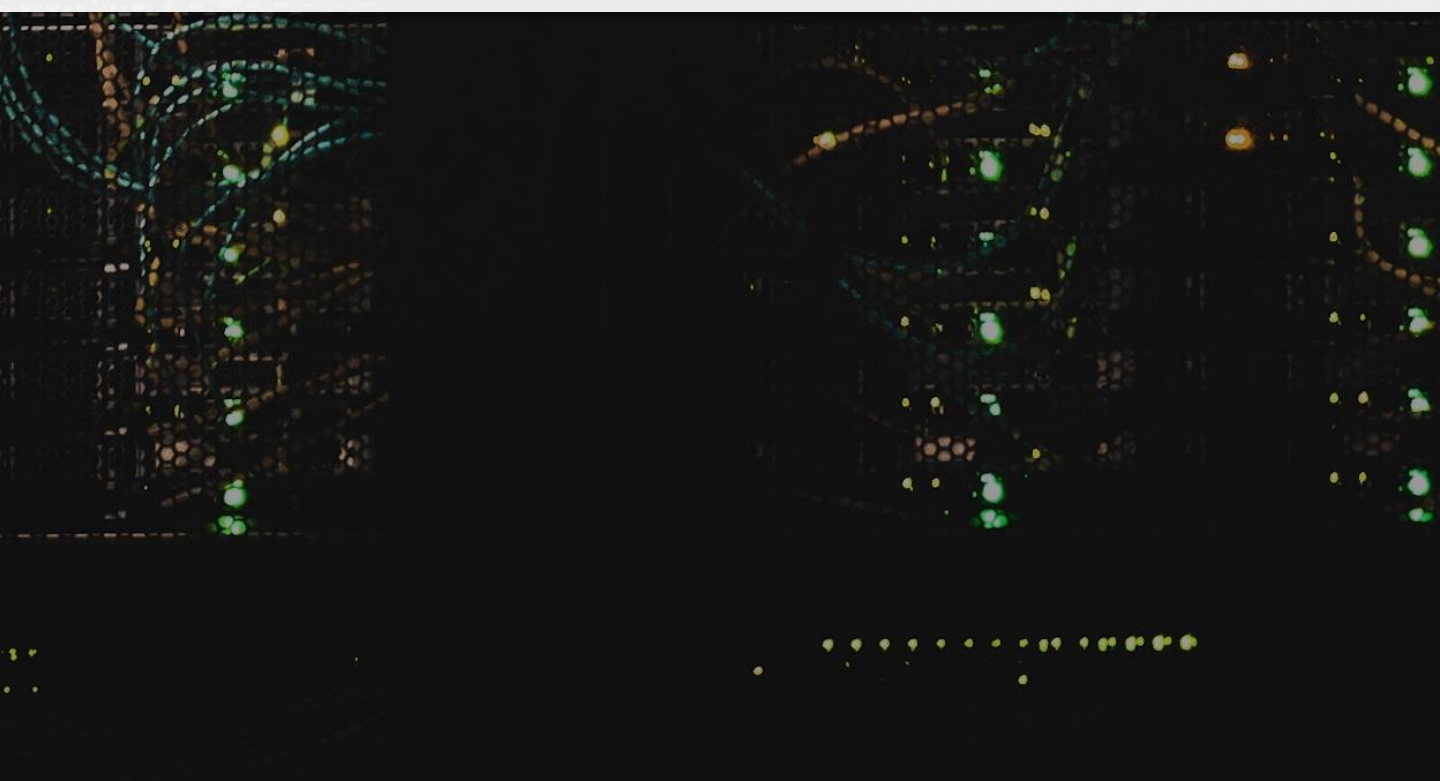
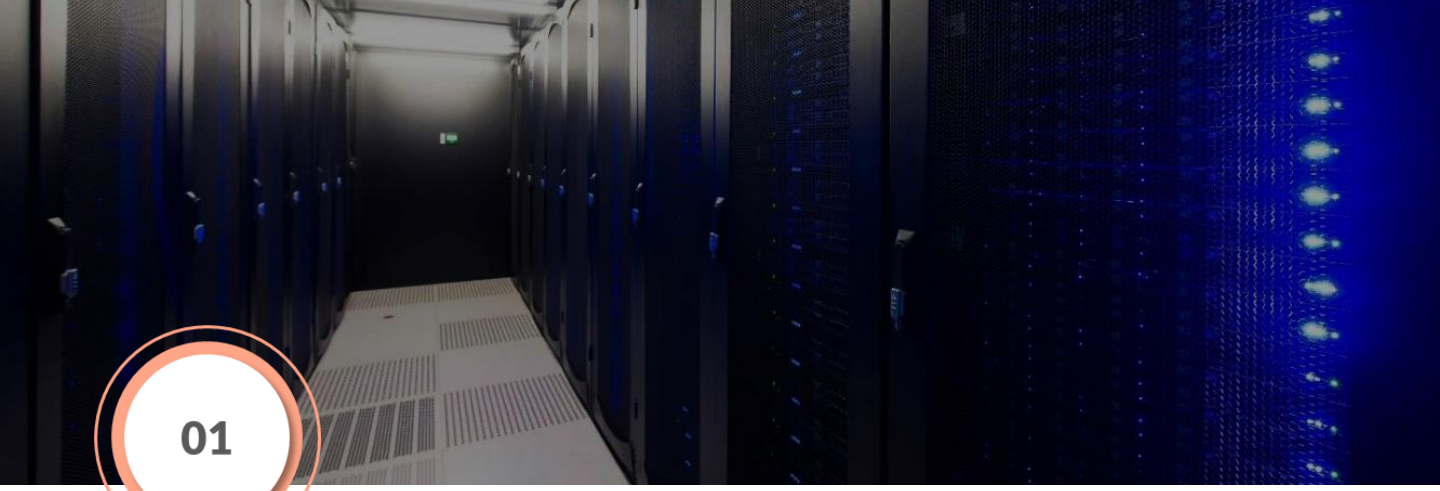
Infraestructura y Seguridad.

Los pilares de nuestros servicios y plataforma.





01

Nuestros Centros de Datos.

El lugar donde se alojan nuestros servidores.

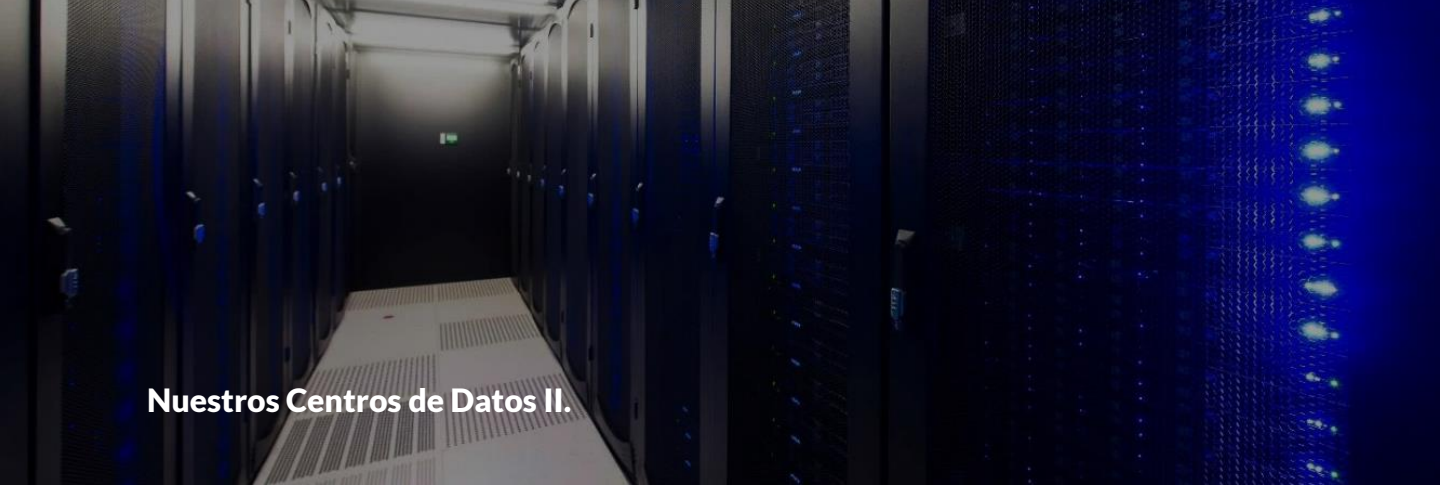
Alojamos nuestra plataforma e infraestructura en centros de datos de vanguardia que elegimos en base a estrictos criterios de seguridad, calidad, eficiencia y conectividad.

En concreto, nos alojamos en dos centros de datos (EU-MAD1) **Interxion** y (EU-MAD2) **Equinix** ubicados en Madrid. Ambos son considerados CPDs de referencia en España y probablemente estén entre los más avanzados construidos hasta la fecha. Tanto MAD1 como MAD2 son **centros de datos neutrales**, cuentan con una amplísima oferta de conectividad lo que nos permite ofrecer una mayor redundancia y disponibilidad en términos de conexión.

Asimismo, nuestros centros de datos disponen de estrictas medidas de seguridad relacionadas con el acceso físico, las condiciones ambientales y alimentación eléctrica, asegurando de esta manera que nuestro servicio tenga una calidad óptima.

Seguridad Física.

El acceso a los CPDs está controlado por personal de seguridad 24/7, dispone de video-vigilancia y está restringido, sólo se permite acceder bajo autorización previa.



Nuestros Centros de Datos II.

Medidas de Seguridad:

- Guardias de seguridad en horario 24h.
- Grabación continua 24/7.
- Detector de metales y torno de entrada para el acceso al Datacenter.
- Cámara en puertas de acceso y pasillos (externos e internos).

Control de Acceso:

- 5 capas de seguridad física (acceso al perímetro, edificio, salas técnicas, armarios rack…)

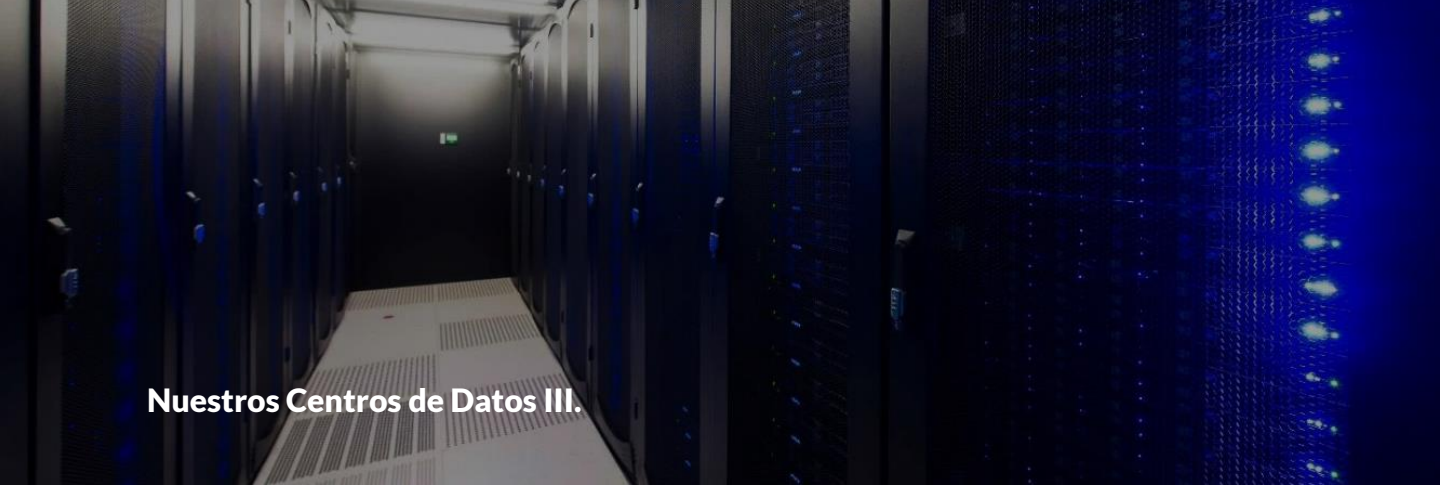
Controles ambientales.

Los equipos IT se mantienen y se monitorizan en **ambientes controlados** con SLAs de temperatura y humedad:

- Refrigeración continuada (24h).
- Equipamiento de Aire Acondicionado redundante.
- Temperatura 21°C y Humedad relativa del 50%.

Asimismo, todos los servidores están **protegidos contra incendios** a través de un sistema de supresión diseñado para extinguir cualquier fuego en segundos y sin residuos:

- Detectores de humo
- Inicio automático de sistemas de extinción
- Pulsadores manuales de emergencia start/stop en todas las salas.
- Detectores de tipo óptico e iónico con sistema VESDA
- Sistema de alarmas monitorizado 24/7.



Nuestros Centros de Datos III.

Energía.

Los centros de datos donde alojamos nuestra infraestructura están equipados con **conexiones redundantes a la red eléctrica** y **generadores diésel cinéticos** dimensionados para soportar las necesidades energéticas de todo el edificio y toda la infraestructura alojada en el mismo.

Certificaciones de nuestros Centros de Datos.

ISO 14001

Gestión medioambiental

ISO 22301

Continuidad del negocio

ISO 27001

Seguridad de la información

ISO 9001

Sistemas de gestión de calidad

ISO 50001

Gestión de la energía

02

Arquitectura Redundada.

Para asegurar la continuidad del servicio.

Se ha implementado una arquitectura 100% redundada con el fin de que un fallo concreto de un componente no afecte al funcionamiento normal de la plataforma y sus servicios.

Nodos de Computación.

Cada Host dispone de **doble fuente de alimentación**, cada una conectada a un segmento eléctrico diferente del centro de datos. Todos los equipos que conforman la infraestructura disponen, como mínimo, de **dos conexiones de red en alta disponibilidad** (LAG), asimismo, cada conexión de red va a un switch diferente, de manera que un fallo en un switch no suponga un corte de servicio. La **memoria RAM** utilizada en nuestros Hosts es **ECC**, lo que nos protege contra la corrupción de datos y posibles fallos.

Contamos también con **Hipervisores en N x 1,25**, de manera que contamos con espacio suficiente para soportar incluso el fallo de un 25% de los mismos. En caso de fallo en un hypervisor, los servidores alojados en el mismo se inician en otros hypervisores de forma automática.

Arquitectura Redundada II.

Almacenamiento.

Ofrecemos un almacenamiento en alta disponibilidad que combina el clustering basado en cabinas con el mirroring síncrono para proporcionar una recuperación transparente de los fallos. Con este sistema de almacenamiento redundado conseguimos:

- Mayor protección frente a fallos de hardware, red o instalaciones.
- Eliminar tiempos de inactividad y la gestión de cambios.
- Actualizar hardware y software sin interrumpir operaciones.

Red de Datos.

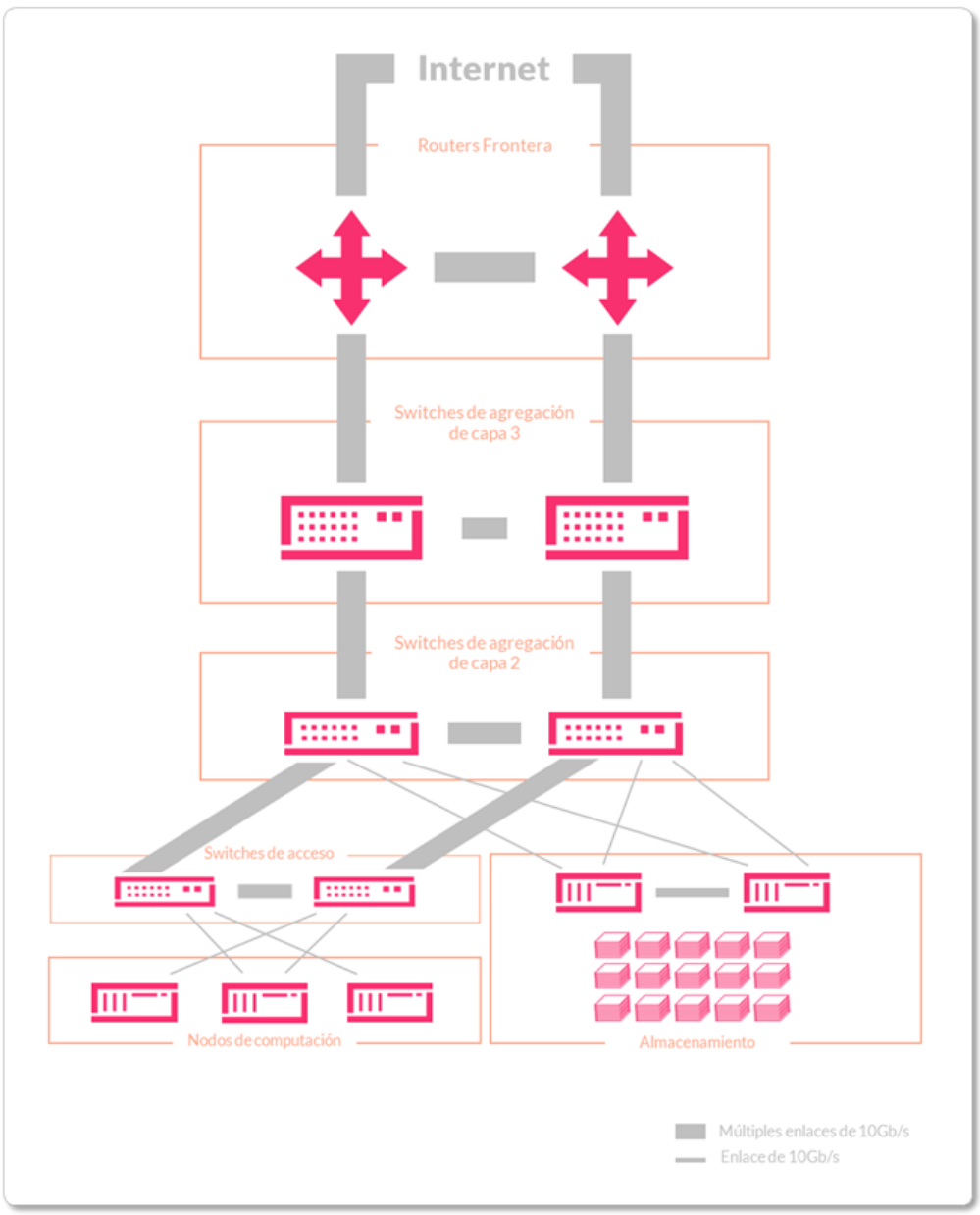
Disponemos de varios circuitos 10G con distintos proveedores de red del centro de datos, de forma que un problema en un proveedor nunca afecta a la conectividad.

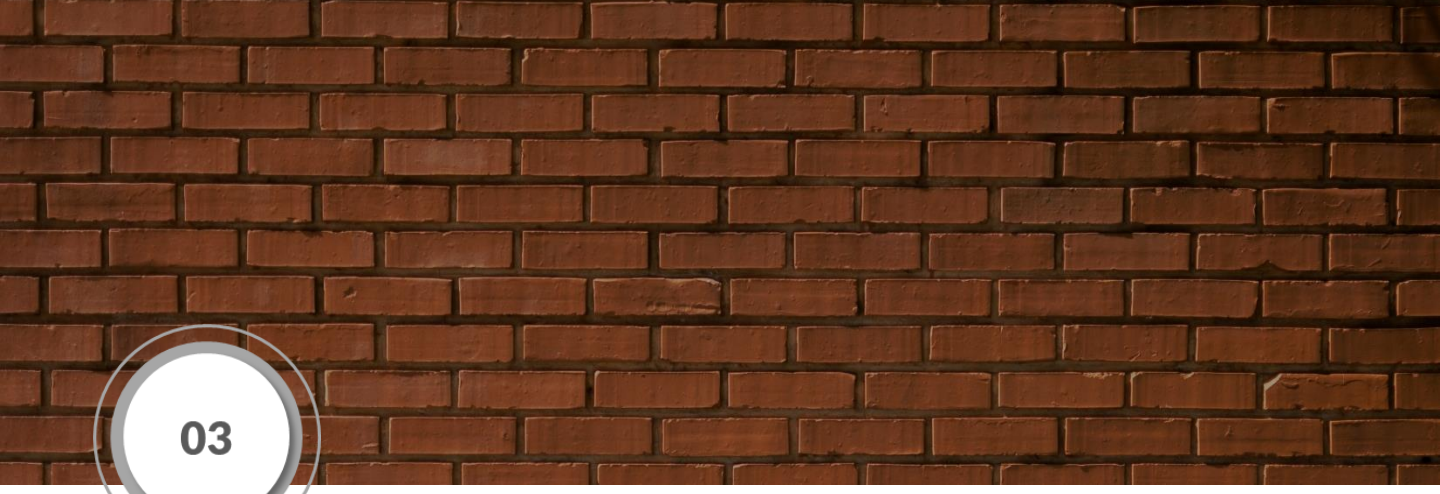
Los enlaces de agregación multi-chasis forman el esqueleto de la red dentro del CPD. Estos enlaces proporcionan **redundancia y escalabilidad** al mismo tiempo que evitan la formación de bucles.

Cada centro de datos cuenta con una pareja de routers frontera que facilitan la conexión con Internet y otros centros. Tras ellos se encuentran los switches de agregación de capa 3, los de capa 2 y, por ultimo, los de acceso, a los que se conectan los nodos de computación.

Arquitectura Redundada III.

Todos los switches lógicos se forman en pareja por redundancia y se conectan a todos los dispositivos a través de enlaces agregados multi-chasis, compuestos de 2 o más conexiones de 10 G o 40 G. Esta tipología **evita el riesgo de formación de bucles en la capa 2.**





03

Seguridad Perimetral.

Seguridad Perimetral y Anti DDOS.

La infraestructura tiene sistemas Anti-DDOS que previenen y filtran ataques de denegación de servicio, manteniendo los servidores siempre disponibles.

Nuestro sistema Anti-DDOS está estructurado en varias líneas de filtrado y detección lo que nos permite cribar y diferenciar ataques pequeños (de pocos cientos de Mbps) de otros ataques de miles de Gbps.

IDS/IPS.

Nuestro sistema de detección de intrusiones (IDS) es el programa que nos permite detectar los accesos no autorizados en nuestra infraestructura. Actúa evaluando la intrusión cuando esta toma lugar y genera una alarma. El IDS se acompaña por una herramienta de prevención de ataques denominada IPS, que rastrea de forma continua y proactiva del tráfico de red sospechoso o inusual.

Los IDS/IPS no pueden detener los ataques pos si solos y necesitan herramientas adicionales, como los Firewall, que ayuden en los procesos de bloqueo.

Filtrado y Bloqueo en Firewalls perimetrales.

Nuestros firewalls perimetrales analizan continuamente el tráfico que llega al nuestros centros de datos y bloquean el tráfico claramente malicioso de forma que no llegue a entrar en nuestro CPD. Paralelamente también revisan el volumen de tráfico que recibe cada máquina, de manera que se pueda tener un control sobre el tráfico recibido en cada servidor y detectar posibles ataques DDOS.

04

SSD y NVMe (NetApp).

Discos de estado sólido de alta gama.

Con el fin de asegurar la mayor disponibilidad sólo utilizamos discos de estado sólido (SSD y NVMes) de la más alta gama (Cabinas all-flash NetApp).

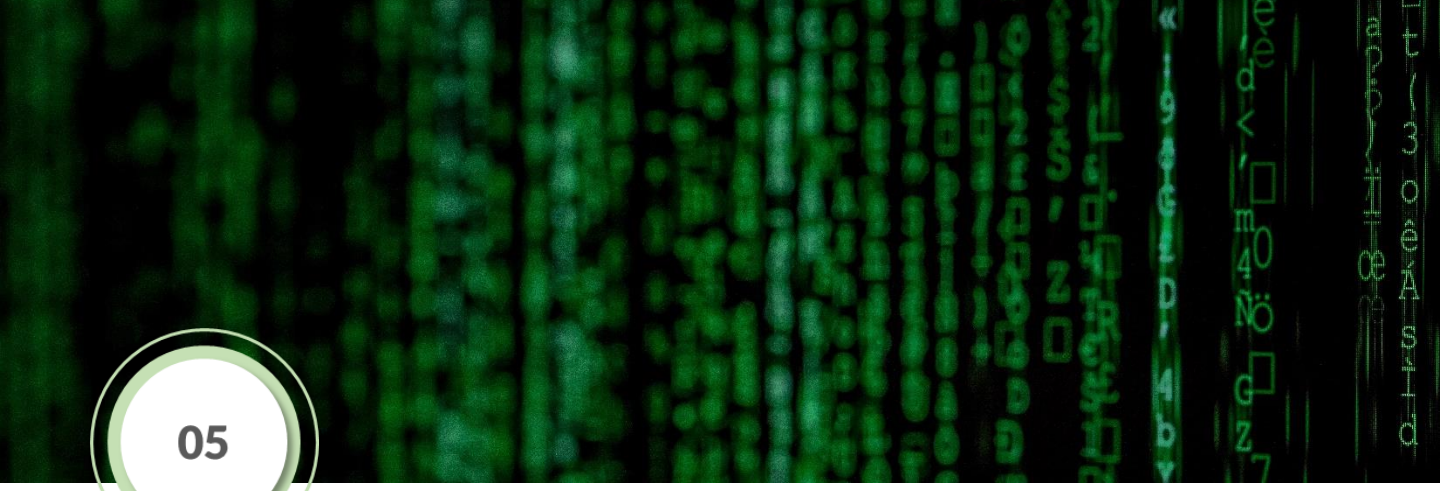
La utilización de este tipo de discos Enterprise busca entre otras cosas:

El mejor rendimiento de forma constante.

Con el uso de cabinas all-flash de NetApp buscamos ofrecer un rendimiento excelente de forma constante independientemente de la carga de trabajo a la que esté sometida el disco o el grado de ocupación del mismo.

La protección de los datos.

El sistema all-flash de NetApp proporciona una capa extra de protección sobre los datos de manera integrada. Replicación síncrona, cifrado incorporado, protección WORM o autenticación multifactor son algunas de las ventajas que presentan nuestras cabinas de almacenamiento y que nos ayudan a mantener los datos esenciales disponibles, protegidos y seguros.



05

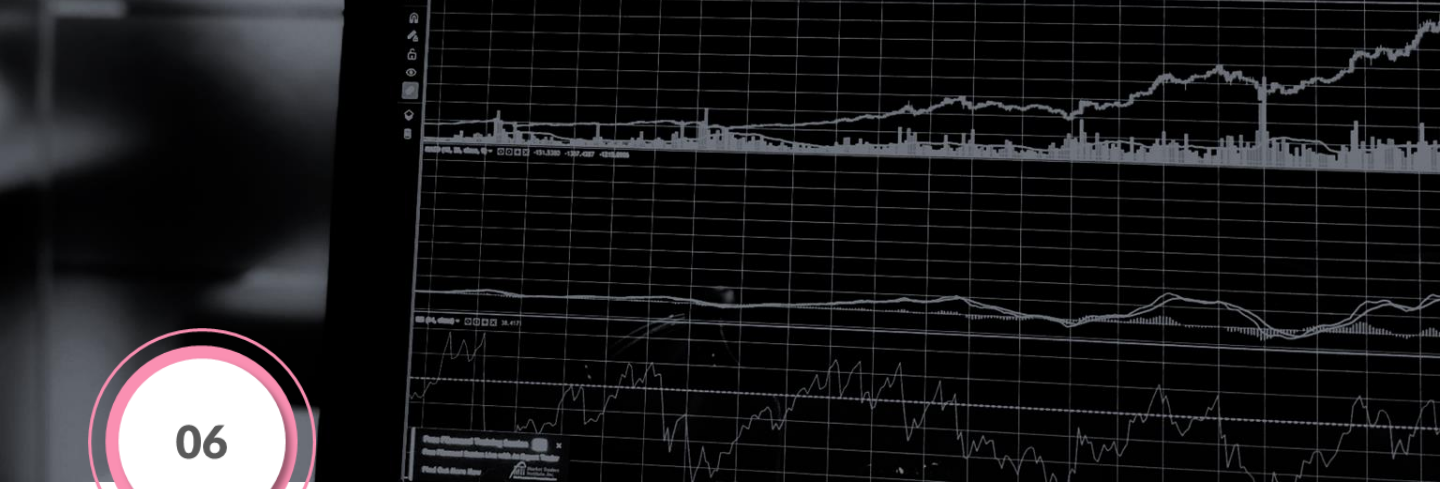
Autenticación y Encriptación.

Doble Autenticación.

Se ha reforzado el acceso a la plataforma y al portal con la posibilidad de implementar la doble autenticación (2FA) a través de un token de acceso generado en un dispositivo móvil. El token generado por este software es un número de seis dígitos que el usuario debe proporcionar además de su nombre de usuario y contraseña para acceder a los servicios.

La protección de los datos.

El encriptado es un **proceso de codificación de la información**. Este proceso convierte la representación de la información original (texto plano) en una forma alternativa conocida como texto cifrado o encriptado que sólo las partes autorizadas pueden descifrar. Los servicios utilizan diferentes sistemas de codificación y cifrado para la gestión y el transferencia de la información dando una capa más de protección frente a posibles hackeos.

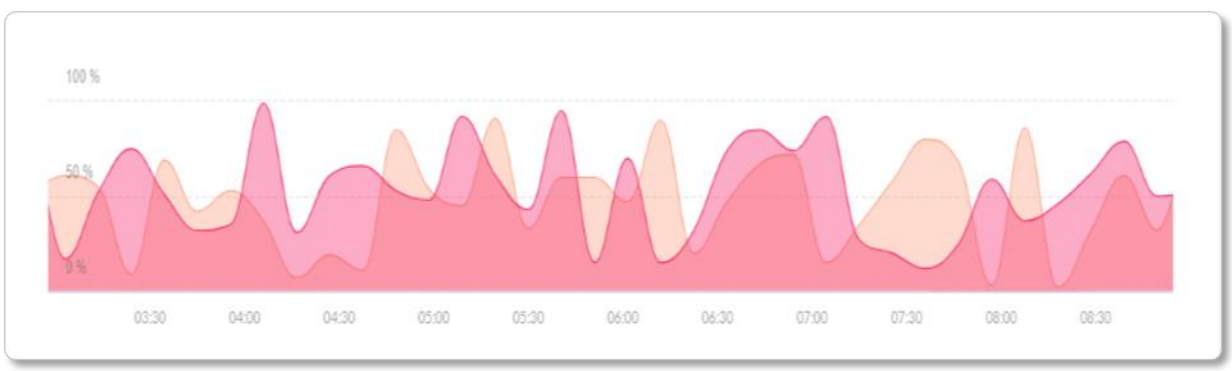


06

Monitorización 24/7.

Más métricas, mayor capacidad de respuesta.

Contamos con un **sistema de monitorización y alertas 24/7** que permite hacer un seguimiento continuo del estado del sistema al completo, tanto de la infraestructura como del resto de subsistemas, con el fin de asegurar la fiabilidad y estabilidad de los servicios y la plataforma. Esto nos permite evaluar el estado y el rendimiento del sistema al completo.



Nuestro sistema de monitorización 24/7 se basa en la recogida de métricas, procesamiento y visualización de datos junto con el establecimiento de reglas y alertas. El fin último es estar informado de posibles síntomas de riesgo o mal funcionamiento previa caída o *downtime*.

07

Backup y Restauraciones.

El backup es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida. Las copias de seguridad son extremadamente útiles en distintos eventos y usos. Lo sabemos y por eso establecemos diferentes políticas y tipos de backups en función del servicio.

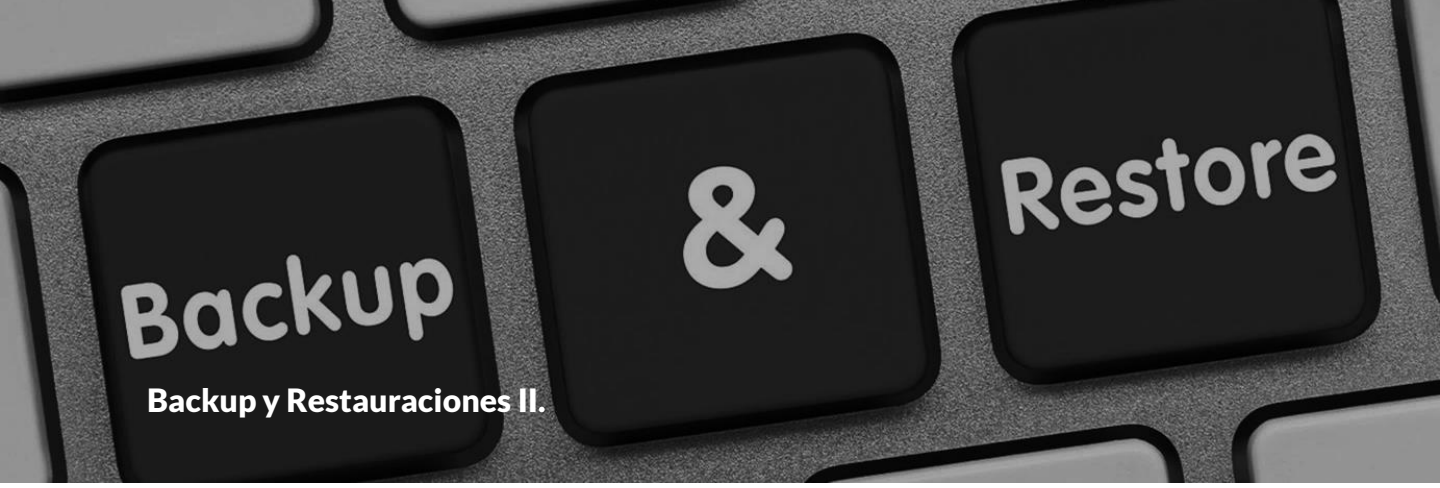
Política de backup en Escritorio Remoto y Servidores.

Los servicios de Escritorio Remoto y Servidores disponen de una política de backup basada en instantáneas de Disco (NetApp) con la siguiente programación fija y preestablecida :

- Cada hora [últimas 5 horas)
- Cada día [últimos 14 días a las 00:10]
- Cada semana [últimas 8 semanas – domingos a las 00:15]

Adicionalmente, los usuarios podrán realizar copias de seguridad, manuales o mensuales, a través de la plataforma de orquestación IaaS, basadas en snapshots de disco. La programación mensual tiene una retención máxima de hasta 24 meses.

La restauración de backups está disponible online en su sección correspondiente dentro de la plataforma.



VSS (Volume Shadow Copy Service) (opcional):

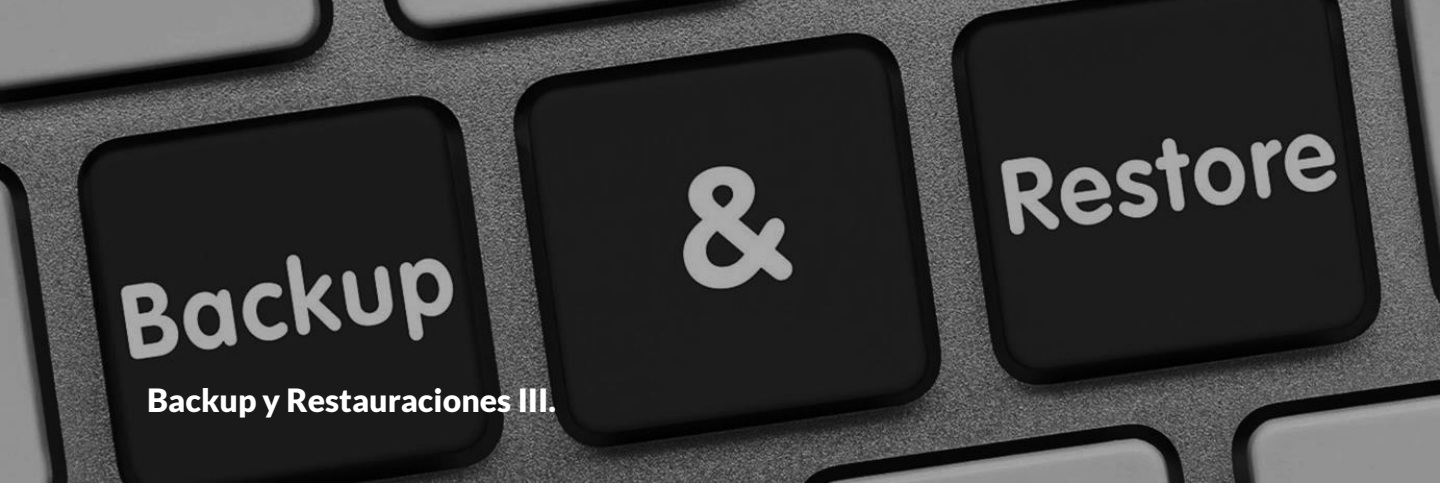
Shadow Copy es una tecnología que permite crear copias de seguridad, snapshots de archivos o volúmenes del servidor de forma oculta permitiendo su realización incluso cuando éstos están en uso.

Se pone a disposición de los usuarios este tipo de copias de forma opcional, necesitando de una activación previa. Por defecto, está configurado realizando 2 al día, de los últimos 14 días.

Réplicas en Repositorio S3.

El sistema de almacenamiento de objetos replica cada objeto **en 3 discos distintos ubicados en 3 servidores distintos**. La política establecida mantendrá por defecto, al menos, una de las copias **en un Centro de Datos diferente.**

El servicio de Repositorio S3, además, cuenta con una funcionalidad de versionado que se puede activar desde la suscripción de la plataforma en cualquier momento. De esta manera que se pueden recuperar versiones anteriores a través del Protocolo S3.



Política de backup en Almacenamiento en la nube.

El servicio de Almacenamiento en la nube tiene una política de backup prestablecida y común para todos los usuarios a nivel a granular y de forma encriptada.

La **política de Copias de Seguridad** se detalla a continuación:

Frecuencia de Backup: 1 copia diaria.

Retención de las Copias de Seguridad:

- Cada hora [últimas 5 horas)
- Cada día [últimos 14 días a las 00:10]
- Cada semana [últimas 8 semanas – domingos a las 00:15]

Por otro lado, se dispone de **instantáneas de volumen VSS** que permiten restaurar versiones anteriores de ficheros y carpetas.

Programación de Snapshots: Todos los días [12:00 y 18:00]

Retención de Snapshots:

- 64 instantáneas.

Sistema de recuperación de datos instantáneo y online disponible para cualquier usuario.

08

Custodia de datos [Stackscale].

Custodia de datos con empresa independiente.

Con el fin de incrementar, aún más, nuestra seguridad y tratar de blindar la información de todos los entornos alojados, hemos llegado a un acuerdo **con Stackscale**, empresa independiente, especializada en cloud privado y ubicada en España, **para que almacene una de nuestras copias de seguridad en sus sistemas de almacenamiento.**

De esta manera, damos un paso más con el fin de garantizar la disponibilidad de la información en caso de ataque y añadiendo una capa más de seguridad. Así mismo, es importante destacar, que todo este sistema de copias se ha realizado bajo el riguroso estándar que establece la Ley de Protección de Datos (RGDP) con respecto a la confidencialidad de los mismos.

09

Service Level Agreement.

DISPONIBILIDAD	COMPENSACIÓN
99,99>D>=99,72	10% de cuota mensual
99,72>D>=99,44	20% de cuota mensual
99,44>D>=99,16	30% de cuota mensual
D<99,16	40% de cuota mensual

Disponibilidad (D) = [(Horas mes – Horas indisponibilidad)/ Horas mes] x 100

No computan para el cálculo de la disponibilidad del acceso (SLA):

- Causas ajenas a nuestro control y causas de fuerza mayor.
- Indisponibilidad del panel de auto-gestión.
- Tiempos de indisponibilidad a consecuencia de fallos en el software que reside en las máquinas virtuales.
- Virus y ataques informáticos que ocasionen la imposibilidad total o parcial de la prestación de los servicios.

Tus datos están seguros.