

LA PLATAFORMA QUE CUIDA SU INFRAESTRUCTURA

ABZU

El océano primordial, convertido en plataforma.

Sus aplicaciones, servidores y datos: protegidos, probados y recuperables en minutos.

Para recuperar un archivo, hoy se restaura un servidor entero.

TODOS O NADA

El respaldo típico guarda la imagen completa del servidor. No existe recuperar una aplicación, un archivo o una tabla por separado.

HORAS, NO MINUTOS

Recuperar significa reconstruir la máquina completa y esperar. Mientras tanto, la operación está detenida.

SIN PRUEBA

Nadie sabe si el respaldo sirve hasta el día del desastre. Y ese día es tarde para descubrirlo.

Su continuidad no debería depender de una restauración de horas.

Así se resuelve: la plataforma aprende su infraestructura — y nunca deja de cuidarla.

01

DESCUBRE

En minutos, Abzu inventaría lo que ya corre: aplicaciones, servidores y bases de datos.

02

DOCUMENTA

Cada servicio queda descrito en una receta con historial: la única fuente de verdad.

03

VIGILA

Si algo cambia sin autorización, la plataforma lo detecta, lo corrige o lo alerta.

04

PRUEBA

Cada respaldo se restaura en un entorno aislado y se verifica antes de contar como válido.

05

RECUPERA

El plan de recuperación se ensaya con regularidad. El día del desastre ya se practicó.

Una consola lo gobierna todo. En cada servidor, un asistente ligero que reporta y ejecuta — sin abrir accesos remotos a su red.

Precisión de cirujano cuando la quiere. Servidor completo cuando lo necesita.

LO QUE EL MERCADO LE OBLIGA A ESCOGER

Imagen completa: segura, pero lenta y todo-o-nada

O herramientas granulares que no cubren todo su parque

Usted elige una vez — y vive con esa limitación

CON ABZU, USTED DECIDE POR SERVICIO

Granular: una aplicación, un archivo o una tabla, en minutos

Completo: el servidor o la máquina virtual enteros, para reconstruir desde cero

Ambos mundos conviven en la misma consola

No lo prometemos. Lo medimos.

7.195

filas de una base de datos real, restauradas en un entorno aislado y comprobadas una a una contra el origen

4,6 s

para devolver una base de datos al instante exacto anterior a un error humano

2.100/2.100

filas de SQL Server idénticas después de la restauración: ni una sola diferencia

193

verificaciones de calidad de la plataforma, ejecutadas y superadas — cero fallos

Evidencia completa en el informe de validación ABZU-VAL-2026-002, firmado digitalmente.

Que el ransomware encuentre una bóveda, no una puerta.

01 IMPOSIBLE DE BORRAR

Los respaldos sellados no los puede eliminar ni el propio sistema antes de su fecha. El ransomware tampoco.

02 HISTORIA SELLADA

Las copias históricas quedan cerradas bajo sello: aunque caiga un servidor, su pasado recuperable sobrevive.

03 ACCESO MÍNIMO

Cada servidor protegido solo puede añadir respaldos nuevos. Modificar o borrar la historia no está en su poder.

04 PROBADO, NO SUPUESTO

Cada respaldo se restaura en un entorno aislado y se revisa contra virus antes de darse por válido. Si está infectado, se marca — y nunca se usa a ciegas.

El cifrado protege el contenido. La inmutabilidad garantiza la vuelta.

El plan se prepara solo. La decisión final la toma una persona.

01

DETECTA

La caída se detecta al instante y el impacto se delimita solo.



02

PREPARA

El plan de recuperación queda listo y ensayado, esperando la orden.



03

APRUEBA

Un responsable autoriza con un toque. Quien pide no puede aprobar: separación de funciones.



04

EJECUTA

Restauración verificada, con el tiempo de recuperación medido y reportado.

Aprobación desde la consola, el móvil o por voz — siempre con registro firmado de quién decidió.

Un solo inventario para todo el parque.

DOCKER

Los contenedores de cualquier servidor, descubiertos en segundos.

KUBERNETES

Clústeres completos, dentro del mismo inventario y la misma consola.

PROXMOX VE

Máquinas virtuales y contenedores LXC — respaldados ambos.

VMWARE

Se opera sin instalar nada dentro de sus servidores VMware.

HYPER-V

Las máquinas virtuales de sus anfitriones Windows, como parte del inventario.

KVM

La virtualización abierta, integrada con la misma experiencia.

Y en la nube: la misma protección en AWS, Azure y Google Cloud.

Dato verificado: Veeam no respalda contenedores LXC de Proxmox — solo máquinas virtuales (guía oficial de su complemento para Proxmox VE, limitaciones). Abzu sí.

Sus bases de datos, protegidas — con vuelta en el tiempo.

PostgreSQL

Vuelta al instante exacto que elija

MySQL · MariaDB

Vuelta al instante exacto que elija

SQLite

Copia fiel, sin detener el servicio

SQL Server

Respaldo completo y continuo, verificado

Cada respaldo viaja y reposa cifrado, con una huella que permite comprobar que nadie lo alteró.

TIEMPO MEDIDO PARA VOLVER AL INSTANTE ELEGIDO

POSTGRESQL · 4,6 s

MARIADB · 6,3 s

SQL SERVER · 16 s

El cumplimiento se demuestra con evidencia, no con folletos.

0

hallazgos críticos en la auditoría
ofensiva final del producto

NORTIC — REPÚBLICA DOMINICANA

El mapa de cumplimiento, control por control, contra las normas A7, A8 y A9 — con las brechas declaradas con honestidad.

ISO 27001 · NIST — EL MUNDO

El mismo mapa de controles, leído en el marco de cada mercado. Un hecho, tres lecturas.

AUDITORÍA OFENSIVA PROPIA

Antes de ofrecérselo, el producto fue atacado por especialistas en intrusión: 0 hallazgos críticos, y los demás corregidos y re-verificados (informe ABZU-RT-2026-004).

INFORMES FIRMADOS

Validación y auditoría se entregan firmadas digitalmente desde la propia plataforma. Sin la firma registrada, el informe no cuenta como entregado.

Toda institución tiene una llave maestra. La pregunta es quién la guarda.

UNA SOLA PERSONA

Si la llave vive en manos de una persona, la institución depende de su memoria, su lealtad y su presencia. Las personas rotan, faltan o se van.

UN PAPEL FOTOGRAFIABLE

Una clave escrita, impresa o en pantalla se copia con una simple foto. Quien la ve una vez, la tiene para siempre.

EL RELEVO QUE NO LLEGA

Cambian los directores y los equipos. Si el traspaso no ocurre a tiempo, la llave se pierde con la persona — y con ella, el control.

En el Estado, una llave perdida o robada no es un incidente técnico: es una crisis de soberanía.

La llave que ninguna persona posee.

La llave maestra de Abzu no existe completa en ningún lugar: vive dividida entre custodios, y reconstruirla exige una ceremonia — no un clic.

COMO UNA LLAVE DE LANZAMIENTO

Se requieren varios custodios, a la misma hora y cada uno desde su terminal. Nadie actúa solo, jamás.

NI CON UNA FOTO

Lo que una cámara puede copiar no sirve de nada por sí solo. Y cada impresión lleva una marca invisible que revela su origen.

BIOMETRÍA PARA TODOS

Cada participante — incluido quien solicita — valida su identidad con su rostro o su huella. Sin excepciones.

LA INSTITUCIÓN SOBREVIVE A LAS PERSONAS

Relevo formal por periodo, custodio de recuperación fuera del equipo operativo y sucesión documentada: la llave nunca queda huérfana.

Toda institución tiene un botón que teme tocar.

El día en que todo se apaga — un incendio, un ataque, un error — alguien tiene que traer la institución de vuelta a la vida. Ese día no se improvisa.

Nuestro botón existe. Y nadie puede tocarlo solo.

- Dos llaves, en manos de personas distintas
- Dos custodios, a la misma hora, cada uno desde su terminal
- La identidad de cada participante, validada con su biometría
- Cada intento — logrado o no — queda registrado



Está protegido como el de verdad, porque lo que levanta no es un servidor: es la institución entera.

Se gira la llave. Se presiona. La institución vuelve.



SE LEVANTAN LOS SERVICIOS

VUELVEN LOS DATOS

SE VERIFICA CADA PASO

En el orden correcto, con los tableros cobrando vida uno a uno. Lo que tomaba horas de reconstrucción manual sucede como una sola operación — dirigida, medida y verificada.

Y cuando termina, queda la prueba.

4,6 s

para volver al instante exacto anterior al error

2.100/2.100

filas idénticas tras la restauración más exigente

16 s

para restaurar y verificar una base completa en aislamiento

Del acto queda un informe firmado: qué se recuperó, quién lo aprobó y cuánto tardó.

Sin ese informe, la recuperación no cuenta como hecha.

La misma plataforma, en la forma que su organización necesita.

COMERCIAL

Integrada a la plataforma SEGRD, con su misma identidad de acceso

Cada cliente, aislado en su propio espacio

Abierta a integrarse con sus sistemas actuales

GOBIERNO

Llave en mano y autocontenida: funciona sin internet

Licencia perpetua, activada fuera de línea

Sus llaves y su firma viven dentro de su instalación — de nadie más

Un modelo simple: por servidor. Sin sorpresas.

COMERCIAL · SUSCRIPCIÓN

US\$1,495

por servidor / año

Contenedores ilimitados por servidor

GOBIERNO · LICENCIA PERPETUA

US\$4,995

por servidor, para siempre

Soporte anual 20 % — primer año incluido

POR SERVIDOR

Todo lo que corre dentro del servidor, cubierto.

SIN COBRO POR USO

Ni por aplicación, ni por base de datos, ni por volumen.

SIN CONTADORES OCULTOS

Un servidor denso cuesta lo mismo que uno ligero.

Se empieza con un servidor. Sin tocar su operación.

PASO 1

UN SERVIDOR, AISLADO

El piloto corre en una red separada, por un periodo acotado y sin tocar su producción.

PASO 2

APRENDE LO QUE YA CORRE

Abzu captura lo que hoy funciona y lo convierte en recetas: migrar deja de ser un salto al vacío.

PASO 3

CRECE POR OLAS

Servicio a servicio, con la recuperación probada en cada paso antes de avanzar.

El contexto: 266 instituciones del país operan bajo el marco NORTIC.

SEGRD

Su infraestructura, en aguas seguras.

Solicite el piloto para su primer servidor y vea la primera restauración verificada con sus propios datos.

segrd.com

ABZU · UNA PLATAFORMA SEGRD