



Desafíos de las compras públicas de ciberseguridad

Cristián Céspedes Viñuela, director (S) de ChileCompra

Seminario Ciberseguridad en las Compras Públicas · 21 de octubre de 2026

ChileCompra



Mercado Público es infraestructura crítica del Estado

ChileCompra

Si la plataforma se detiene, se ven afectadas las compras de hospitales, municipios y servicios

US\$ 21.953 millones

transados al año, más del 6% del PIB

~100 mil

proveedores, en su mayoría empresas de menor tamaño

1,8 millones

de órdenes de compra al año

1.165

organismos del Estado compran en Mercado Público

Detrás de cada compra pública hay una persona esperando un servicio

01

Lo que nos enseñó el ciberataque de 2023

Un ataque a nuestro proveedor dejó fuera de línea a Mercado Público

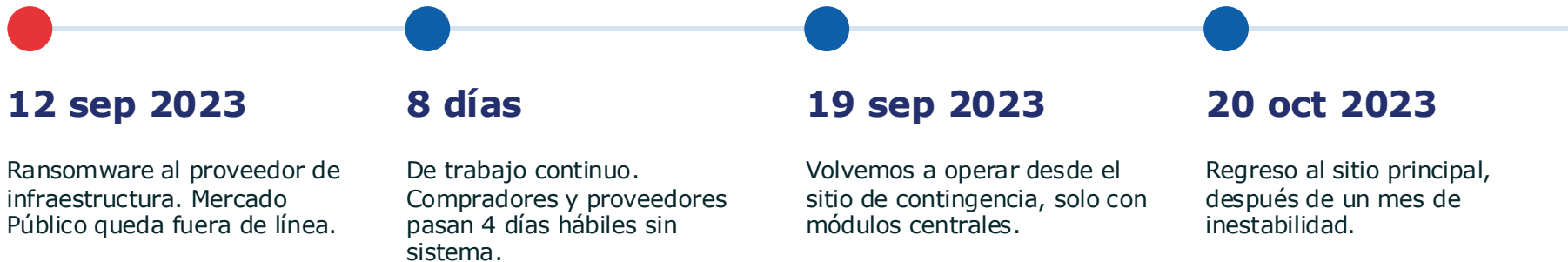




12 de
septiembre de
2023

12 de septiembre de 2023: sin plataforma por un ataque a un proveedor

No fue un ataque directo a ChileCompra: fue un ataque a la cadena de suministro



Apoyo clave: CSIRT de Gobierno, Secretaría de Gobierno Digital, SII y DIPRES trabajaron junto a nuestros equipos desde el primer día.

Las compras siguieron y la competencia se mantuvo

Lo que muestran los datos de Mercado Público sobre la caída de 2023

4 días hábiles

sin plataforma. La contingencia operó con los módulos centrales y algunos procesos se postergaron.

+\$150 mil millones

en compras postergadas, que se transaron en su totalidad entre el 20 de septiembre y el 31 de octubre.

Más licitación pública

Se transó más por licitación y menos por Compra Ágil y Convenio Marco: la competencia no se resintió.

Sin alza del trato directo

La participación de proveedores se mantuvo y no aumentó la discrecionalidad.

Las compras públicas no se detuvieron y se recuperaron sin afectar la competencia ni la participación.

Cuatro lecciones que orientan nuestra estrategia

1 El riesgo entra por los proveedores

Los contratos deben exigir estándares, aviso de incidentes y devolución de la información.

2 Contingencia sin capacidad no sirve

El sitio de respaldo debe poder operar a plena carga, y hay que probarlo.

3 El Estado coordinado puede más

CSIRT, SII, DIPRES y Gobierno Digital resolvieron juntos lo que solos no podíamos.

4 El riesgo cero no existe

Lo central es recuperarse rápido y seguir operando: DRP y BCP.

02

Cómo nos transformamos

Estrategia de modernización tecnológica y ciberseguridad.

ChileCompra



Incidente de infraestructura y paso a la nube elástica

Caída principal:

El ataque al proveedor obligó a activar la contingencia.

Límite del DRP:

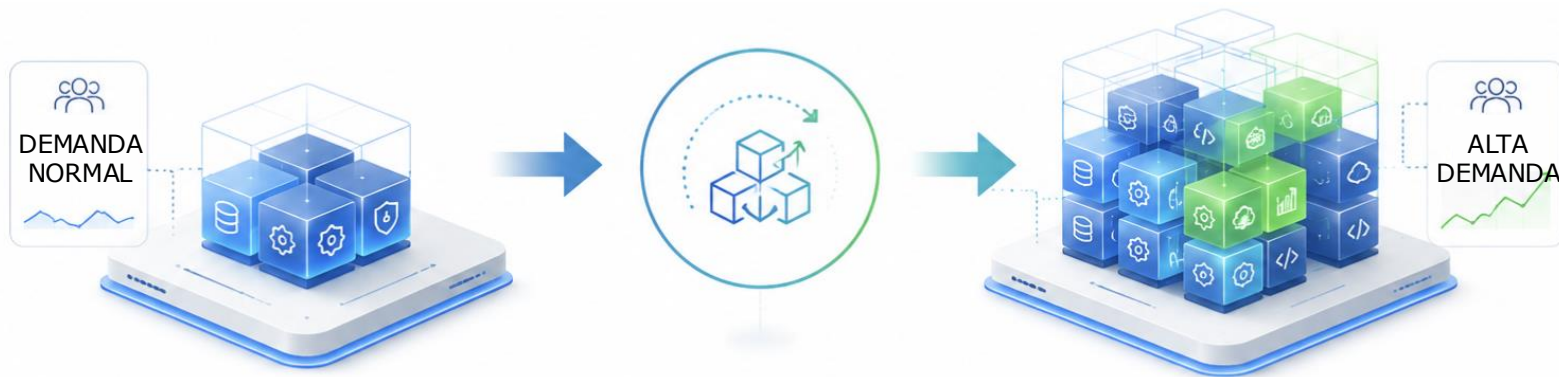
El sitio secundario replicaba datos, pero con menos capacidad, y colapsó con el tráfico real.

Solución de emergencia:

Hubo que sumar infraestructura urgente y cara para volver a operar.

Estrategia en la nube:

Un DRP elástico en la nube reemplazó a equipos ociosos y caros.



Estrategia en la nube para escalar con la reforma



Cambio normativo:

La ley de compras pasó de 39 a 103 artículos.

La nube como necesidad:

Arquitectura nativa en la nube y elástica, que escala en los peaks de tráfico y mantiene bajos los costos operativos base.



Aumento del volumen de operación:



+35%
organismos
compradores



+30%
transacciones



+20%
proveedores



+22%
usuarios
concurrentes

Elasticidad desde el diseño

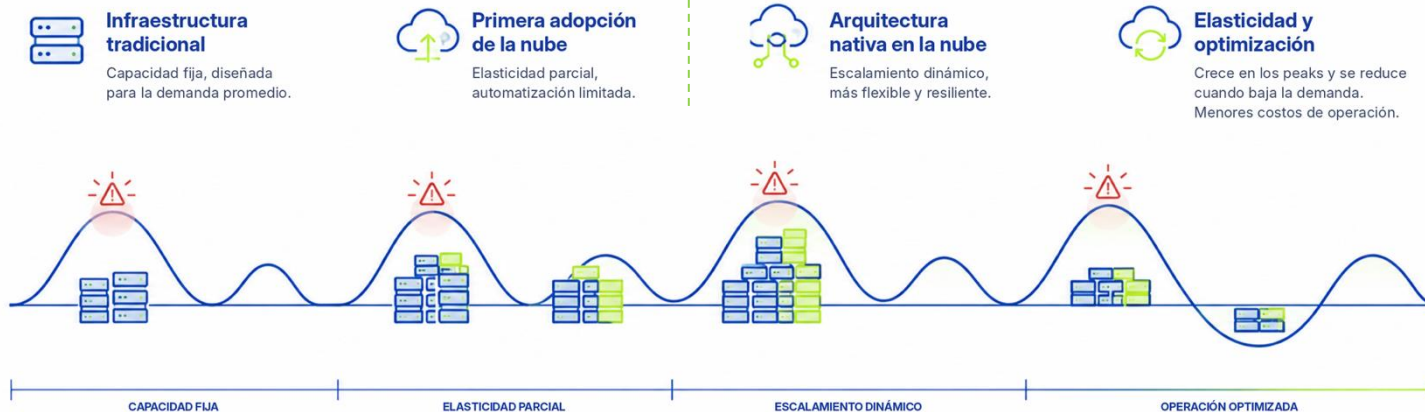
Migrar a la nube es adoptar una arquitectura nativa en la nube, que se adapta a la demanda.

Infraestructura física tradicional

Capacidad fija: provoca caídas y cuellos de botella en los peaks de tráfico.

Elasticidad en la nube: escalamiento automático

- **Escalamiento inmediato:** amplía la capacidad en los peaks y la reduce cuando baja la demanda.
- **Eficiencia fiscal:** disponibilidad 24/7 sin pagar por infraestructura ociosa.



MODERNIZACIÓN TECNOLÓGICA Y
CIBERSEGURIDAD

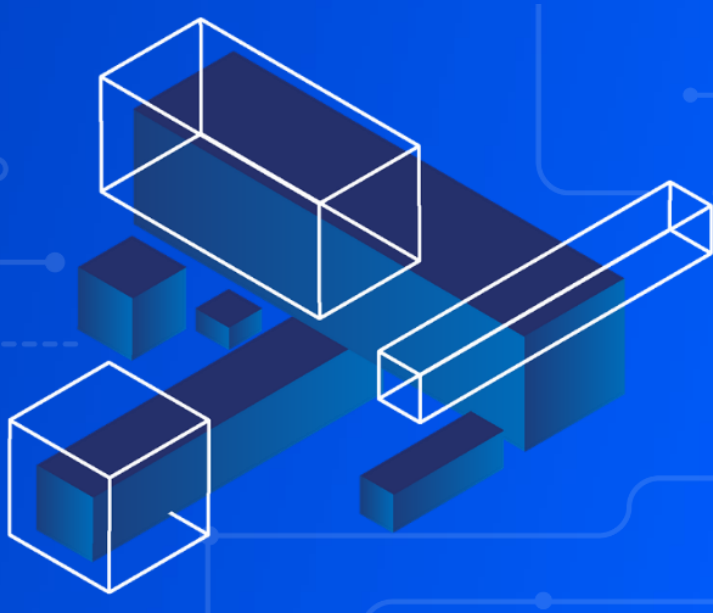
ChileCompra

Arquitectura modular

Migración a una plataforma multinube con altos estándares de seguridad y resiliencia.

12 de junio de 2025

Lanzamos la nueva plataforma modular de compras públicas con la Subasta Inversa Electrónica.



03

Lo que proponemos al Estado

Una directiva de ciberseguridad y
una compra coordinada



Las compras públicas como motor de resiliencia

Más que eficiencia: una herramienta para la seguridad del país

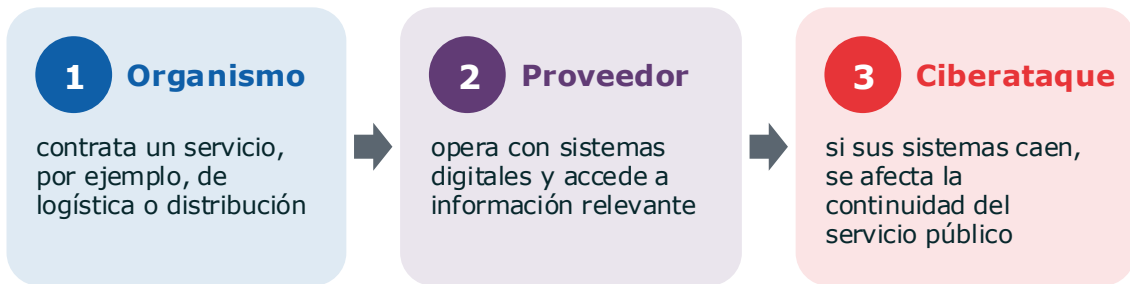
Poder de compra del Estado

US\$ 21 mil millones

al año en compras públicas

Esa escala permite influir en el comportamiento de los proveedores, fijar estándares comunes e impulsar mejores prácticas en todo el mercado.

La ciberseguridad va más allá de la tecnología que compramos



Hay que evaluar el riesgo en toda la cadena de suministro, incluso cuando la tecnología no es el objeto principal de la compra.

Contratación pública estratégica: un enfoque que la OCDE promueve en gestión de riesgos y resiliencia de las cadenas de suministro.

Hoy el Estado compra ciberseguridad de forma fragmentada

Órdenes de compra de ciberseguridad, enero 2025 a mayo 2026

US\$ 10,6 millones

en 283 órdenes de compra

150

instituciones compradoras

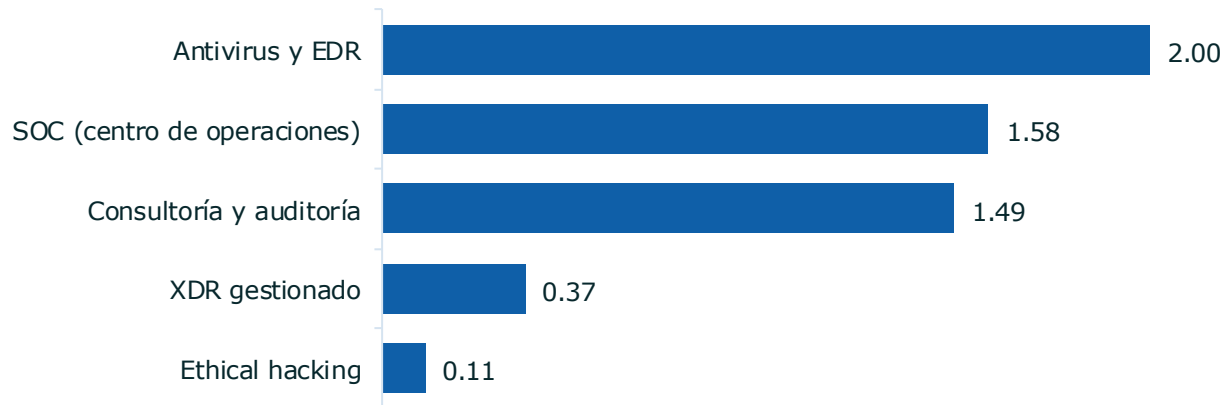
96

de ellas compraron una sola vez

US\$ 5.900

monto mediano por línea de compra

Monto por tipo de servicio (US\$ millones)



PAC 2026: US\$ 4,4 millones declarados como ciberseguridad. Buena parte del gasto queda dentro de contratos TI más amplios.

Fuente: ChileCompra, análisis de órdenes de compra de ciberseguridad en Mercado Público. Antivirus y EDR, monto aproximado.

Directiva pionera: ciberseguridad en cada etapa de la compra

La primera de ChileCompra en ciberseguridad

7

riesgos típicos de las contrataciones

6

criterios para elegir qué exigir

17

cláusulas tipo listas para las bases

Planificación

Bases

Evaluación

Ejecución

Término

Alineada con la Ley N° 21.663: su artículo 9 obliga a los jefes de servicio a exigir a sus proveedores TI que compartan información sobre vulnerabilidades e incidentes.

Referencial y proporcional: cada organismo elige las cláusulas según el riesgo de su compra y las asocia a sanciones en las bases.

Siete riesgos potenciales asociados a un proveedor

La directiva parte por identificarlos en cada contratación

1

Accesos no autorizados

Credenciales o permisos mal controlados abren la puerta a sistemas e información.

2

Filtración de información

Datos personales o confidenciales expuestos, perdidos o divulgados.

3

Servicio interrumpido

Un incidente en el proveedor detiene la operación del organismo.

4

Vulnerabilidades

Software o equipos con fallas de seguridad que alguien puede explotar.

5

Incidentes mal gestionados

Sin aviso ni coordinación, la respuesta llega tarde.

6

Dependencia del proveedor

Sin portabilidad, recuperar los datos o cambiar de plataforma se vuelve difícil.

7

Falta de supervisión

Sin auditorías ni evidencias, no hay cómo verificar lo comprometido.

¿Qué cláusulas pido?

Cinco preguntas

Cada «sí» suma cláusulas a las bases de la compra

Punto de partida: ¿la compra involucra información, sistemas o servicios TI? Si es así, sigue las preguntas.

1

¿Tratará información o datos personales?

Sí

1 Confidencialidad

3 Eliminación segura

17 Restitución de datos

2

¿Accederá a sistemas o redes?

Sí

4 Acceso a sistemas

5 Equipos propios

11 Cambios de personal

3

¿Es un servicio crítico?

Sí

2 Aviso de incidentes

7 Cooperación

9 Vulnerabilidades

4

¿Genera dependencia (nube, hosting)?

Sí

10 Cambios de infraestructura

15 Política de seguridad

16 Inscripción ANCI*

5

¿Hay que supervisarlos?

Sí

6 Auditorías

8 Contraparte

12 Software

13 Reuniones

14 Comunicación oficial

* Si el oferente es operador de importancia vital o presta servicios esenciales. Ejemplo de la directiva: un servicio de hosting suma las cláusulas 10 y 16. Siempre: asociar cada cláusula a sanciones en las bases.

Comprar juntos para pagar menos y proteger mejor

Primera compra coordinada de ciberseguridad: licencias XDR

Compras coordinadas 2026

29%

de ahorro respecto del precio
presupuestado

**US\$ 17,7
millones**

ahorrados por el Estado

¿Por qué este servicio?

1

Una necesidad común

Todos los organismos deben proteger sus equipos y servidores frente a ransomware y malware. Al agregar la demanda se buscan mejores precios y condiciones.

2

El estándar de la ANCI

El estándar técnico incorpora sus recomendaciones: los organismos acceden a una seguridad más alta y homogénea.

Licencias XDR: qué incluye y cómo sumarse

Inscripción abierta hasta el 2 de noviembre

¿Qué es XDR?

Un sistema de ciberseguridad inteligente que conecta y analiza la información de dispositivos, redes y correos para detectar y detener ataques de forma automática, antes de que causen daño.

La compra incluye

Licencias

para estaciones de trabajo y servidores

Capacitación

y soporte técnico

Puesta en marcha

instalación y configuración

12 + 12 meses

contrato renovable

17 proveedores

participaron en la consulta al mercado

ChileCompra + ANCI

definieron juntos el estándar técnico

Oficio N° 22 de DIPRES: los organismos que requieran este servicio deben adquirirlo por esta compra coordinada.

Chile abre camino en las compras públicas de ciberseguridad

ChileCompra

Hasta donde hemos revisado entre nuestros pares, no hay otros sistemas de compras públicas con una directiva específica de ciberseguridad ni una compra coordinada de estos servicios.

La ciberseguridad es gobernanza

Dejó de ser un tema solo tecnológico: es un desafío de gestión institucional.

Las compras públicas son una palanca

Buena parte del riesgo entra por los contratos; ahí podemos subir el estándar.

Nadie tiene que hacerlo solo

ANCI, Contraloría, DIPRES y ChileCompra entregan lineamientos, herramientas y acompañamiento.

No se trata solo de comprar más barato: se trata de comprar mejor, reducir riesgos y construir un país más resiliente.



Muchas gracias

www.chilecompra.cl

ChileCompra

