WHITEPAPER · PRIMERA EDICIÓN

Lo que no es visible en internet, no se puede atacar.

La ciberseguridad que elimina tu superficie de ataque externa. Presentada en España por **Kapres Technology**, partner oficial de Capzul.

Kapres Technology | CAPZUL

Madrid · 2026

EL PROBLEMA

Proteges lo que **sigue siendo visible**

El modelo dominante asume que la brecha es inevitable: **detectar, defender, responder.**

Se acumulan capas de seguridad sobre una infraestructura que sigue expuesta y, por tanto, atacable. Mientras tu servidor tenga IP pública, puertos abiertos y DNS, siempre habrá algo que escanear, enumerar y atacar.

Incidentes como la caída global de CrowdStrike demostraron la fragilidad del enfoque reactivo: cada capa añade complejidad y nuevas dependencias que pueden fallar por sí mismas.

+75 %

más ataques semanales por organización (interanual)

€75.000

coste medio de un incidente para una empresa española

Fuentes: informes sectoriales de ciberseguridad 2024; coste de incidente en España.

EL CAMBIO

No una capa más.
Un cambio de paradigma.

Las soluciones tradicionales y Capzul no juegan al mismo juego.

ENFOQUE TRADICIONAL

Protege lo que existe.

VPN, firewalls y Zero Trust cifran el canal y filtran el tráfico, pero dejan la infraestructura visible y direccionable.

Siempre queda un objetivo que escanear, y una capa más que mantener.

CON CAPZUL

Elimina el objetivo.

Capzul hace que, para el atacante, tu servidor no exista: sin IP pública, sin puertos, sin DNS.

No compite con tu stack de seguridad: se sitúa un paso antes, eliminando la superficie de ataque en su origen.

LA TECNOLOGÍA

Eliminar lo que **no puede ser atacado**

Los servidores protegidos no son direccionables desde internet. La única vía de acceso es el canal propietario de Capzul, y solo para clientes verificados: **primero identidad y autorización; después, y solo entonces, alcanzabilidad.**

CNCP
Capzul Network Communication Protocol

Transporte propietario, poscuántico y sin certificados. Sustituye por completo a TLS + VPN + PKI.

CSE
Capzul Security Engine

Blinda el endpoint: aunque comprometan el host, ni la lógica ni las claves pueden extraerse ni reutilizarse.

LA CADENA DE PROTECCIÓN

Usuario → Client → Capzul Link → Front-end → App protegida

El cliente nunca se conecta directamente al servidor: permanece aislado e invisible.

CÓMO FUNCIONA

De la exposición **a la invisibilidad**

Capzul no añade otra capa de defensa: **retira el objetivo del mapa.**

INTERNET · ATACANTES

No encuentran nada que atacar

- ✕ Escaneo de puertos
- ✕ Enumeración DNS
- ✕ Reconocimiento
- ✕ DDoS

✕ Tráfico no autorizado: bloqueado

CAPA CAPZUL

Sin IP pública · Sin puertos de entrada · Sin DNS público · Solo CNCP autenticado

✓ Sesión verificada: acceso permitido

TU INFRAESTRUCTURA

Invisible por fuera. Operativa por dentro.

- Servidores
- Bases de datos
- Aplicaciones
- Agentes de IA

ACCESO SOLO PARA AUTORIZADOS

- **Equipos internos** — Usuarios y administradores
- **Sedes y nubes** — Enlaces site-to-site
- **Terceros y remotos** — Partners y mantenimiento

✓ Superficie cero | ✓ No escaneable | ✓ Sin tocar tu app | ✓ Trazabilidad total

PORTFOLIO

Una tecnología, **cuatro soluciones**

01 CapzulProtect

Aísla el servidor y lo hace invisible en internet, manteniéndolo plenamente funcional. Para servidores críticos, ERPs y sistemas on-premise.

02 CapzulConnect

Alternativa superior a la VPN: conecta sedes y centros de datos con enlaces invisibles, sin exponer red ni asumir su complejidad.

03 Capzul AI Connect

Comunicación privada entre agentes de IA sobre MCP, mediante un túnel sigiloso, punto a punto y poscuántico.

04 CapzulFrontier

Appliance edge que integra Connect y Protect en un micro centro de datos de bajo consumo.

Y para integradores, **Capzul Core Technology**: la tecnología base, desplegable a medida e interoperable.

CASOS REALES

Ya funciona **en producción**

Mismo patrón en todos: eliminar la exposición pública sin tocar la aplicación ni parar el servicio.

Servicios financieros · Procesamiento de pagos

Endpoints de pago sin exposición pública y cada salto, del checkout a la liquidación, autenticado.

Checkout < 1 s bajo carga máxima · rotación de claves OTA · sin cambios en la app

Agentes de IA sobre MCP · Vehículo eléctrico

Servicios MCP fuera de la internet abierta; cada salto agente-servicio viaja por CNCP autenticado.

Semántica MCP intacta · sin tocar firewall ni código · sin downtime

Cadena de suministro · Logística sanitaria

Almacenes y edge en campo sin servicios SSH/HTTPS expuestos, preservando trazabilidad y serialización.

Cumplimiento reforzado · menor coste total · auditorías más simples

Fuente: casos de estudio de Capzul (2026), anonimizados.

LA PRUEBA

Lo pusimos a prueba **ante el mundo**

En **InfoSecurity Europe 2025** (Londres, +13.000 profesionales), Capzul retó a cualquiera a localizar y comprometer un servidor protegido. Recompensa: **25.000 £.**

72 h

de ataques desde todo el mundo

+1.000/s

picos de intentos por segundo

0

vulneraciones. Premio no reclamado.

No fue casualidad: repitió el resultado impecable del Hackathon de 2024 (+100 equipos, 48 h). Y en 2025 Capzul recibió el **Intellyx Digital Innovator Award.**

> *"Cuando no hay un servidor visible, no hay un objetivo que atacar. Para un decisor, es evidencia tangible, no una promesa de marketing."*

CUMPLIMIENTO

NIS2 y DORA: **riesgo que desaparece**

Al eliminar la superficie de ataque, Capzul reduce la probabilidad y el impacto de los incidentes que ambas normativas obligan a gestionar.

NIS2

Obligatoria para medianas y grandes empresas en sectores críticos. Al no ser direccionable la infraestructura, la exposición a incidentes cae drásticamente.

DORA

Resiliencia operativa del sector financiero y gestión del riesgo de terceros. La eliminación de la superficie refuerza la resiliencia y reduce incidentes.

Por diseño: segregación de controles (CNCP + CSE) independientes del perímetro, migración por fases sin reescribir aplicaciones y auditabilidad mediante registros de decisión sin exponer datos sensibles.

POR QUÉ AHORA

Tu superficie de ataque es **el mayor riesgo evitable**

Mientras tu infraestructura siga siendo visible, seguirá siendo un objetivo. Capzul ofrece una vía probada para eliminar ese riesgo en su origen. El primer paso es sencillo.

1 · Diagnóstico de exposición

Identificamos qué activos críticos están hoy accesibles desde internet.

2 · Demo técnica

Vemos, sobre tu entorno, cómo Capzul los haría invisibles.

HABLEMOS

Da el primer paso **con Kapres**

Kapres Technology

Partner oficial de Capzul en España

Barcelona: Av. Diagonal, 131. 08018

Canarias: Avda El Puente, 29, Santa Cruz de La Palma, 38700.

Madrid: Calle Vía de los Poblados 1, Edificio C, Planta 1ª, oficina 21B. 28033. (Sede central)

+34 919 351 031 · info@kapres.es · kapres.es

Lo que no se ve,
no se puede atacar.