Obmondo

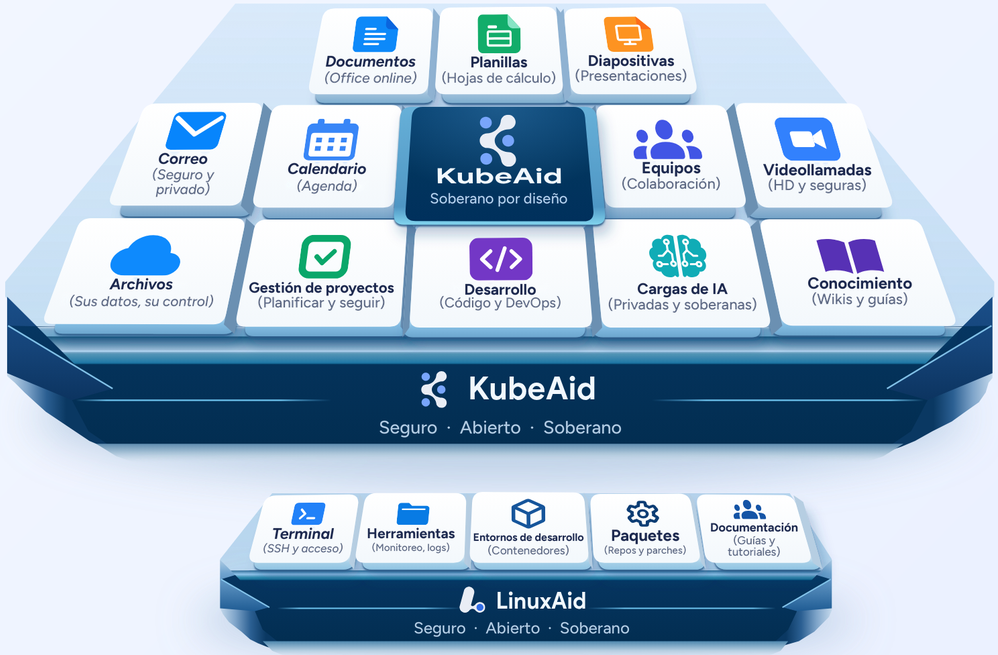
CÓMO TRABAJAMOS

Su infraestructura es suya. Nosotros la operamos.

Operaciones de Linux y Kubernetes basadas en código abierto, sin dependencia de proveedor.

Soluciones soberanas

desde alternativas a Microsoft 365 hasta IA en tus propias GPUs



Infraestructura soberana
Alojada en su región (o en su propio entorno)

Seguridad de extremo a extremo
Cifrada, auditable, con cumplimiento normativo

Estándares abiertos
Interoperables y flexibles

Sostenible
Uso eficiente de los recursos

Pensado para equipos
Desde equipos pequeños hasta grandes organizaciones

CLIENTES

Algunos de los equipos con los que hemos trabajado



"Estoy muy contento de contar con Obmondo para nuestras operaciones; llevamos más de 10 años trabajando con ellos."

Esben Madsen
CEO, Ebillet a/s

"Obmondo ha sido nuestro socio tecnológico para todo lo relacionado con el código abierto. Sus frameworks de automatización de código abierto y sus soluciones a medida garantizan la disponibilidad de GN."

Jakob Ovesen
Arquitecto Linux, GN Store Nord

"Antes de empezar a trabajar con Obmondo, era muy difícil obtener información como qué servidores corrían Red Hat, entre otras cosas. Obmondo también ordenó las actualizaciones de seguridad y el mantenimiento, lo que le facilitó mucho el trabajo al equipo."

Mark Gittins
Ingeniero DevOps Sénior, HBK

La historia en once capítulos

00
Nuestro enfoque de código abierto
Por qué KubeAid y LinuxAid son públicos

01
Soberanía digital
Es suyo, nosotros lo operamos

02
Cómo trabajamos
Parte de su equipo

03
Servicios
De qué nos encargamos

04
Incorporación
Primero, el acceso

05
Seguridad y acceso
Llaves de hardware, zero trust

06
Monitoreo y alertas
Seguridad, alertas y plazos

07
Estrategia de backup
Según sus objetivos de recuperación

08
Restauración y recuperación ante desastres
Probada, no supuesta

09
Precios y contrato
Por servidor, mes a mes

10
SKI 02.22
Operaciones híbridas

25 años de operaciones Linux, publicados como código abierto

Nuestro fundador trabaja en operaciones Linux desde hace más de 25 años. Esa experiencia está en dos proyectos de código abierto: KubeAid y LinuxAid.

Ambos configuran servidores y clusters desde Git y cubren lo que todo sistema en producción necesita: seguridad, actualizaciones, backup y recuperación.

El código es compartido. Una corrección o funcionalidad que desarrollamos para un cliente llega a todos los clientes que usan el mismo proyecto, lo que reduce para todos el costo de una configuración segura.

EN KUBEAID HOY

120+

Helm charts en el repositorio público de KubeAid, compartidos por todos los clientes que usan KubeAid.

kubeaid

Para Kubernetes
kubeaid.io

linuxaid

Para servidores Linux
linuxaid.io

Su hosting, sus cuentas, su acceso root

Dondequiera que corran sus sistemas, el entorno sigue siendo suyo.



USTED MANTIENE EL CONTROL DE

- El proveedor de hosting
- Servidores y cuentas en la nube
- Código y arquitectura de las aplicaciones
- Acceso root y permisos de administrador

Nosotros operamos la capa del sistema operativo: hardening, parches, cumplimiento, monitoreo, backups y planificación de la recuperación. Si lo desea, también tratamos con su proveedor de hosting los problemas de hardware y red.

Puede irse cuando quiera, casi gratis

Muchos proveedores encarecen el cambio con herramientas propietarias, monitoreo a medida y configuraciones atadas a su plataforma. Nosotros usamos código abierto y todo es suyo: si se va, todo sigue funcionando.

01

Mes a mes

Facturación mensual, sin compromiso a largo plazo. Usted mismo cambia o cancela su plan en el portal, y el soporte termina con el período en curso.

02

Su configuración, su Git

Su configuración vive en su propio repositorio Git. Puede alojarlo usted mismo en GitHub, GitLab, Gitea u otros, y darnos una deploy key que puede revocar.

03

Fácil de traspasar

El monitoreo, las alertas y los backups están documentados y son reproducibles, con herramientas de código abierto. Otro proveedor puede hacerse cargo sin reconstruir nada.

Si la calidad no está a la altura, puede reemplazarnos de inmediato.

Niveles de servicio por tiempo de respuesta, no por disponibilidad

Un SLA de disponibilidad clásico supone que un solo proveedor controla todo el stack. Usted controla el suyo, así que no prometemos lo que solo usted controla.

FUERA DE NUESTRO CONTROL

- La fiabilidad de su red
- La disponibilidad de su proveedor de hosting
- Los cambios que sus propios equipos hacen en servidores que usted controla

NUESTRO COMPROMISO

- Tiempos de respuesta según su plan de soporte, desde 1 día hábil hasta 1 hora, 24×7
- Monitoreo de vulnerabilidades/CVE y aplicación de parches
- Soporte para sus equipos de operaciones y desarrollo

Es una decisión deliberada. Usted mantiene el control y nada lo ata a nosotros.

Parte de su equipo técnico

SISTEMAS EXISTENTES

Trabajamos con lo que ya usa

Usamos los sistemas, las herramientas y la infraestructura que ya tiene, y los mejoramos junto con usted.

SISTEMAS NUEVOS

Lo construimos desde cero

Construimos un entorno nuevo sobre LinuxAid o KubeAid, siguiendo las mejores prácticas de la industria, y migramos sus servicios a él.

Observar

El monitoreo se instala primero y sigue funcionando.

Revisar

Analizamos los puntos fuertes y débiles de su entorno.

Mejorar

Proponemos mejoras concretas y las planificamos con usted.

Compartir

Salvo que se acuerde lo contrario, el trabajo se incorpora a LinuxAid o KubeAid para todos los clientes.

Mejoras compartidas, costo compartido

Muchos clientes usan los mismos proyectos de código abierto. Cuando un trabajo mejora un proyecto, los clientes que se benefician se reparten el costo.

EJEMPLO · UNA TAREA · 30 HORAS DE DESARROLLO Y PRUEBAS



5 horas

Su parte, en su factura

25 horas

Pagadas por los demás clientes que reciben la misma mejora

En el portal de clientes, el trabajo compartido es una funcionalidad que los clientes patrocinan. Su costo se reparte a partes iguales o según la cantidad de nodos de cada cliente, y cada hora aprobada aparece como comentario en su ticket.

Qué hacemos, qué sigue siendo suyo

Configuración de Linux y Kubernetes

Servidores y clusters nuevos sobre LinuxAid y KubeAid, con sus servicios migrados a una base limpia y estándar. O empezamos monitoreando lo que usa hoy.

Monitoreo

Desde Bronze, las alertas llegan directo a nuestro equipo de operaciones. El monitoreo lo alojamos nosotros, o usted usa su propio Prometheus y Puppet y nos reenvía las alertas.

Backups y restauraciones

Configuramos y operamos el backup y la restauración de su infraestructura, ajustados a sus requisitos de fiabilidad.

Actualizaciones de seguridad

Parches del sistema operativo y de las aplicaciones, más allá de la distribución base, aplicados en las ventanas de servicio que elija. Gestionamos los repositorios de paquetes, idealmente desde un servidor dedicado.

SIGUE SIENDO SUYO, SALVO ACUERDO

- Aplicaciones a medida
- Configuración del negocio
- Gestión de accesos
- Flujos de aprobación internos

El portal de clientes muestra los CVE abiertos de cada servidor y su próxima ventana de actualización.

Primero el acceso, después una evaluación completa

1 Acceso

Lo primero es el acceso por bastión o VPN. Los tiempos dependen de qué tan rápido estén listas sus reglas de firewall y su enrutamiento.

2 Incorporación

Agregue un servidor en el portal de clientes en obmondo.com y ejecute como root el comando de instalación que se le indica. O denos acceso por SSH/VPN y lo hacemos nosotros.

3 Evaluación

Revisamos la configuración, la seguridad y los accesos, el backup y la recuperación, el monitoreo, la salud operativa y la arquitectura.

4 Plan de trabajo

Juntos acordamos un plan de trabajo con las mejoras y la operación a largo plazo.

Clusters de Kubernetes existentes

Podemos monitorear un cluster existente durante un período corto mientras diseñamos un nuevo cluster KubeAid que resuelva los problemas que encontremos.

¿Ya usa Puppet?

Recomendamos la configuración de Puppet de LinuxAid, basada en OpenVox, el fork comunitario de Puppet. Su agente reemplaza el paquete puppet-agent y puede funcionar completamente en sus propios hosts.

Zero trust, con llaves de hardware

La identidad de cada ingeniero vive en una YubiKey. La clave privada no se puede extraer, se desbloquea con un PIN y cada operación requiere un toque físico. El acceso no se puede compartir, robar mediante phishing ni usar en silencio desde una máquina comprometida.

Toque
en cada inicio de sesión, firma y descifrado

1 identidad
SSH y GnuPG, por ingeniero

TRES FORMAS DE ENTRAR

- **Bastión saliente.** Una pequeña VM en su red abre hacia nosotros un túnel de salida solo para SSH.
- **Bastión entrante.** Puerto 22, accesible solo desde nuestras IP fijas en Dinamarca, Alemania y Finlandia.
- **VPN NetBird.** VPN de código abierto basada en WireGuard, con inicio de sesión en Keycloak y MFA.

INICIOS DE SESIÓN, SECRETOS Y AUDITORÍA

- En los clusters KubeAid, el acceso a Kubernetes pasa por NetBird, y el inicio de sesión de Keycloak se asigna a roles de Kubernetes.
- Las contraseñas se guardan en pass, de passwordstore.org, y cada secreto requiere su propio toque.
- Los registros de auditoría muestran quién accedió a un cluster, cuándo, con qué identidad y qué acciones de Kubernetes ejecutó.

Puede leer cada regla con la que alertamos

Sus servidores y clusters se monitorean con Prometheus usando nuestras reglas de alerta de código abierto, publicadas en github.com/Obmondo/KubeAid.

Servidores, con LinuxAid

- Métricas de host y hardware
- CPU, RAM, E/S y salud de los discos
- Sistemas de archivos y almacenamiento
- Rendimiento de red

Las reglas se actualizan con regularidad y tienen su propio conjunto de pruebas.

Kubernetes, con KubeAid

- Nodos, pods y contenedores
- Rendimiento de etcd
- Ingress, servicios y red
- Plano de control y API server
- Scheduler y controller-manager
- Aplicaciones de código abierto seleccionadas

Basado en kube-prometheus, con nuestras propias reglas encima y paquetes de alertas opcionales por cluster.

Si lo desea, excluimos de las alertas determinados hosts o componentes.

Monitoreo y mitigación de seguridad

linuxaid | SERVIDORES

- **Vulnerabilidades conocidas.** El portal muestra los CVE abiertos de cada servidor, con su severidad y la próxima ventana de actualización.
- **Fin de soporte.** Una alerta 75 días antes de que la versión del sistema operativo deje de recibir actualizaciones de seguridad gratuitas, y otra cuando eso ocurre.
- **Firewall.** Una alerta cuando el firewall empieza a bloquear una cantidad inusual de tráfico, señal de intentos de intrusión.
- **Hardening.** SSH solo permite algoritmos robustos de intercambio de claves, cifrados y MAC, y auditd y SELinux se pueden activar por servidor.
- **Snapshots de repositorios.** Los paquetes provienen de un snapshot fechado que se adelanta el día anterior a cada ciclo de actualización, para que todos los servidores reciban las mismas actualizaciones.

kubeaid | KUBERNETES

- **Seguridad de la cadena de suministro.**
  - **Escaneo de imágenes.** Trivy analiza las imágenes de contenedor que usa en busca de vulnerabilidades conocidas, y el portal muestra los resultados.
  - **Mirror de registro.** Harbor puede replicar esas imágenes y también escanearlas.
- **Fin de soporte.** Una alerta cuando la versión de Kubernetes del cluster se acerca al fin de soporte.
- **Firewall.** Las network policies de Cilium filtran el tráfico de entrada y salida, y se dispara una alerta cuando el tráfico denegado se mantiene alto, señal de intentos de intrusión.
- **Seguridad en tiempo de ejecución.** Tetragon vigila la actividad de procesos y de red en el cluster, y KubeArmor puede bloquear lo que sus políticas prohíben.
- **Políticas de admisión.** Kyverno o Gatekeeper pueden detener las cargas de trabajo que incumplen sus reglas antes de que arranquen.

El escaneo de imágenes, la detección en tiempo de ejecución y las políticas de admisión son opciones que se activan por cluster.

Las correcciones se aplican en sus ventanas de servicio, como pull requests en su repositorio de configuración.

Con Bronze o superior, cada alerta se convierte en un ticket con plazo

01
Prometheus
Se dispara una regla de alerta en su servidor o cluster.

→

02
Ingesta
Alertmanager la envía a nuestro endpoint.

→

03
Ticket
Se abre o se actualiza automáticamente y se muestra en su portal.

→

04
Plazo
Desde 1 día hábil en Bronze hasta 1 hora en Platinum.

→

05
Personas
Nuestro equipo de operaciones ve cada alerta en el chat.

ESCALAMIENTO

Se avisa al ingeniero de guardia cuando falta menos de una hora para que venza un plazo de respuesta. Las alertas críticas también llegan a la dirección.

Las alertas que se disparan durante su ventana de servicio se retienen. Si siguen activas cuando termina la ventana, se convierten en tickets.

La mayoría de las alertas se disparan antes de que algún servicio se vea afectado, lo que nos da tiempo para resolver el problema antes de que algo falle. Cuando algo sí falla, primero restablecemos el servicio y después corregimos la causa raíz.

Backups según sus objetivos de recuperación

Su RPO es cuántos datos puede permitirse perder. Su RTO, qué tan rápido necesita recuperarlos. Partimos de lo que ya funciona y proponemos cambios donde haga falta.

PUNTO DE PARTIDA

- **Instalaciones nuevas.** Denos un servidor en blanco, normalmente un Ubuntu o Debian LTS mínimo, y entregamos una solución de backup completamente de código abierto.
- **Sistemas existentes.** No damos nada por sentado sobre lo que está configurado, y acordamos con usted el camino antes de cambiar nada.

MÉTODOS

- **Recuperación a un punto en el tiempo** para PostgreSQL, con el WAL archivado en S3, y para otros sistemas que lo soporten.
- **Snapshots de Kubernetes** para una recuperación local rápida, replicados en S3.
- **Copias externas.** Recomendamos replicar el backup en una segunda ubicación.

ALMACENAMIENTO Y CIFRADO

- Almacenamiento compatible con S3.
- Cifrado del lado del cliente (recomendado) o LUKS en el disco de datos del servidor de backup.
- Siempre cifrado en tránsito, por HTTPS o SSH.

Las restauraciones se prueban, no se dan por hechas

PRUEBAS DE RECUPERACIÓN

Planificadas con usted, registradas en un ticket

ISO 27001 y NIS2 suelen exigir pruebas de recuperación periódicas. Cada hora dedicada a una se registra en su ticket, como todo nuestro trabajo.

- **Clusters reproducibles.** La CLI de KubeAid construye cada cluster KubeAid de la misma forma automatizada. Las reconstrucciones requieren menos pasos manuales y hay menos datos que respaldar.
- **Qué determina el tiempo de restauración.** Una restauración completa depende del tamaño del almacenamiento, de si es en la nube u on-premise, y de qué snapshots y WAL hay disponibles.
- **Lecciones compartidas.** Una corrección encontrada en la prueba de un cliente llega a todos los clientes de LinuxAid y KubeAid.

Precio por servidor, mes a mes

PLAN	NIVEL DE SERVICIO
Basic	Monitoreo y chat en vivo
Bronze	Respuesta en 1 día hábil
Silver	Respuesta en 4 horas en horario laboral
Gold	Respuesta en 2 horas, 24×7
Platinum	Respuesta en 1 hora, 24×7

- Los descuentos por volumen se aplican automáticamente a medida que agrega servidores.
- El asesoramiento y el trabajo de operaciones se facturan como consultoría, por minuto. La calculadora muestra las horas de consultoría gratuitas de su combinación de planes.
- El horario laboral es de 08:00 a 17:00 en su zona horaria principal, en días hábiles.
- Cancele cuando quiera. El soporte termina con el período de suscripción en curso.

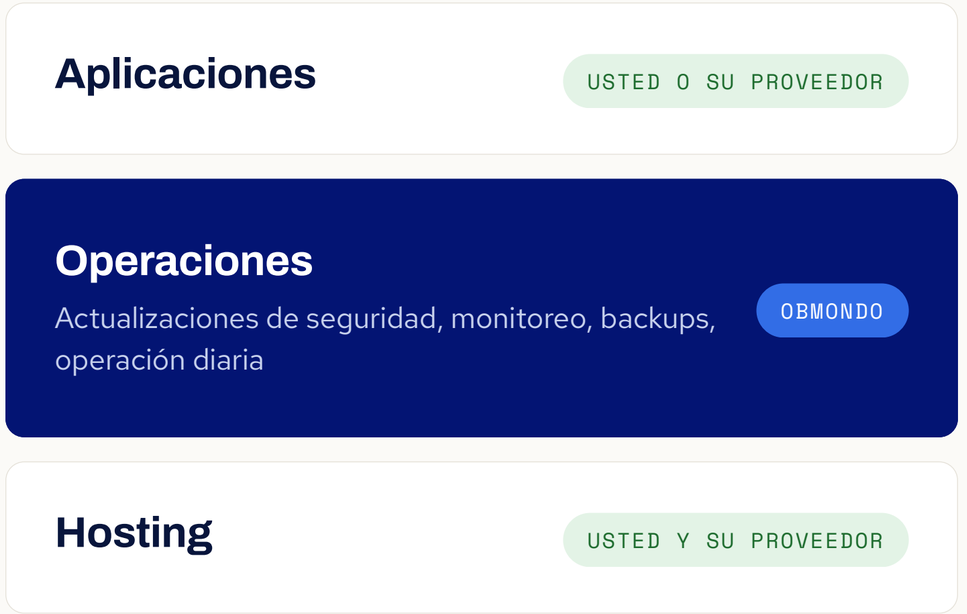
Precios actuales y calculadora:
obmondo.com/pricing

Cómo encajamos en SKI 02.22

SKI 02.22 abarca operaciones de TI de cualquier alcance, desde la externalización completa hasta modelos híbridos en los que las organizaciones conservan su infraestructura y externalizan partes concretas a proveedores especializados.

Encajamos en el modelo híbrido. Nos encargamos de la capa de operaciones: actualizaciones de seguridad, monitoreo, estrategia de backup y operación diaria de la infraestructura. El hosting y las aplicaciones siguen en sus manos.

Solo la capa de operaciones, por diseño. Usted mantiene el control de su infraestructura, la ubicación de sus datos, su postura de seguridad y la elección de proveedores.



Obmondo

PRÓXIMO PASO

Hablemos de su infraestructura

Agende una reunión

CORREO Y TELÉFONO

sales@obmondo.com · +45 61 28 12 00

WEB

obmondo.com

CÓDIGO ABIERTO

github.com/Obmondo · kubeaid.io · linuxaid.io