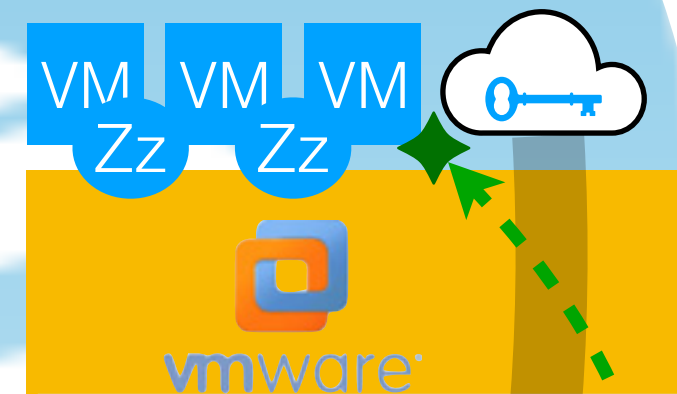
5 Flexible

Cloud + Veeam

Réplicas



VEEAM CLOUD PROVIDER



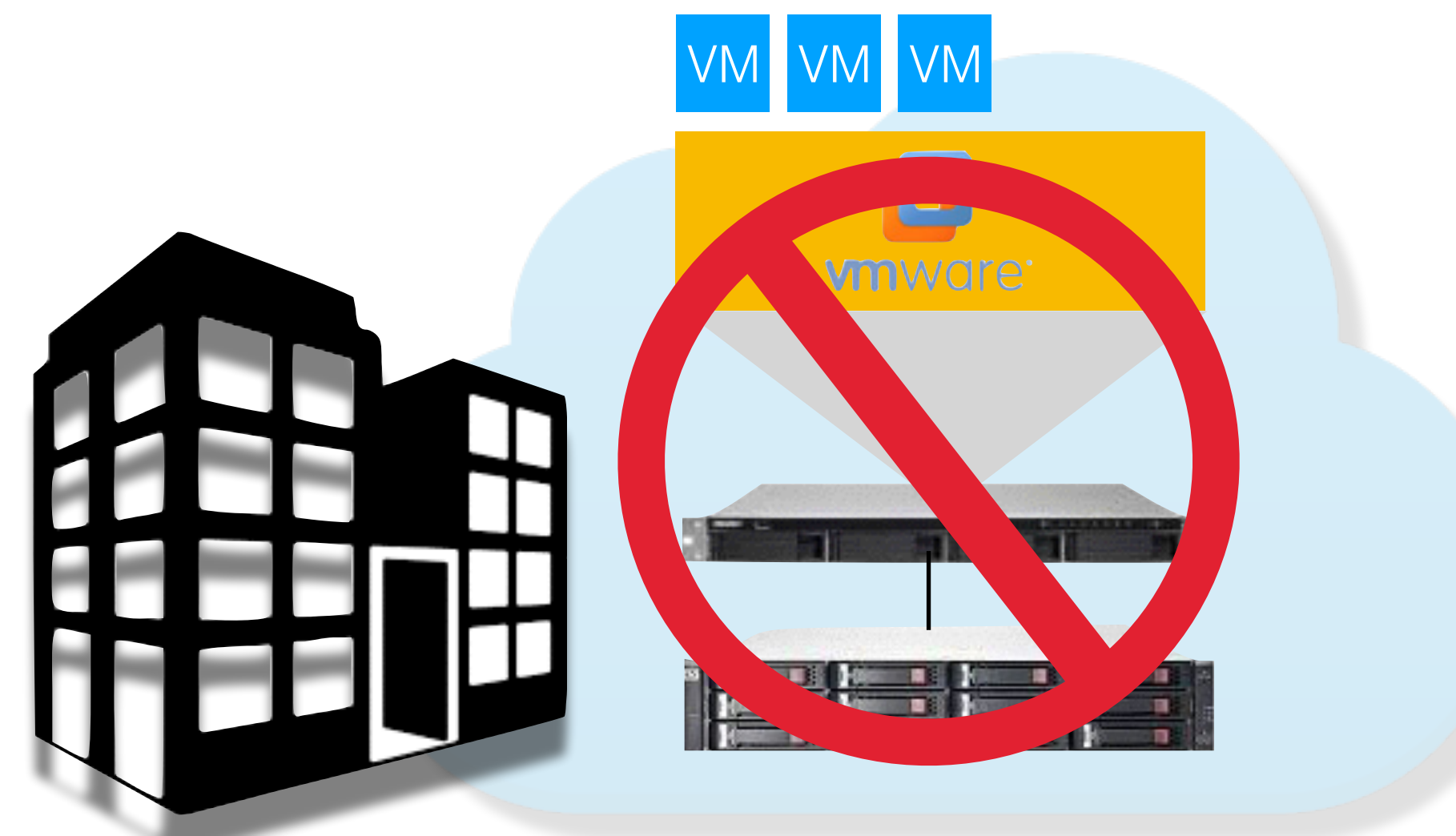
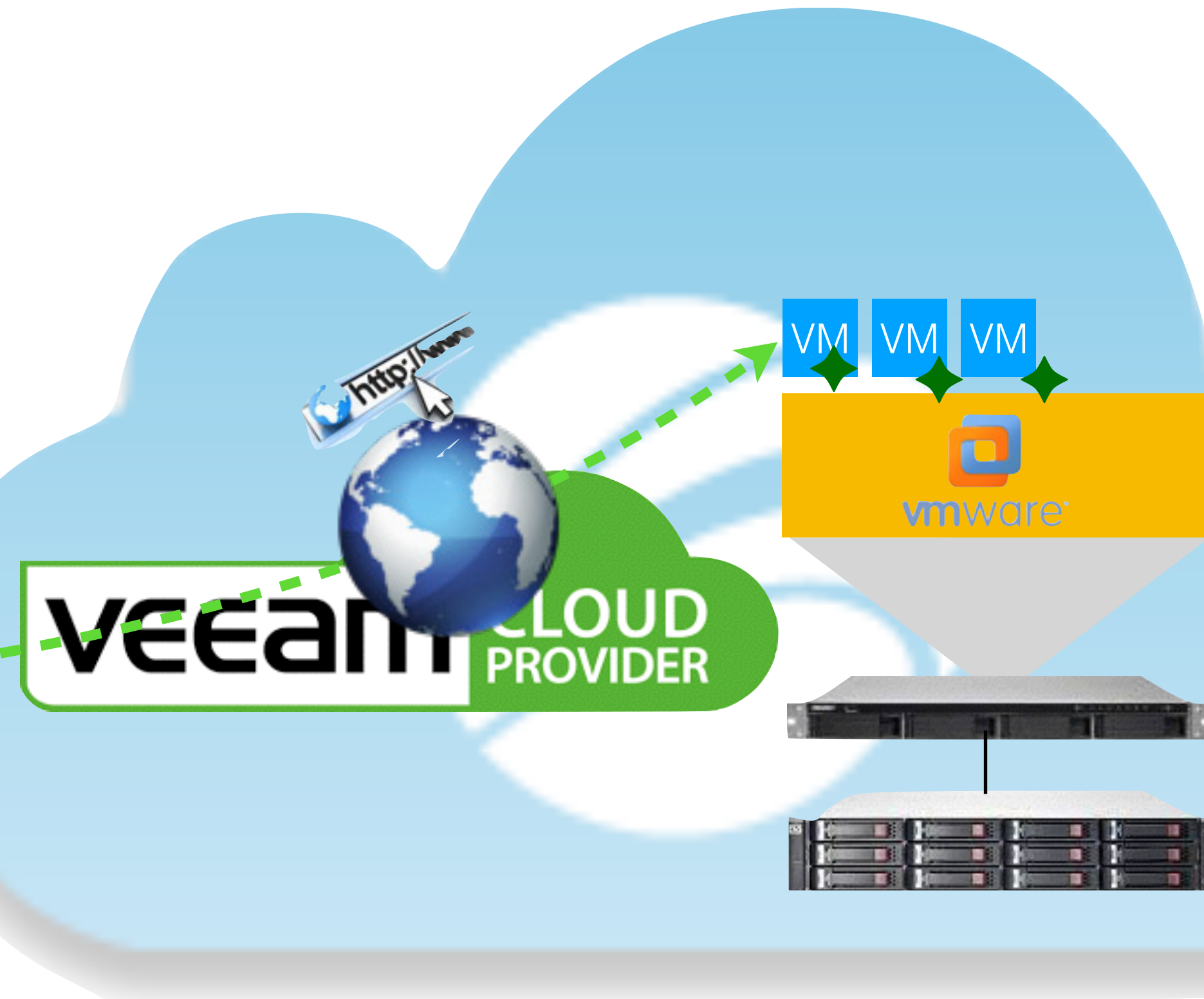
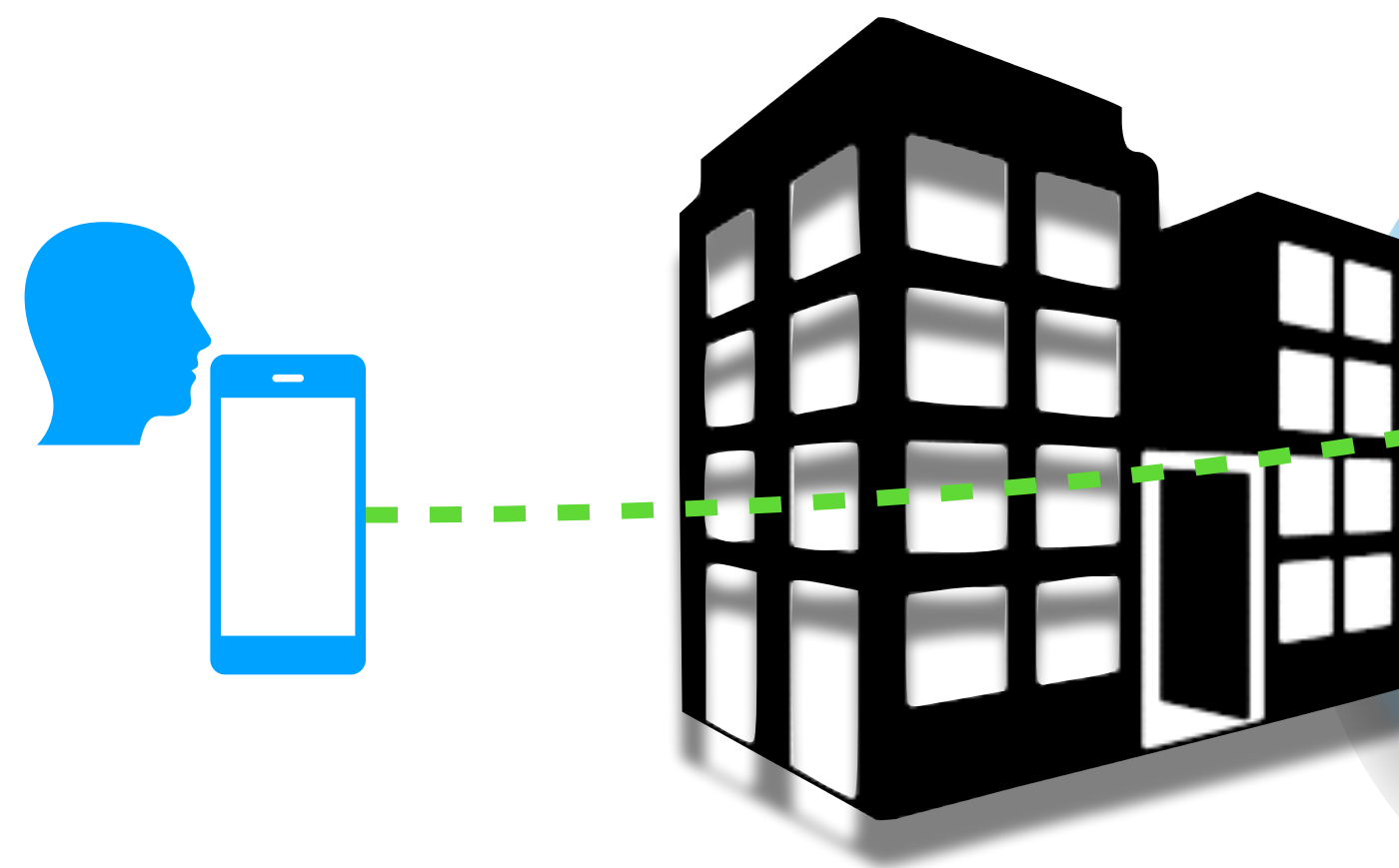
Network Extension Appliance



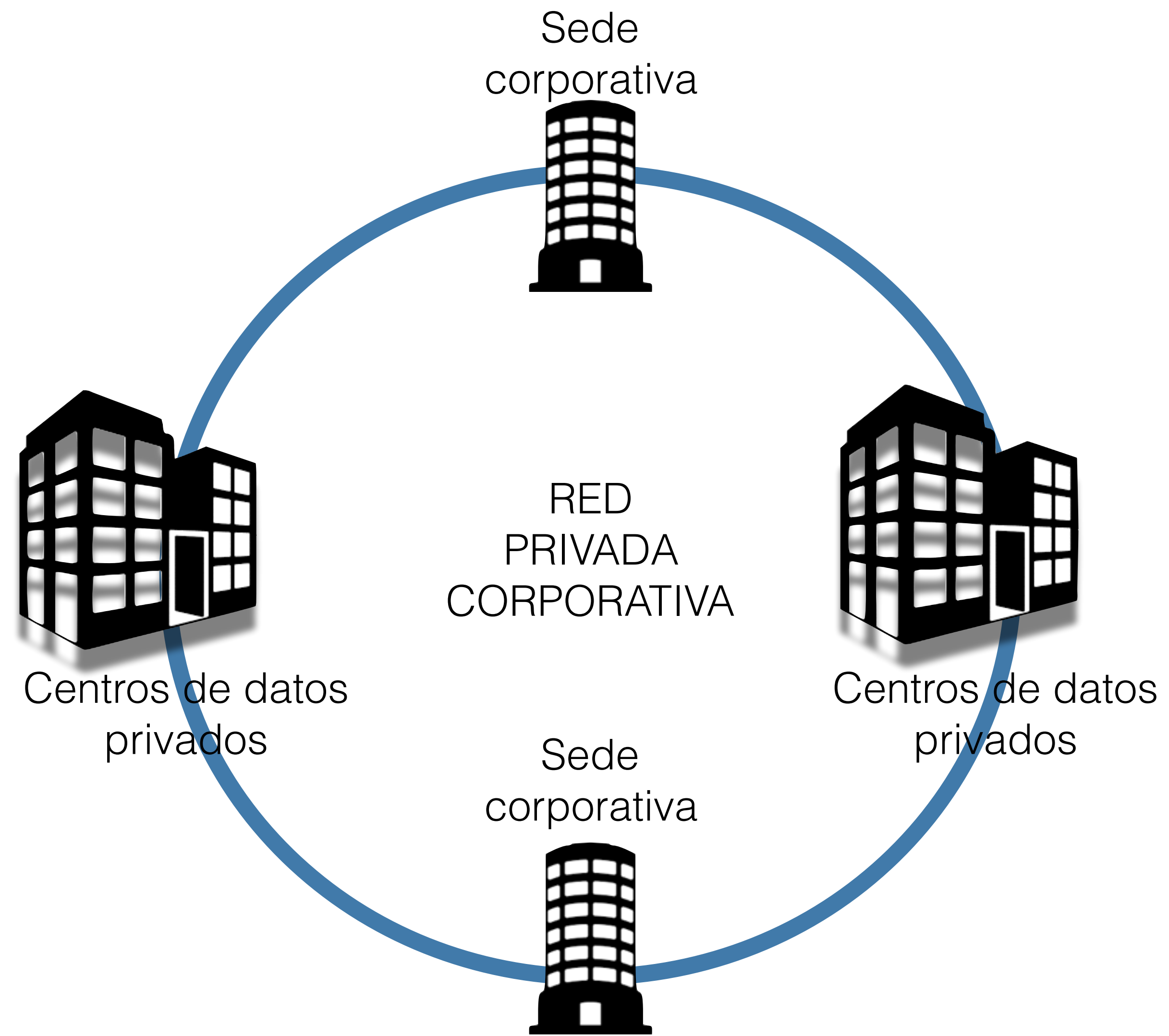
5 Flexible

Cloud + Veeam

Réplicas
+
Failover plan



5 Flexible

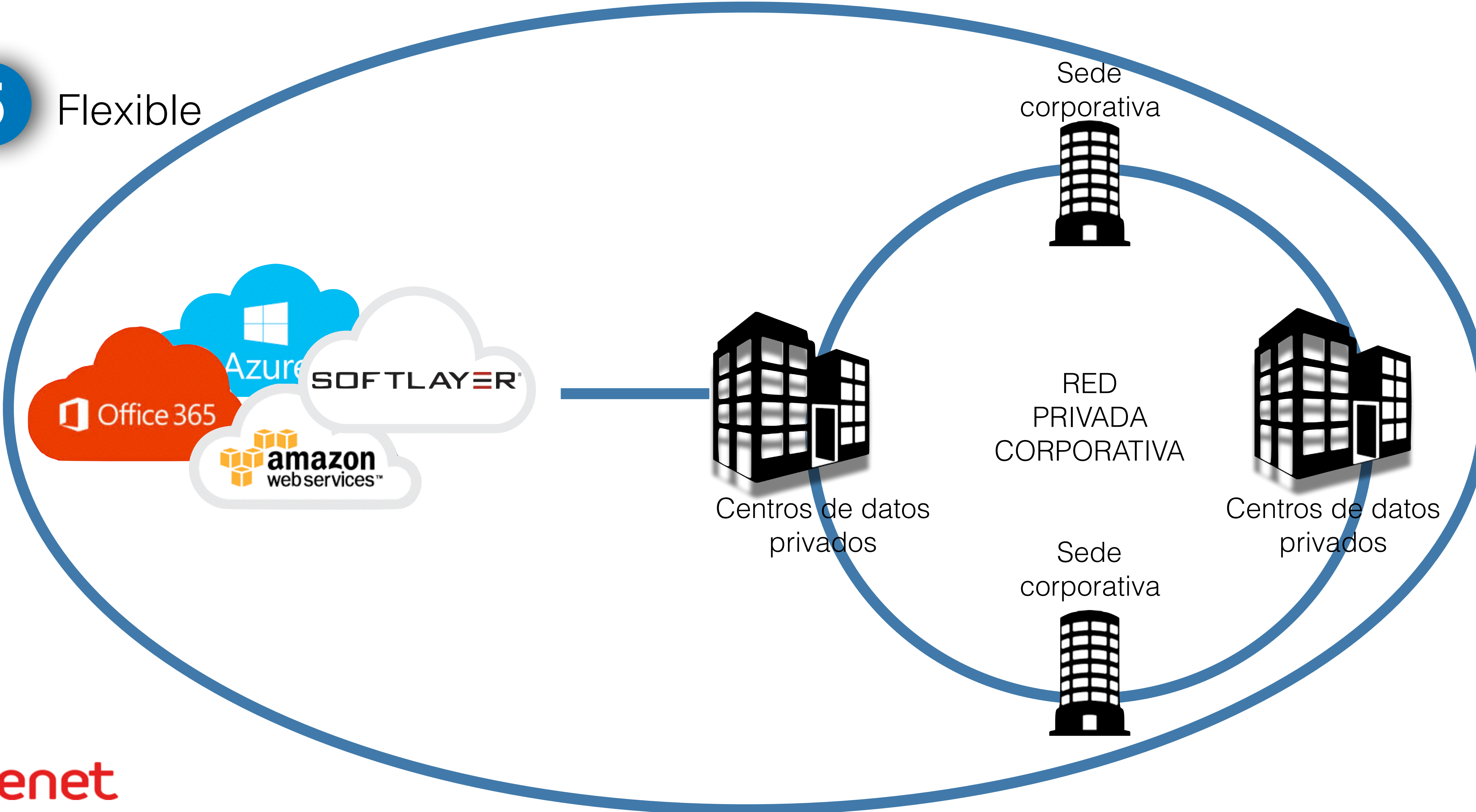


5 Flexible

Cloud Híbrida



5 Flexible





- Qué complementos adicionales puedo contratar

adicionales **Servicios**

6 Servicios adicionales



Centralita virtual



Cortafuegos de aplicaciones



Correo electrónico



Licenciamiento



Asesoramiento



Envíos de e-mail y SMSs



Seguridad Gestionada



Copias de Seguridad



Servicios de tránsito para correo



- Transparencia

Ventana
cliente

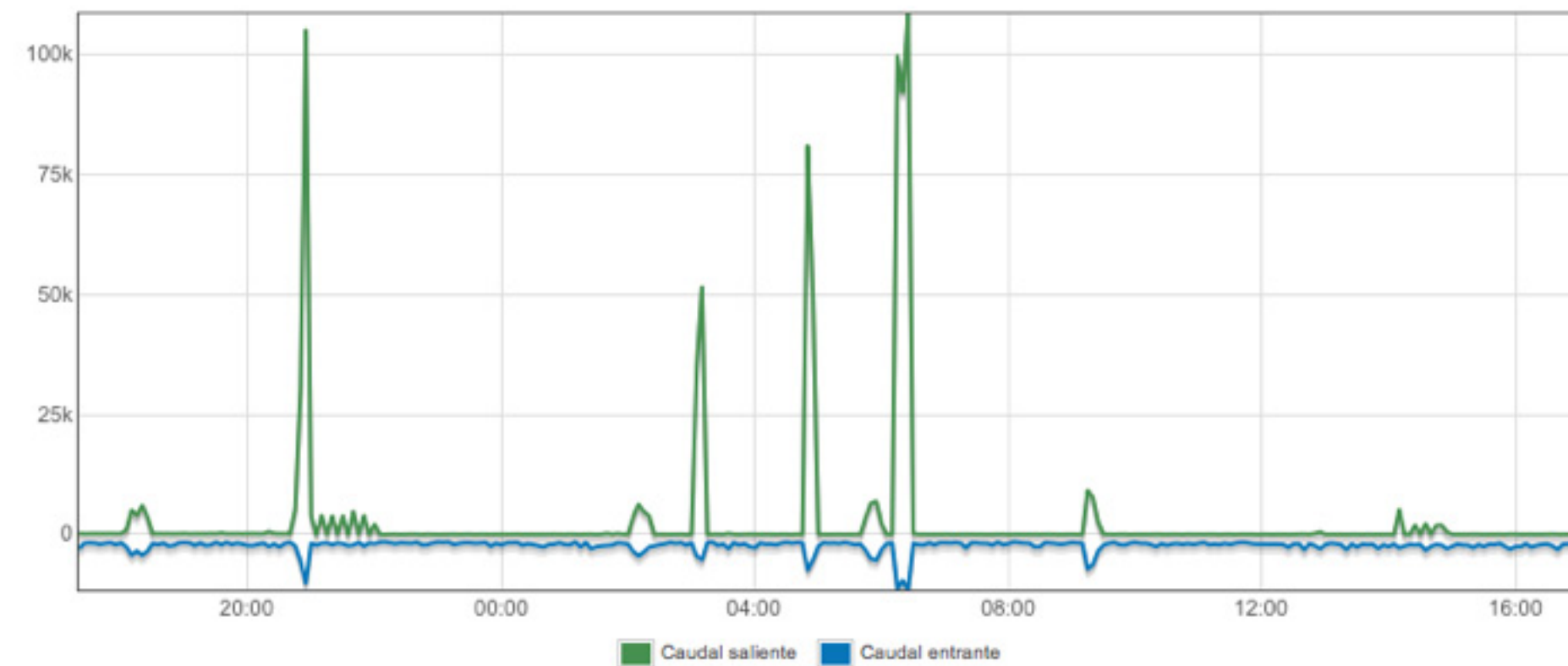
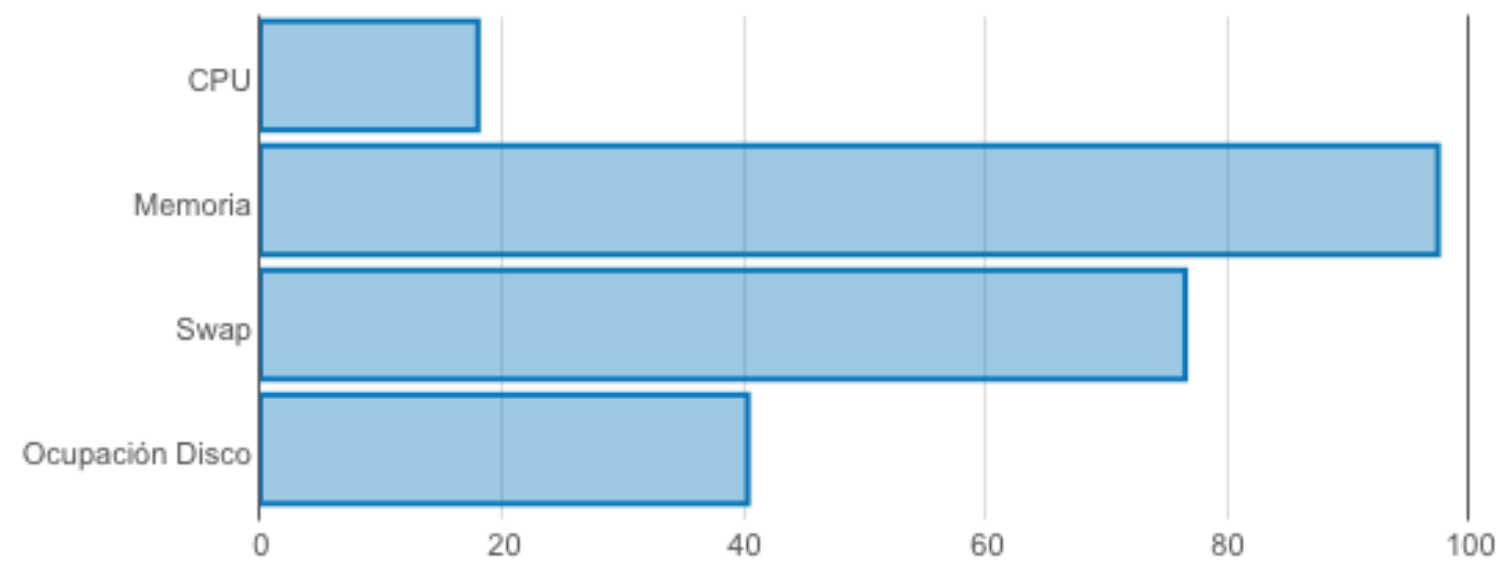
7 **Transparencia**



<https://ventana.sarenet.es>

7 Transparencia

Adm. Sarenet	CPUs	Memoria	Disco	S.O.	Servidor Web	Direcciones IPv4
HOU0708818	2	8,00 GB	200,00 GB	Windows 2008 R2	IIS	194.30.0.58/32



Gestión de recursos y monitorización

[CONFIGURACIÓN DE ALERTAS](#)

[NUEVO MONITOR](#)

7 Transparencia

Alerta: Ocupación Disco CERRAR x

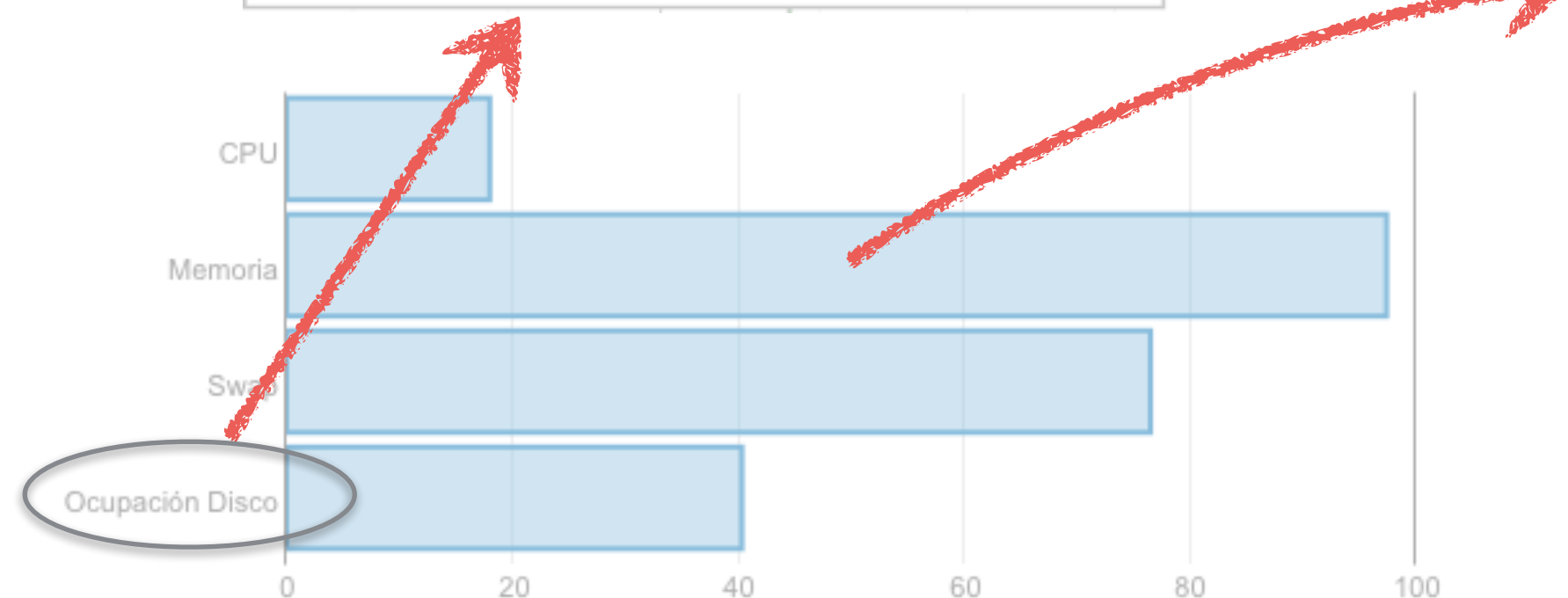
Total GB

Libre

Warning < GB

Critical < GB

CREAR **CANCELAR**



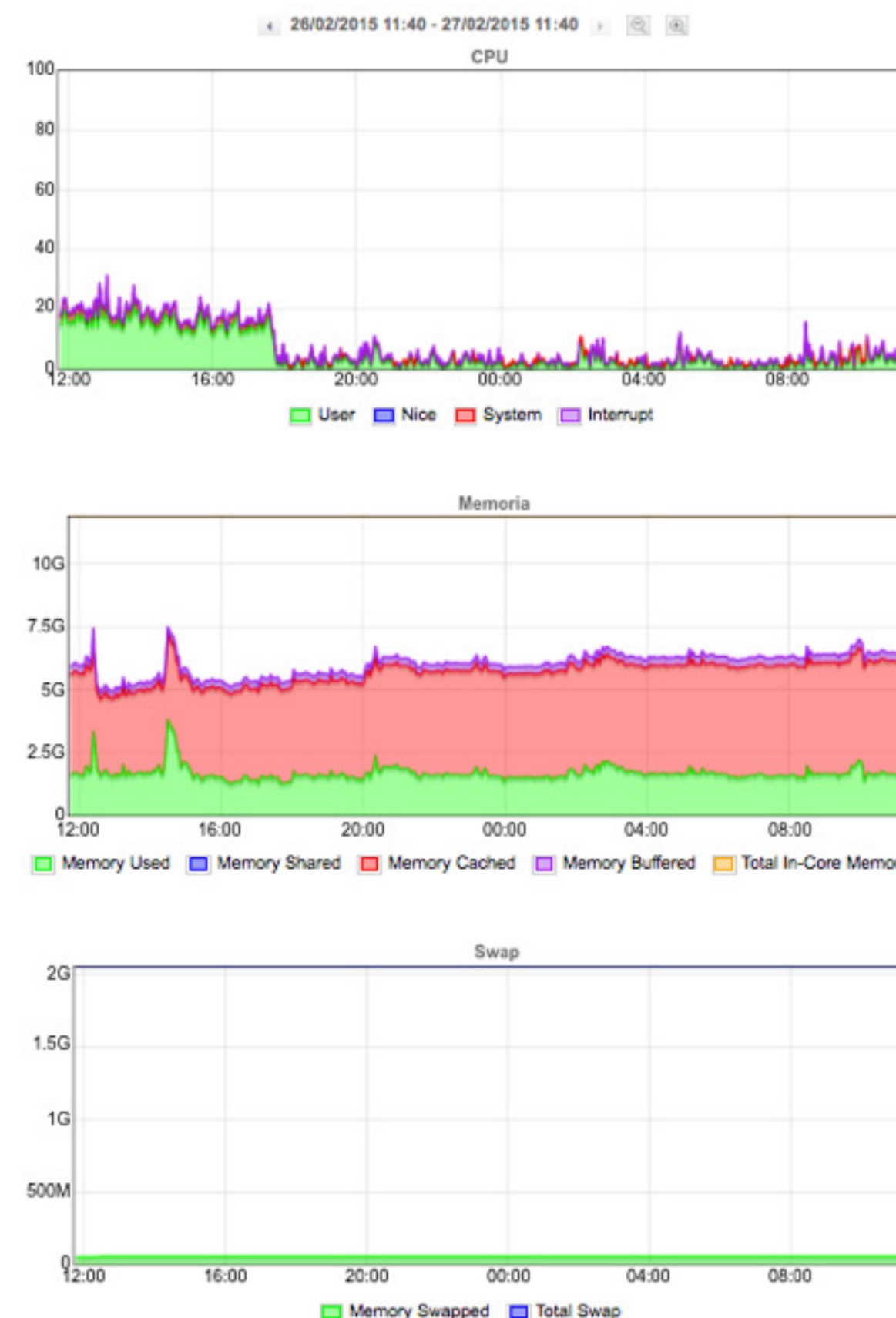
CONFIGURACIÓN DE ALERTAS

Modificar CERRAR x

Envío alertas a

Retardo alertas

MODIFICAR **CANCELAR**



(*) si hay varias gráficas en la barra se muestra la de valores mas altos

Monitorización del rendimiento

NUEVO MONITOR

El cliente puede configurar umbrales de generación de alertas e indicar una dirección de correo a la que se enviarán las notificaciones de alerta

7 Transparencia

PING BORRAR

Retardo (ms)

Disponibilidad (%)

27/02/2015 12:00 - 12:59

Fecha y hora	Estado	Respuesta del plugin
27/02/2015 12:03:23	OK	PING OK - Packet loss = 0%, RTA = 2.05 ms
27/02/2015 12:08:23	OK	PING OK - Packet loss = 0%, RTA = 0.73 ms
27/02/2015 12:13:23	OK	PING OK - Packet loss = 0%, RTA = 0.64 ms

Nuevo monitor CERRAR x

Tipo Sondeo FTP
 HTTP
 IMAP
 MySQL
 PING
 POP3
 SMTP
 SQLServer

IP:

Warning: s

Critical: s

Gestión: enet

CREAR **CANCELAR**

NUEVO MONITOR

FILTRAR

Monitor	Estado	Fecha y hora	Gestión
PING	ok	27/02/2015 10:53:18	Cliente BORRAR

El cliente puede crear monitores estandar de servicio

Servicios y seguimiento del SLA

1 **Infraestructura**

2 **Bajas latencias**

3 **Soporte cercano**

4 **Niveles de seguridad**

5 **Arquitecturas flexibles**

6 **Servicios adicionales**

7 **Ventana cliente**

“Ciberseguridad superficies de
ataque y mecanismos de
defensa”



Riesgo : Contingencia o proximidad de un daño

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización

Medidas de reducción de **probabilidad**

De eliminación — Impide que tenga lugar

Preventiva — Reduce las oportunidades de que el suceso ocurra

Disuasoria — Disuade al atacante

De monitorización — Atajan el incidente o aprenden

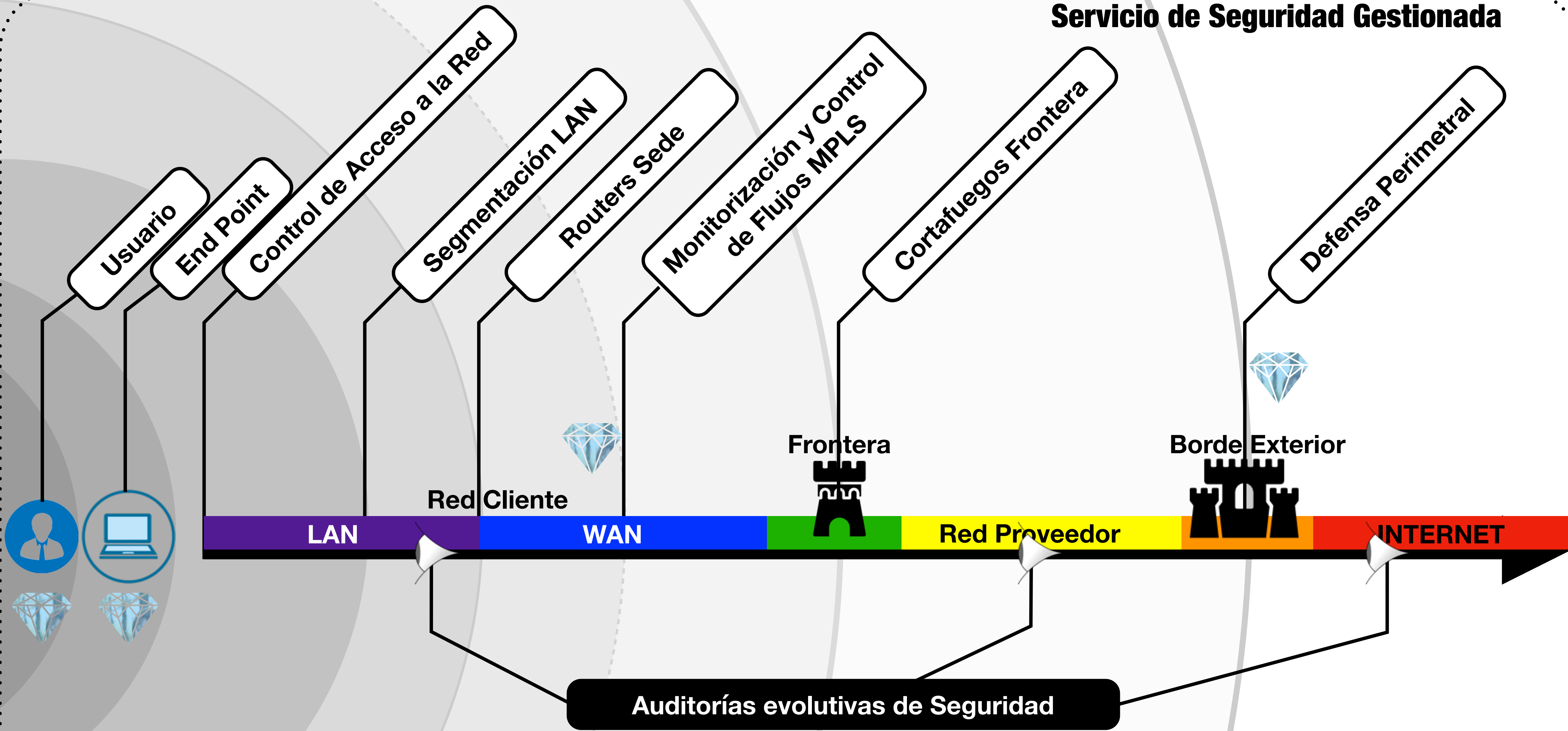
De detección — Ayudan a actuar rápidamente si el suceso ya ha tenido lugar

Medidas de reducción de **impacto**

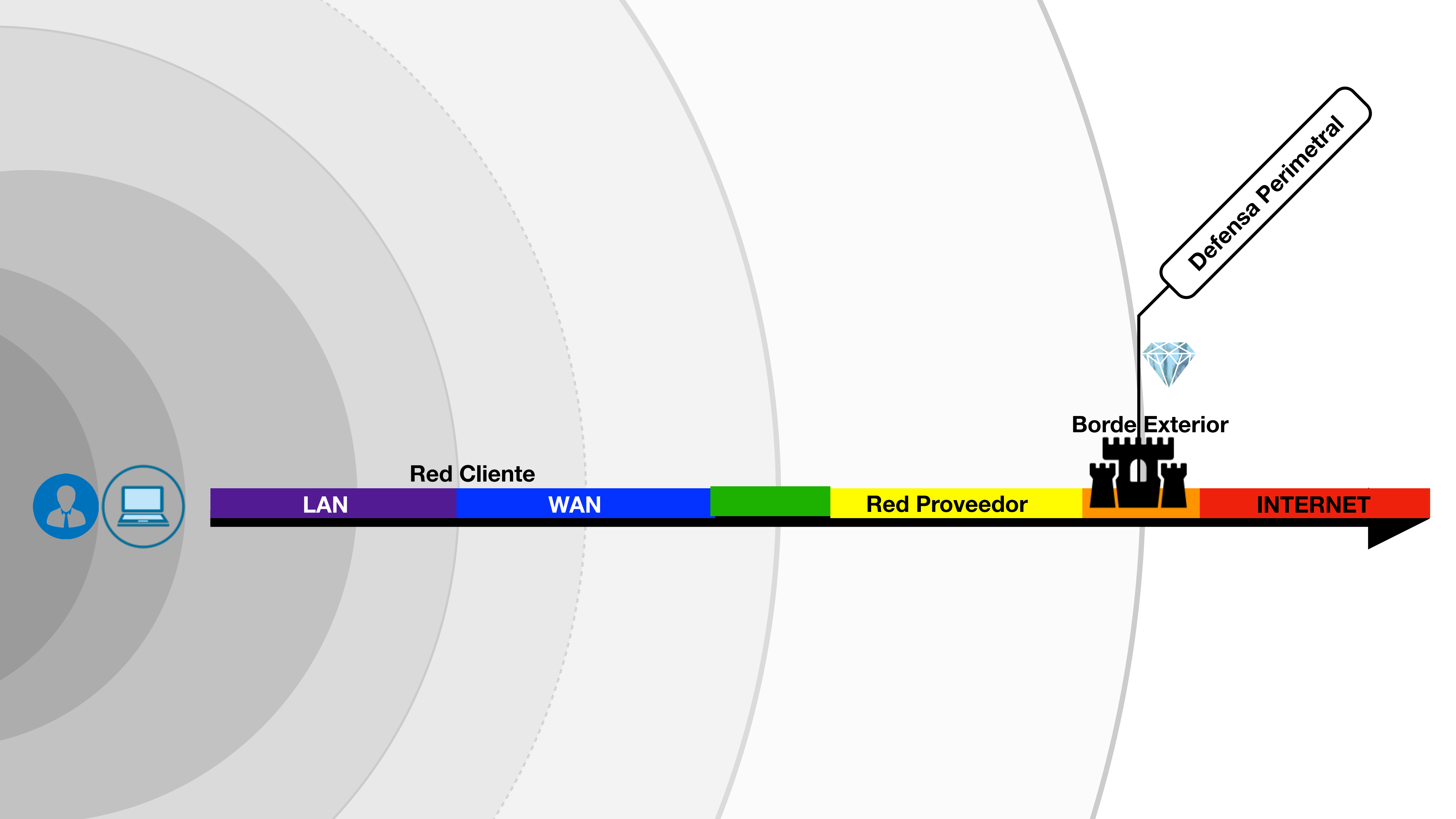
Minimizadoras — Cobertura de un seguro , cumplimiento de la legislación

Correctivas o Recuperativas — El incidente ocurre pero lo repara

Servicio de Seguridad Gestionada



Plan de Contingencia 
Cuando todo falla ...



LAN

Red Cliente

WAN

Red Proveedor

Borde Exterior



INTERNET



Defensa Perimetral