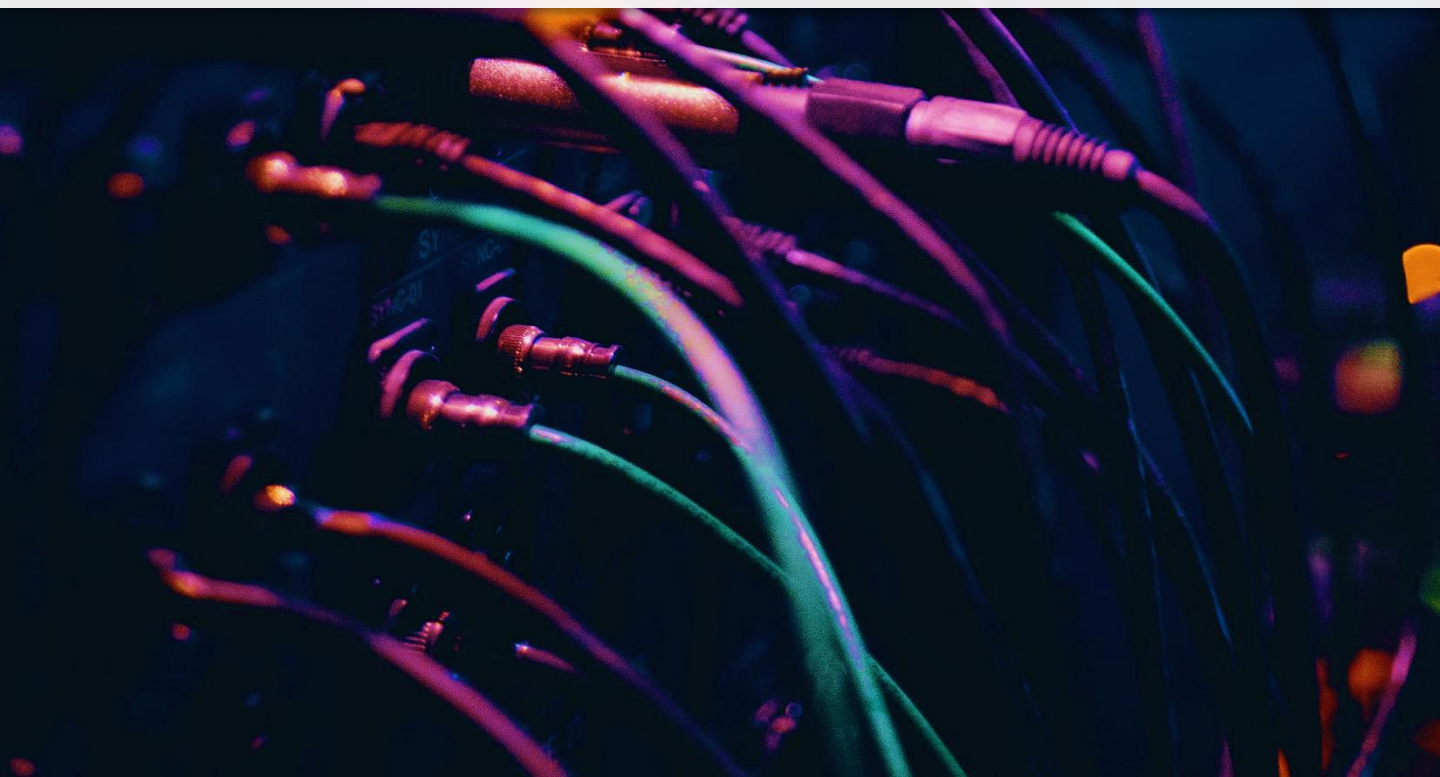
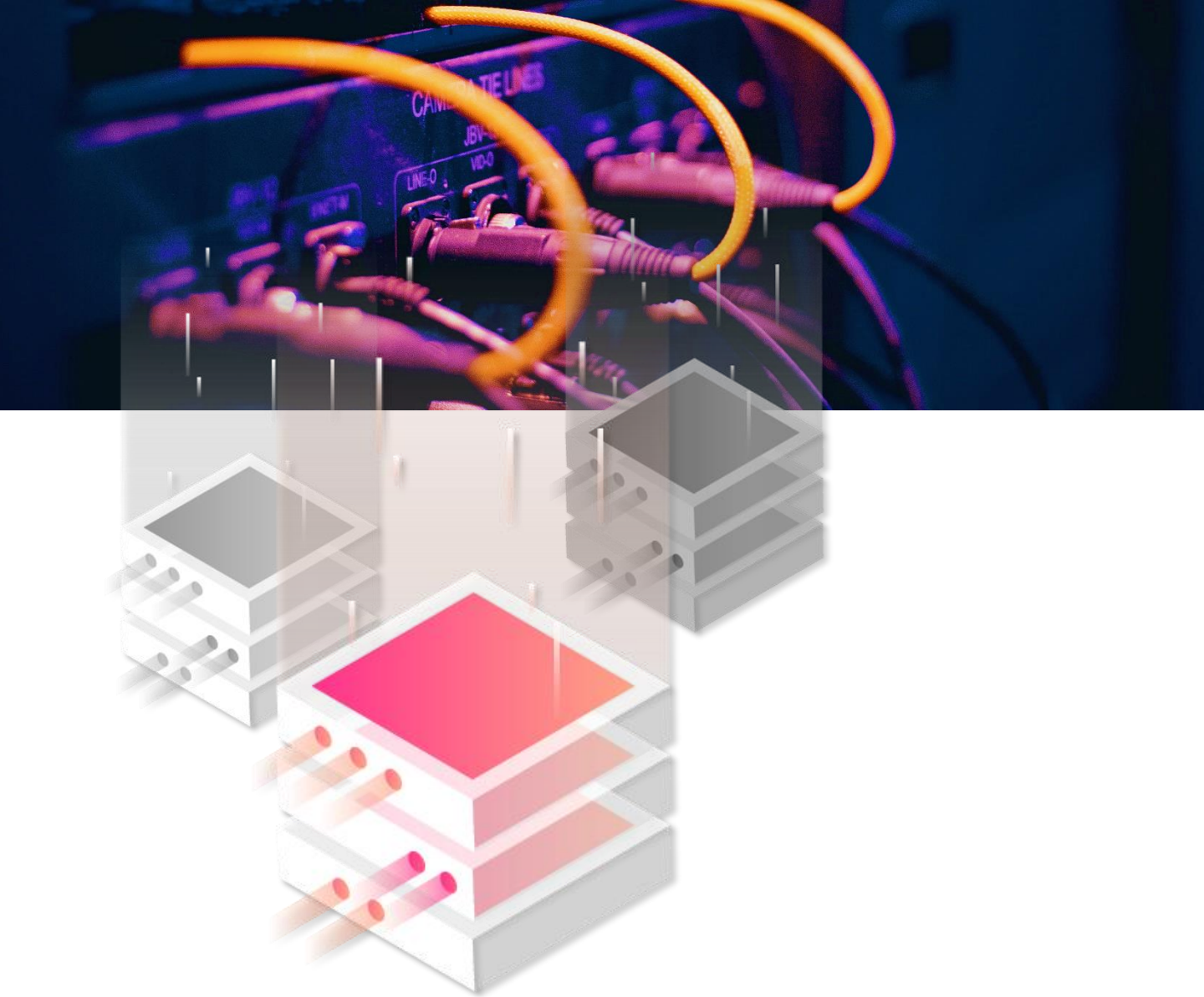




Servidores.

Alojamento de aplicações críticas de forma segura e acessível.





Servidores.

Aloje aplicações críticas de forma segura e acessível.

Servidores é um ambiente Cloud Datacenter dimensionado para o alojamento de aplicações críticas, de forma segura e económica, devido à automatização de processos e à gestão simplificada.

Não se trata de um VPS! Este serviço inclui, além da máquina virtual e do disco, uma **rede privada**, **router** e **firewall virtual** dedicados, assim como uma **política rigorosa de backups** pré-configurados.

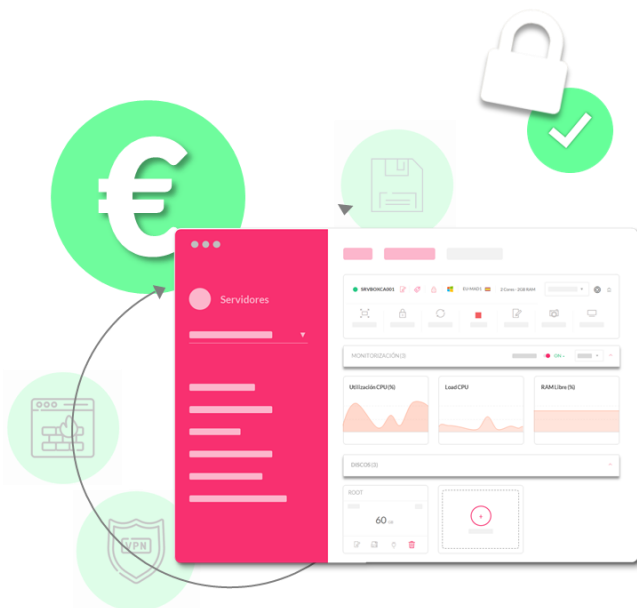
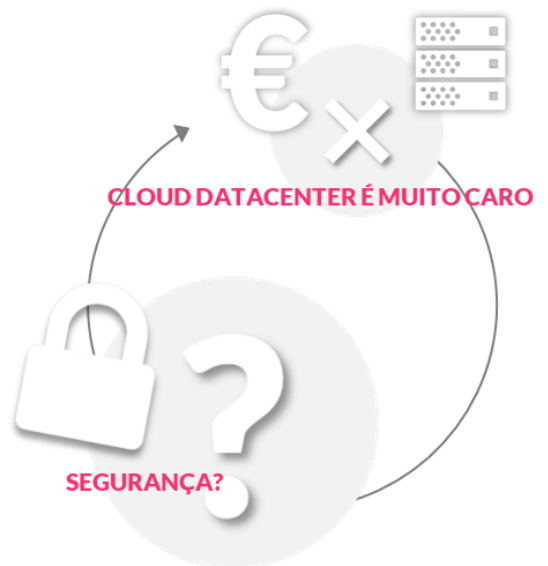
A segurança é uma das nossas prioridades porque sabemos que é uma das preocupações das micro e pequenas empresas.



O Problema Principal.

Os serviços de *Cloud Datacenter* não estão pensados para as micro e pequenas empresas. O preço importa.

A realidade é essa Os ambientes *Cloud Datacenter* são muito caros para as PMEs. É por isso que muitas empresas de TI vendem servidores VPS, muitas vezes sacrificando a segurança.



A Nossa Solução.

Servidores é uma solução *Cloud Datacenter* acessível, fácil de gerir e segura.

Servidores é um serviço *Cloud Datacenter* focado na segurança e que permite alojar ambientes críticos a um preço acessível para qualquer micro ou pequena empresa.



Vantagens do serviço Servidores.

Segurança, Escalabilidade e Simplicidade: os grandes benefícios do serviço.

FOCO NA SEGURANÇA.

Trabalhamos em *data centers* neutros e com os mais altos padrões de segurança (ISO 27001), e temos **armazenamento distribuído**.

Além disso, os nossos servidores **incluem backups pré-configurados por defeito** para que no máximo se perca uma hora de trabalho. Além disso, todos eles possuem uma rede privada, um *router* e uma *firewall* virtual dedicados.



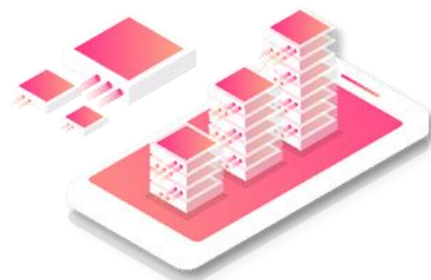
FÁCIL DE GERIR.

Contar com assistentes de implementação e processos de configuração assistida (para VPN, regras de firewall, etc.) ajuda-nos a gerir melhor, a criar ambientes mais seguros e ser mais eficientes em todos os processos. Em suma, a ser **mais competitivos**.



ESCALABILIDADE TOTAL.

Aumente e diminua recursos **de acordo com as necessidades**. Reajuste em tempo real as configurações de disco, CPU ou RAM com base naquilo que precisa e dimensione os seus negócios sem restrições.





Ambientes eficientes e mais seguros.

Somos mais eficientes na gestão dos seus servidores.

Dispomos de uma plataforma que nos torna mais eficientes na gestão, configuração e segurança dos sistemas com que trabalhamos, o que se traduz em rapidez, melhor preço e segurança.

INSTALAÇÃO AUTOMÁTICA DE APLICAÇÕES.

Sabemos que muitas PME's usam o mesmo software e aplicações, por isso temos processos automatizados para simplificar as implementações e configurações iniciais.

CONFIE NO SEU VPN.

Desfrute de túneis site a site e de acesso remoto de forma rápida e sem complicações. Deixe-nos aumentar a sua segurança em dois passos as e blindar conexões.

VLAN, FIREWALL E ROUTER VIRTUAIS DEDICADOS.

A segurança e estabilidade dos nossos serviços é uma prioridade. É por isso que todos os nossos servidores possuem rede privada, router e firewall dedicados.

BACKUPS PRÉ-CONFIGURADOS POR DEFEITO.

O serviço inclui cópias de segurança por defeito, em diferentes Data Centers localizados em Espanha, o que lhe garantirá uma perda de informação de, no máximo, uma hora.

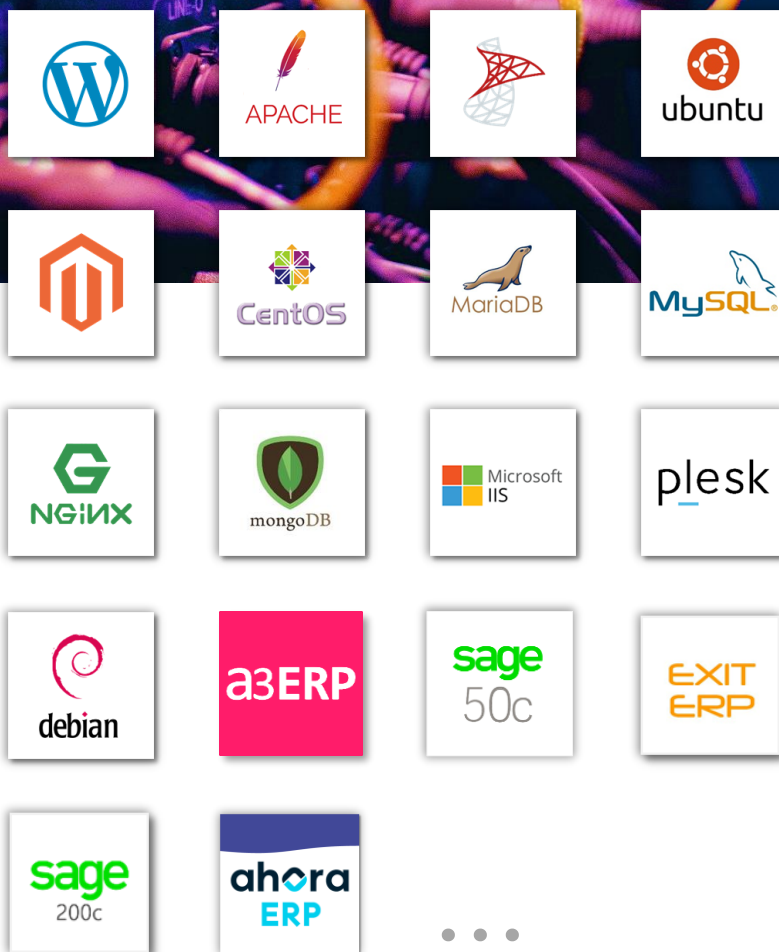
01

02

03

04

01

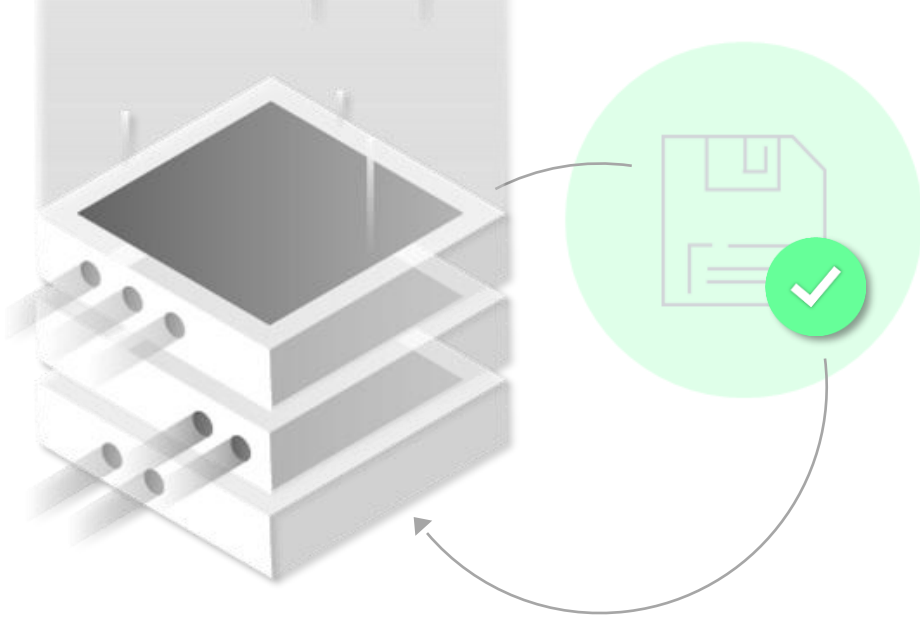


Instale qualquer tipo de software.

Compatibilidade e adaptação a diferentes softwares.

Sabemos que cada empresa é diferente e que cada software e sistema operacional também. Por esta razão, o serviço Servidores foi desenhado e otimizado tendo em conta a compatibilidade e adaptação a diferentes ambientes, programas e SO.

Seja qual for o software a ser instalado, será muito provavelmente compatível com o serviço Servidores. Wordpress, Magento, MySQL, Sage 200, Ahora ERP, Exit ERP, A3 ERP, MS SQL, são apenas alguns dos softwares mais instalados atualmente nos nossos servidores.



Política rigorosa de cópias de segurança pré-configuradas.

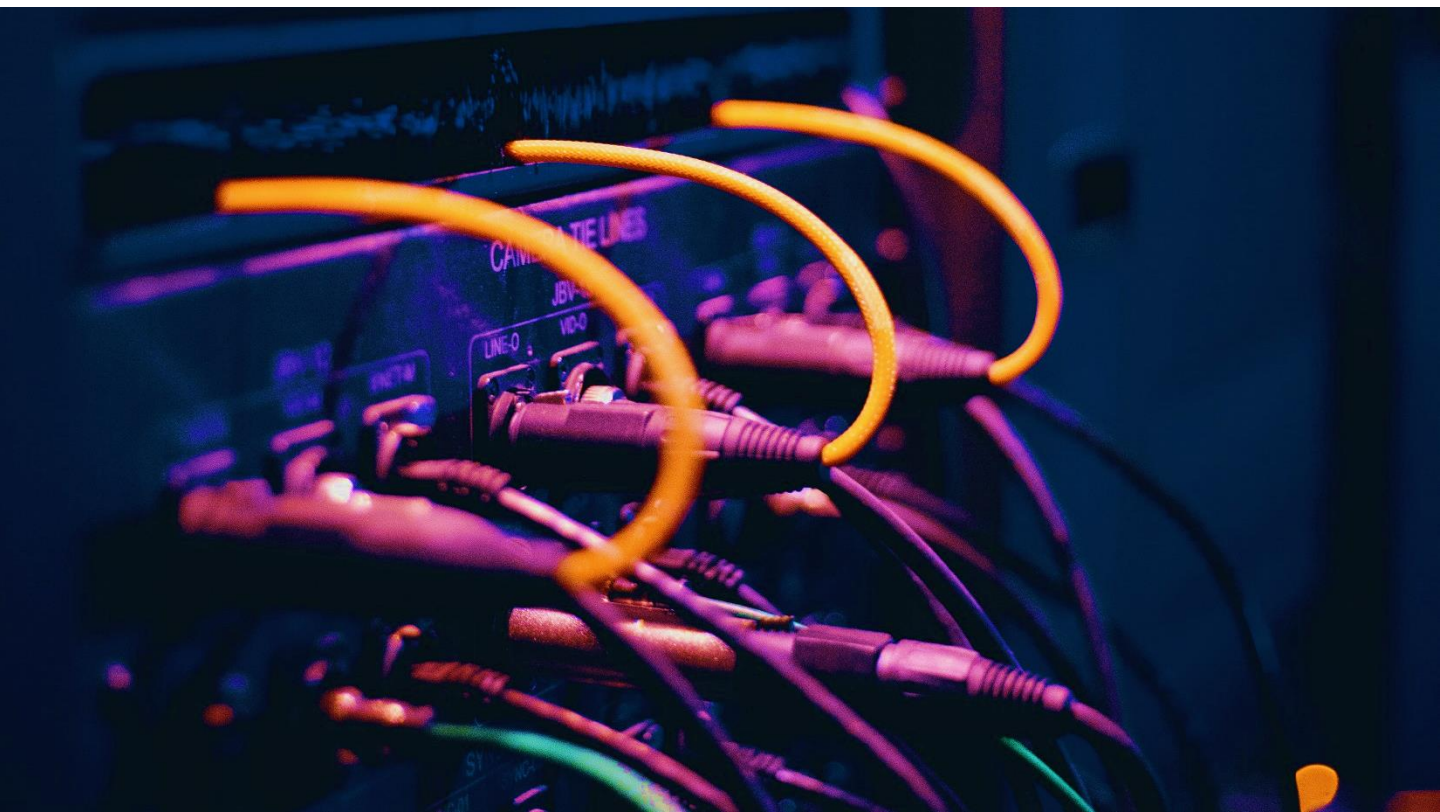
Perca, no máximo, uma hora de trabalho.

Todos os servidores são implementados com *backups* pré-configurados por defeito e incluídos no preço. A configuração das cópias de segurança é completamente modificável, embora o serviço Servidores seja sempre implementado com um processo de *backup* que consiste em instantâneos de disco (NetApp) agendados:

- Todas as horas [retenção últimas 5 horas]
- Todos os dias [retenção últimos 14 dias às 00:10]
- Todas as semanas [retenção últimas 8 semanas – domingos às 00:15]

Esta política de *backups* ajuda a garantir a segurança da informação, para que se perca no máximo **uma hora de trabalho**. Além disso, o restauro dos servidores está disponível online e acessível a qualquer momento.

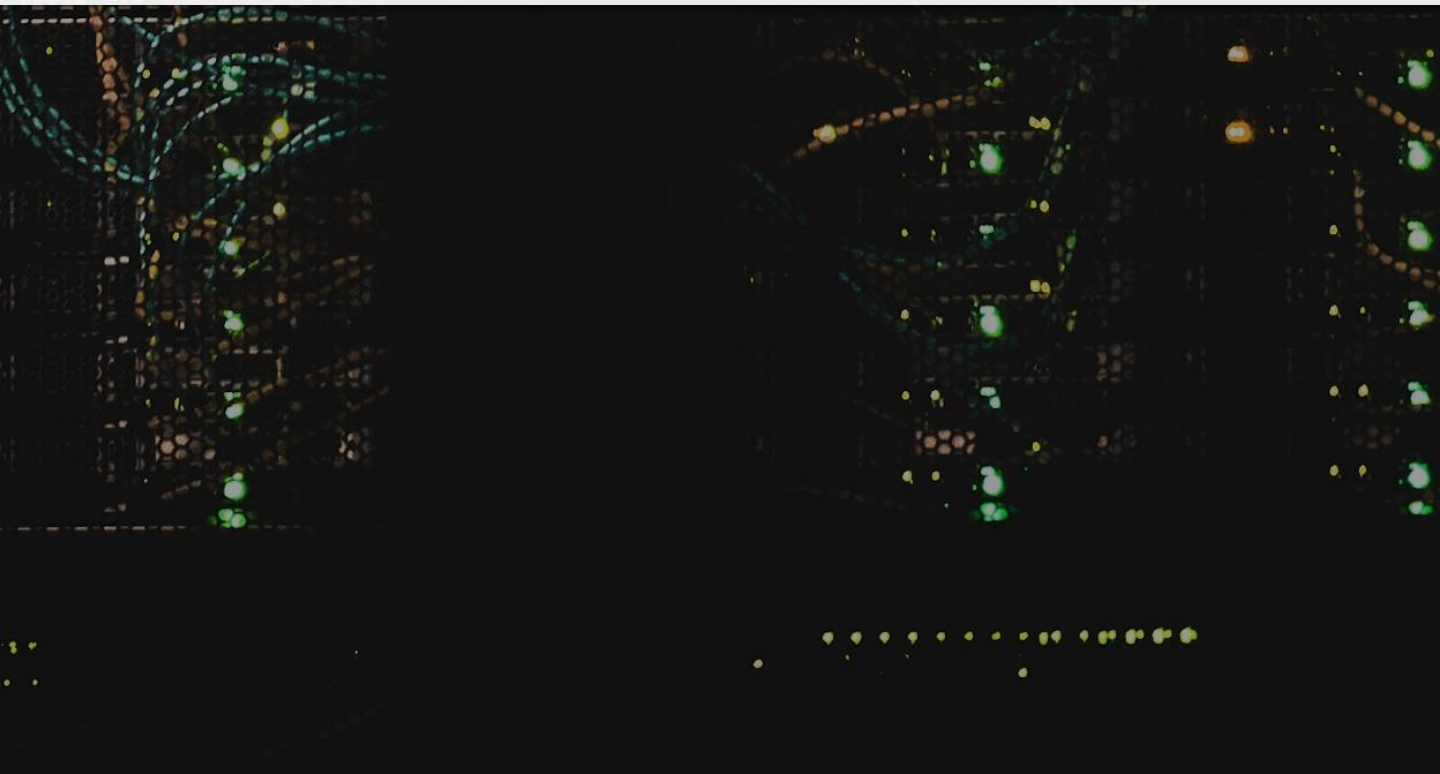
Estamos à sua espera.





Infraestrutura e Segurança.

Os pilares dos nossos serviços e plataforma.





01

Os Nossos Centros de Dados.

O lugar onde os nossos servidores se alojam.

Alojamos a nossa plataforma e infraestrutura em data centers de última geração escolhidos com base em critérios rígidos de segurança, qualidade, eficiência e conectividade.

Especificamente, três data centers (EU-MAD1) (EU-PAR1) **Interxion** e (EU-MAD2) **Equinix**, localizados em Madrid e Paris. Todos são considerados centros de dados de referência em Europa e provavelmente estão entre os mais avançados construídos até hoje. Tanto o MAD1 como o MAD2 e PAR1 são **data centers neutros** e possuem uma gama de conectividade muito ampla, o que nos permite oferecer maior redundância e disponibilidade em termos de conexão.

Os nossos data centers contam também com rigorosas medidas de segurança relacionadas ao acesso físico, condições ambientais e fornecimento de energia, garantindo assim a qualidade do nosso serviço.

Segurança Física.

O acesso aos CPDs é controlado por pessoal de segurança 24 horas por dia, 7 dias por semana, tem videovigilância e é restrito, já que só é permitido com autorização prévia.



Os Nossos Centros de Dados II.

Medidas de Segurança:

- Seguranças 24 horas.
- Gravação contínua 24/7.
- Detetor de metais e torniquete de entrada para acesso ao Datacenter.
- Câmara nas portas de acesso e corredores (externos e internos).

Controlo de Acesso:

- 5 camadas de segurança física (acesso ao perímetro, edifício, salas técnicas, armários de rack, etc.)

Controlos ambientais.

Os equipamentos de TI são mantidos e monitorizados em ambientes controlados com SLAs para temperatura e humidade:

- Refrigeração contínua (24h).
- Equipamento de Ar Condicionado Redundante.
- Temperatura de 21°C e humidade relativa de 50%.

Além disso, todos os servidores são **protegidos contra incêndios** através de um sistema de supressão projetado para extinguir qualquer incêndio em segundos e sem deixar resíduos:

- Detetores de fumo
- Arranque automático de sistemas de extinção
- Botões de emergência de arranque/paragem manuais em todos os espaços.
- Detetores do tipo ótico e iónico com sistema VESDA
- Sistema de alarme monitorizado 24/7.

Os Nossos Centros de Dados III.

Energia.

Os data centers onde alojamos a nossa infraestrutura estão equipados com ligações redundantes à rede elétrica e geradores cinéticos a diesel dimensionados para suportar as necessidades energéticas de todo o edifício e de toda a infraestrutura nele alojada.

Certificações dos nossos Centros de Dados.



ISO 14001

Environmental
Management systems



ISO 22301

Security and
resilience



ISO 27001

Information
security



ISO 9001

Quality Management
System



ISO 50001

Energy
Management

Arquitetura Redundante.

Para garantir a continuidade do serviço.

Foi implementada uma arquitetura 100% redundante para que uma falha específica de um componente não afete o funcionamento normal da plataforma e dos seus serviços.

Nós de Computação.

Cada Host possui **fontes de alimentação duplas**, cada uma conectada a um segmento elétrico diferente do data center. Todos os equipamentos que compõem a infraestrutura possuem pelo menos **duas conexões de rede de alta disponibilidade (LAG)**, e cada conexão de rede vai para um switch diferente, para que uma falha num switch não implique a interrupção do serviço. A **memória RAM** utilizada nos nossos Hosts é **ECC**, o que nos protege contra corrupção de dados e possíveis falhas.

Também temos **hipervisores em N x 1,25**, portanto temos espaço suficiente para suportar falhas de até 25% destes. No caso de uma falha de um hipervisor, os servidores nele alojados iniciam-se em outros hipervisores automaticamente.

Armazenamento.

Oferecemos armazenamento de alta disponibilidade que combina clustering de armazenamento com espelhamento síncrono para fornecer uma recuperação transparente de falhas. Com este sistema de armazenamento redundante conseguimos:

- Maior proteção contra falhas de hardware, rede ou instalação.
- Eliminar o tempo de inatividade e de gestão de mudanças.
- Atualizar hardware e software sem interromper as operações.

Rede de Dados.

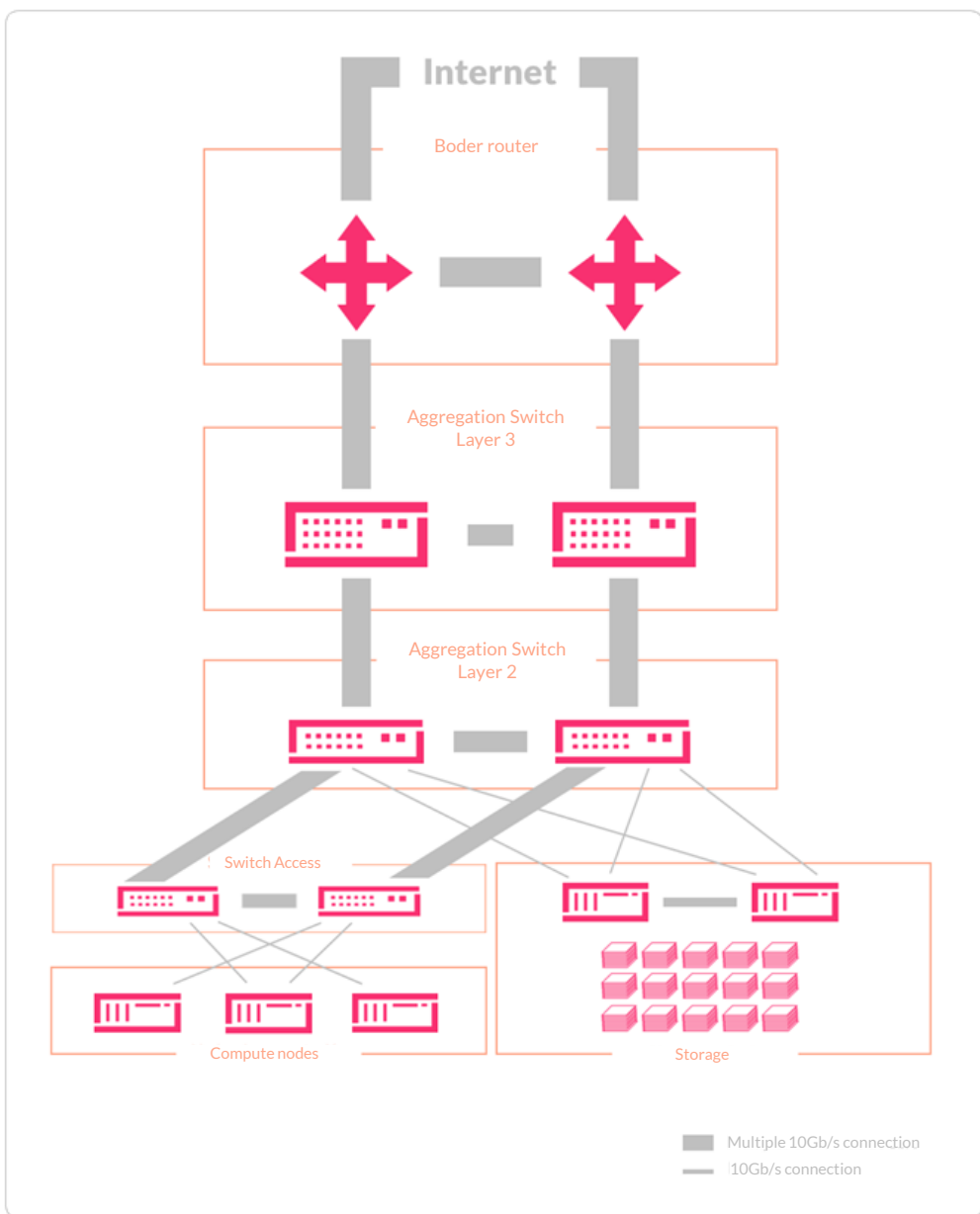
Contamos com vários circuitos 10G com diferentes fornecedores de rede de data center, por isso, um problema com um fornecedor nunca afeta a conectividade.

Os links de agregação multi-chassis formam o esqueleto da rede dentro do CPD. Estes links fornecem **redundância e escalabilidade** ao mesmo tempo que evitam a formação de loops.

Cada data center possui 2 routers de fronteira que facilitam a conexão com a Internet e outros centros. Mais atrás estão os switches para agregação da camada 3, os da camada 2 e, finalmente, os switches de acesso, aos quais os nós de computação estão conectados.

Arquitetura Redundante III.

Todos os switches lógicos são formados em pares por uma questão de redundância e são conectados a todos os dispositivos através de links agregados multi-chassis, compostos por duas ou mais conexões 10G ou 40G. Esta tipologia evita o risco de formação de loops na camada 2.



Segurança Perimetral.

Segurança Perimetral e Anti-DDOS.

A infraestrutura conta com sistemas Anti-DDOS que previnem e filtram ataques de negação de serviço, mantendo os servidores sempre disponíveis.

O nosso sistema Anti-DDOS está estruturado em diversas linhas de filtragem e detecção, o que nos permite rastrear e diferenciar pequenos ataques (de algumas centenas de Mbps) de outros ataques de milhares de Gbps.

IDS/IPS.

O nosso sistema de detecção de intrusão (IDS) é o programa que nos permite detetar o acesso não autorizado à nossa infraestrutura. Existe uma avaliação da intrusão quando ocorre e é gerado um alarme. O IDS é acompanhado por uma ferramenta de prevenção de ataques chamada IPS, que rastreia de forma contínua e proativa o tráfego de rede suspeito ou inusual.

Os sistemas IDS/IPS não conseguem parar os ataques e precisam de ferramentas adicionais, como Firewalls, para auxiliar nos processos de bloqueio.

Filtragem e Bloqueio nas Firewalls perimetrais.

As nossas firewalls de perímetro analisam continuamente o tráfego que chega aos nossos data centers e bloqueiam tráfego claramente malicioso, para que não entre no nosso CPD. Ao mesmo tempo, eles também analisam o volume de tráfego recebido por cada máquina, para que possam ter controlo sobre o tráfego recebido por cada servidor e detetar possíveis ataques DDOS.

SSD e NVMe (NetApp).

Discos de estado sólido de alta gama.

Para garantir a mais alta disponibilidade, usamos apenas as unidades de estado sólido (SSDs e NVMe) de última geração (all-flash da NetApp).

A utilização deste tipo de discos Enterprise visa, entre outras coisas:

O melhor rendimento de forma constante.

Ao usar armazenamento all-flash da NetApp, o nosso objetivo é oferecer um desempenho excelente de forma constante, independentemente da carga de trabalho do disco ou da ocupação do disco.

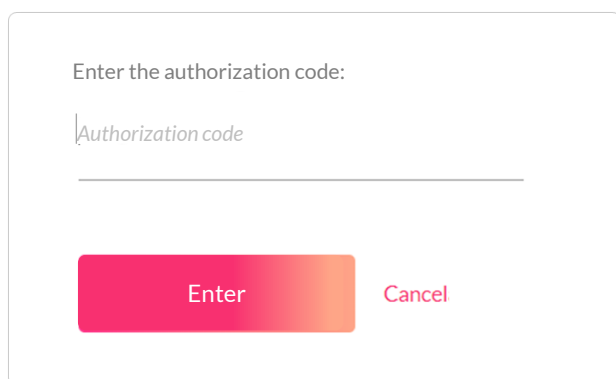
A proteção dos dados.

O sistema all-flash da NetApp oferece uma camada extra de proteção sobre os dados de forma integrada. Replicação síncrona, encriptação integrada, proteção WORM ou autenticação multifator são algumas das vantagens que os nossos sistemas de armazenamento apresentam e que nos ajudam a manter os dados essenciais disponíveis, protegidos e seguros.

Autenticação e Encriptação.

Dupla Autenticação.

O acesso à plataforma e ao portal foi reforçado com a possibilidade de implementação de dupla autenticação (2FA) através de um token de acesso gerado num dispositivo móvel. O token gerado por este software é um número de seis dígitos que o utilizador deve fornecer, além do seu nome de utilizador e password para aceder aos serviços.



Enter the authorization code:

Authorization code

Enter Cancel

A proteção dos dados.

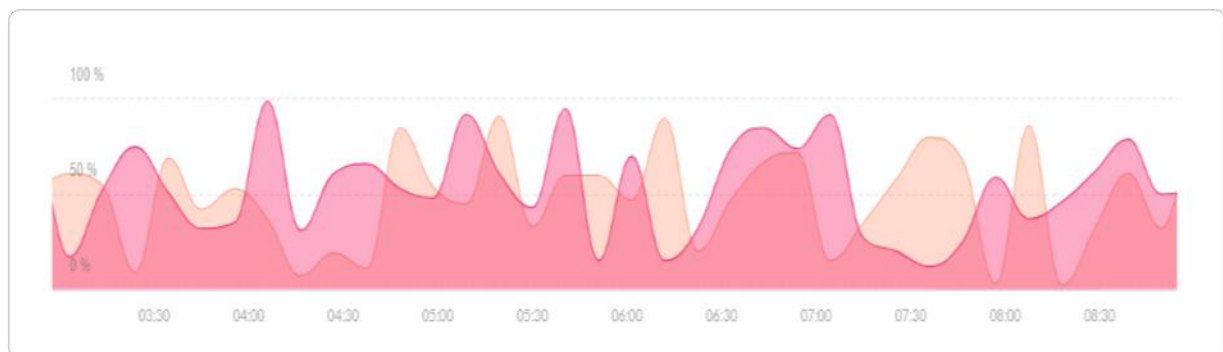
A encriptação é um processo de codificação de informação. Este processo converte a representação da informação original (texto simples) numa forma alternativa conhecida como texto cifrado ou encriptado, que apenas as partes autorizadas podem desencriptar. Os serviços utilizam diferentes sistemas de codificação e criptografia para a gestão e transferência de informações, dando mais uma camada de proteção contra possíveis ataques.



Monitorização 24/7.

Mais métricas, maior capacidade de resposta.

Dispomos de um sistema de monitorização e alerta 24 horas por dia, 7 dias por semana, que permite a monitorização contínua do estado de todo o sistema, tanto da infraestrutura como dos restantes subsistemas, para garantir a fiabilidade e estabilidade dos serviços e da plataforma. Isso permite-nos avaliar a saúde e o desempenho de todo o sistema.



O nosso sistema de monitorização 24 horas por dia, 7 dias por semana, é baseado na recolha de métricas, processamento e visualização de dados, juntamente com o estabelecimento de regras e alertas. O objetivo final é ser informado sobre possíveis sintomas de risco ou mau funcionamento antes de uma queda ou tempo de inatividade.



Backup

07

Backups e Restausros.

O *backup* é uma cópia dos dados originais que é feita para ter uma forma de os recuperar em caso de perda. Os *backups* são extremamente úteis em diferentes circunsntâncias e para diferentes utilizações. Como sabemos disso, estabelecemos diferentes políticas e tipos de *backups* dependendo do serviço.

Política de backup em Servidores.

Os serviços Desktop Remoto e Servidores possuem uma política de *backups* baseada em instantâneos de disco (NetApp) com a seguinte programação fixa e pré-estabelecida:

- Todas as horas [últimas 5 horas)
- Todos os dias [últimos 14 días às 00:10]
- Todas as semanas [últimas 8 semanas – domingos às 00:15]

Além disso, os utilizadores poderão realizar *backups* manuais ou mensais na plataforma de orquestração IaaS, com base em instantâneos de disco. A programação mensal tem uma retenção máxima de até 24 meses.

A restauração de backups está disponível online na sua secção correspondente da plataforma.



VSS (Volume Shadow Copy Service) (opcional):

Shadow Copy é uma tecnologia que permite criar cópias de segurança, snapshots de arquivos ou volumes do servidor de forma oculta, permitindo que sejam realizados mesmo quando estiverem em uso.

Este tipo de cópia é disponibilizado aos utilizadores de forma opcional, exigindo ativação prévia. Por padrão, está configurado para realizar 2 cópias por dia, dos últimos 14 dias.

Réplicas no Repositório S3.

O sistema de armazenamento de objetos replica cada objeto para **3 discos diferentes localizados em 3 servidores diferentes**. A política estabelecida manterá, por padrão, pelo menos uma das cópias **num Data Center diferente**.

O serviço Repositório S3 também possui uma funcionalidade de versionamento que pode ser ativada a qualquer momento a partir da subscrição da plataforma. Desta forma, as versões anteriores podem ser recuperadas através do protocolo S3.



Política de *backup* no Armazenamento cloud.

O serviço Armazenamento cloud possui uma política de *backups* pré-estabelecida e comum para todos os utilizadores em nível granular e de forma encriptada.

A política de cópias de segurança é indicada abaixo:

Frequência de *Backups*: 1 cópia diária.

Retenção das Cópias de Segurança:

- Todas as horas [últimas 5 horas)
- Todos os dias [últimos 14 dias às 00:10]
- Todas as semanas [últimas 8 semanas – domingos às 00:15]

Por outro lado, estão disponíveis **instantâneos de volume VSS** que permitem restaurar versões anteriores de arquivos e pastas.

Programação de Snapshots: Todos os dias [12:00 e 18:00]

Retenção de Snapshots:

- 64 instantâneos.

Sistema de recuperação de dados instantâneo e online disponível para qualquer utilizador.



Custódia de dados [Stackscale].

Custódia de dados com uma empresa independente.

Para aumentar ainda mais a nossa segurança e tentar proteger a informação em todos os ambientes alojados, chegámos a um acordo com a Stackscale, empresa independente especializada em nuvem privada e localizada em Espanha, para armazenar uma das nossas cópias de segurança nos seus sistemas de armazenamento.

Desta forma, damos um passo em frente para garantir a disponibilidade das informações em caso de ataque e adicionar mais uma camada de segurança. Da mesma forma, é importante notar que todo este sistema de cópia foi realizado sob o rigoroso padrão estabelecido pela Lei de Proteção de Dados (RGPD) no que diz respeito à sua confidencialidade.

Service Level Agreement.

AVAILABILITY	COMPENSATION
99,99 > D >= 99,72	10% of monthly payment
99,72 > D >= 99,44	20% of monthly payment
99,44 > D >= 99,16	30% of monthly payment
D < 99,16	40% of monthly payment

Disponibilidade (D) = $[(\text{Horas mês} - \text{Horas indisponibilidade}) / \text{Horas mês}] \times 100$

Não contam para o cálculo da disponibilidade de acesso (SLA):

- Causas alheias ao nosso controlo e força maior.
- Indisponibilidade do painel de autogestão.
- Tempo de inatividade como resultado de falhas no software que reside nas máquinas virtuais.
- Vírus e ataques informáticos que provoquem a impossibilidade total ou parcial de prestação dos serviços.

Os seus dados estão seguros.

