HIGH LEVEL

2026

CERO LICENCIAS, CONTROL TOTAL

MONITOREO Y CIBERDEFENSA

PARA EL SECTOR PÚBLICO

Transformamos tecnología abierta
en valor público y control total.

Prepared By:
Ing, Limber Cumara

Tabla de Contenidos

INTRODUCCIÓN

En un contexto donde los ciberataques contra instituciones públicas crecen cada trimestre, monitorear la infraestructura tecnológica ya no es un lujo técnico: es una necesidad operativa y, pronto, una obligación normativa.

Este documento presenta una arquitectura de monitoreo y ciberdefensa construida enteramente con software libre, probada en una institución del Estado boliviano, y pensada para replicarse en cualquier entidad pública que hoy no tenga visibilidad real de lo que ocurre en su red.

Qué encontrarás en este documento

A lo largo de estas páginas vas a conocer:

- Los problemas de seguridad y monitoreo que hoy enfrentan la mayoría de las instituciones públicas, respaldados con datos reales de los últimos años.
- El marco normativo boliviano que ya establece un plazo para migrar a software libre.
- Una arquitectura completa de monitoreo, detección y respuesta a amenazas, explicada en términos simples.
- Un catálogo de diez herramientas de código abierto, qué hace cada una y qué beneficio concreto aporta.
- Resultados reales, medidos, de una implementación ya en funcionamiento.
- Los pasos concretos para llevar esta misma solución a tu institución.

Por qué esto importa ahora

Bolivia gestiona cientos de ciberataques cada trimestre contra entidades públicas, y una parte importante de ellos ocurre porque nadie los detecta a tiempo: credenciales institucionales terminan vendiéndose en la Dark Web, vulnerabilidades conocidas quedan sin corregir durante meses, y los registros de actividad quedan dispersos en sistemas que nadie correlaciona.

A esto se suma un plazo normativo concreto: el Estado boliviano ya definió que todas las entidades públicas deben migrar a software libre y estándares abiertos. Esto no es una recomendación a futuro — es una hoja de ruta con fecha límite.

Este documento no es una propuesta teórica. Es una guía basada en una implementación real, con herramientas que no requieren pago de licencia, y con un camino claro para que tu institución deje de operar a ciegas.

LOS PROBLEMAS QUE YA ESTÁN ENFRENTANDO LAS INSTITUCIONES

Panorama regional y boliviano, en cifras

- El Centro de Gestión de Incidentes Informáticos (CGII) de Bolivia gestiona cientos de ciberataques contra entidades públicas cada trimestre, y la tendencia va en aumento: 215 casos en el segundo trimestre de 2024, 325 en el tercero, y más de 300 durante buena parte de 2025. Los incidentes más frecuentes no son ataques sofisticados: son accesos no autorizados, credenciales institucionales vendiéndose en la Dark Web, y vulnerabilidades básicas como fallas de inyección SQL que representaron más de la mitad de las vulnerabilidades críticas detectadas en 2025.
- A nivel regional, el panorama confirma que Bolivia no es un caso aislado: América Latina cerró 2025 como la región más afectada por ransomware a nivel mundial, con el 8,13% de las organizaciones registrando este tipo de ataques (Kaspersky, 2026). El costo promedio de una filtración de datos en la región alcanzó los US$2,46 millones (IBM Security, 2023), y seis de cada diez empresas latinoamericanas no cuentan con un plan formal de respuesta a incidentes (Forrester, 2024).

Los patrones que se repiten una y otra vez

Detrás de las cifras, los mismos problemas aparecen institución tras institución:

1. **No hay visibilidad real.** Nadie sabe qué está pasando en la red hasta que el daño ya ocurrió.
2. **Los registros están dispersos.** Cada sistema guarda sus propios logs, sin que nadie los cruce ni los correlacione.
3. **Las credenciales se filtran antes de que la institución se entere.** Usuarios y contraseñas terminan a la venta en la Dark Web mientras el área de sistemas sigue sin saberlo.
4. **Vulnerabilidades conocidas quedan sin corregir.** Configuraciones por defecto y fallas básicas siguen abiertas durante meses.
5. **Cuando ocurre el incidente, se improvisa.** No existe un proceso definido de respuesta, y cada minuto sin reaccionar aumenta el daño.

ESTOS NO SON RIESGOS HIPOTÉTICOS. SON LOS PROBLEMAS QUE, CON DISTINTOS NOMBRES, APARECEN EN LOS REPORTES TRIMESTRALES DE BOLIVIA

Fuente: Centro de Gestión de Incidentes Informáticos (CGII) – AGETIC, Informes de Gestión de Incidentes y Vulnerabilidades Informáticas, 2do y 3er trimestre de 2024.

EL RESPALDO NORMATIVO

Ley 164 y el plazo del PISLEA

En Bolivia, la adopción de software libre en las entidades públicas no es una preferencia técnica: es un mandato legal. La Ley N.º 164, de Telecomunicaciones y Tecnologías de Información y Comunicación, establece que los Órganos Ejecutivo, Legislativo, Judicial y Electoral, en todos sus niveles, deben priorizar el uso de software libre y estándares abiertos, en el marco de la soberanía y la seguridad nacional.

Este mandato se reglamentó y se actualizó con el tiempo. El más reciente Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA), aprobado en enero de 2025, fija un plazo concreto: todas las entidades públicas deben concluir su migración a software libre y estándares abiertos antes del 12 de enero de 2030.

Esto cambia la conversación con cualquier institución. La pregunta ya no es si conviene adoptar herramientas de código abierto para monitoreo y ciberseguridad, sino qué tan preparada está la institución para cumplir un plazo que ya corre.

Lo que esto significa en la práctica

- Toda inversión en herramientas de código abierto para monitoreo y seguridad no es un gasto adicional: es avance directo hacia el cumplimiento de una obligación normativa vigente.
- Las entidades que empiecen antes tienen más tiempo para capacitar a su personal, ajustar procesos y validar resultados — las que esperen al límite del plazo tendrán que migrar bajo presión.
- Una arquitectura como la que se presenta en este documento no solo resuelve el problema de visibilidad y seguridad: también deja a la institución con evidencia concreta de avance en su plan de migración institucional.

En otras palabras: la ventana de tiempo para adoptar esta solución con calma, en vez de por obligación de último momento, está abierta ahora.

LA ARQUITECTURA

Cómo funciona

La solución no es una herramienta aislada, sino tres capas que trabajan juntas: una observa el estado de la infraestructura, otra detecta amenazas, y una tercera organiza la respuesta cuando algo requiere acción. Cada capa alimenta a la siguiente, así que la institución pasa de "no sabíamos que esto estaba pasando" a "esto pasó, así reaccionamos" en un solo flujo, no en sistemas sueltos que nadie conecta.

Las 3 capas de protección

Monitoreo y visualización

Vigila en tiempo real servidores, redes, servicios y bases de datos, y muestra todo en paneles centralizados.

Detección de amenazas

Analiza logs, tráfico de red y vulnerabilidades para identificar accesos indebidos, malware y comportamientos anómalos.

Respuesta Inteligente + Automatización

Organiza los incidentes detectados, los enriquece con inteligencia de amenazas, y automatiza tareas de configuración y respuesta para reducir el tiempo de reacción.

Beneficios directamente entregados

- El estado de cada servidor, servicio y dispositivo crítico, en un solo panel.
- Alertas automáticas ante caídas, accesos sospechosos o tráfico anómalo.
- Un registro centralizado de todo lo que antes estaba disperso entre sistemas.
- Una base para empezar a automatizar tareas que hoy se hacen a mano.

Qué se requiere para sostener esto en el tiempo

- Personal técnico con disponibilidad para monitorear alertas y dar seguimiento a incidentes.
- Capacitación inicial del equipo en las herramientas (incluida en la fase de implementación).
- Actualización periódica de reglas y fuentes de inteligencia de amenazas.

CATÁLOGO DE HERRAMIENTAS | ZABBIX

Zabbix es el punto de partida de todo el sistema: antes de detectar una amenaza o resolver un incidente, primero hay que saber si la infraestructura está funcionando como debería. Eso es exactamente lo que resuelve — visibilidad constante sobre cada componente crítico de tu red.

¿Qué es Zabbix?

Zabbix es la capa que le da a tu equipo de sistemas ojos sobre toda la infraestructura tecnológica, sin importar su tamaño. Se adapta igual de bien a una entidad con pocos servidores que a una con cientos de equipos distribuidos. Lo que vigila incluye:

- Redes y dispositivos: confirma que el tráfico circula con normalidad y que ningún equipo quedó fuera de línea sin que nadie se entere.
- Servidores y sistemas operativos: mide el uso de recursos y anticipa saturaciones antes de que se conviertan en una caída de servicio.
- Aplicaciones y servicios críticos: verifica que estén disponibles y respondiendo, no solo "encendidos".
- Bases de datos: detecta cuellos de botella antes de que afecten a los usuarios finales.

Beneficios del monitoreo con Zabbix

1. **Nada pasa desapercibido.** Cualquier caída o comportamiento anómalo se detecta en el momento en que ocurre, no horas o días después.
2. **Alertas que se ajustan a tu operación.** Cada institución define qué umbrales le importan — Zabbix avisa exactamente sobre eso, sin ruido innecesario.
3. **Crece con la institución.** Empieza cubriendo lo esencial y se amplía sin rehacer nada, a medida que la infraestructura se vuelve más compleja.

CATÁLOGO DE HERRAMIENTAS | wazuh.

Si **Zabbix** cubre el monitoreo del rendimiento, **Wazuh** entra en juego para **asegurar la seguridad de tu infraestructura IT. Wazuh** es una **plataforma de detección de intrusiones** (**IDS**) que permite identificar actividades sospechosas y responder ante incidentes de seguridad de manera automática.

¿Qué es Wazuh?

Wazuh es una herramienta de monitorización de seguridad que se enfoca en la **protección proactiva** de los sistemas. Mientras Zabbix te ayuda a ver el estado de los dispositivos y aplicaciones, **Wazuh** te permite **detectar y prevenir** amenazas.

Algunas de las capacidades que ofrece incluyen:

Seguridad del Endpoint

- Evaluacion de la configuración
- Detección de Malware
- Monitoreo de la integridad de los archivos

Inteligencia de amenazas

- Caza de amenazas.
- Análisis de logs.
- Detección de Vulnerabilidades

Operaciones de seguridad

- Respuesta ante incidentes
- Cumplimiento normativo
- Higiene Informática

Seguridad en la nube

- Seguridad de contenedores
- Gestión de la postura.
- Protección de la carga de trabajo

CATÁLOGO DE HERRAMIENTAS | Grafana

Zabbix y Wazuh generan datos constantemente — el problema real es que esos datos, sin un lugar donde verlos juntos, terminan dispersos entre pantallas distintas. **Grafana** es la pieza que junta todo eso en un solo lugar, para que una persona pueda **entender el estado completo de la infraestructura de un vistazo**, sin abrir cinco sistemas distintos.

¿Qué es Grafana?

Grafana toma la información que producen Zabbix y Wazuh (y cualquier otra fuente de datos que se sume después) y la convierte en paneles visuales pensados para decisiones rápidas, no para leer líneas de texto plano. No reemplaza a las otras herramientas — las hace legibles.

Beneficios de Grafana

1. **Un solo panel, toda la infraestructura:** El estado de servidores, redes y alertas de seguridad conviven en una misma pantalla, sin cambiar de sistema.
2. **Decisiones más rápidas:** Cuando un problema se ve antes de que alguien tenga que reportarlo, se actúa antes también.
3. **Un panel que crece con el sistema:** A medida que se suman nuevas fuentes de datos (como MISP o TheHive más adelante), Grafana las integra sin necesidad de rediseñar nada.

CATÁLOGO DE HERRAMIENTAS

Hasta ahora, Wazuh vigila lo que pasa dentro de tu infraestructura. Pero muchas amenazas ya son conocidas antes de que lleguen a tocar tus sistemas — solo que nadie te avisó. MISP es la pieza que conecta a tu institución con ese conocimiento colectivo: indicadores de amenazas ya identificados por otras organizaciones, en tiempo real.

¿Qué es MISP?

MISP es una plataforma de inteligencia de amenazas que centraliza y comparte indicadores de compromiso — direcciones IP maliciosas, dominios fraudulentos, hashes de archivos infectados, patrones de ataque conocidos. En vez de que tu institución descubra una amenaza por las malas, MISP te permite reconocerla apenas aparece, porque ya fue identificada en otro lugar. Sus capacidades incluyen:

- **Indicadores de compromiso (IOCs):** IPs, dominios, URLs y archivos ya vinculados a actividad maliciosa conocida.
- **Comunidades de intercambio:** acceso a feeds de amenazas compartidos por organismos de ciberseguridad y otras instituciones, públicas y privadas.
- **Correlación automática:** cruza la información entrante con lo que ya ocurre en tu red, sin trabajo manual.
- **Alimentación directa a Wazuh:** convierte esa inteligencia externa en reglas de detección activas dentro de tu propio sistema.

Beneficios de MISP

1. **Te enteras antes, no después.** La institución conoce una amenaza en cuanto se identifica en cualquier parte del mundo, no cuando ya la afectó.
2. **Menos trabajo de investigación manual.** El cruce entre lo que pasa en tu red y las amenazas conocidas ocurre automáticamente.
3. **Conecta a tu institución con una comunidad más grande.** En vez de defenderse sola, tu institución se beneficia de lo que ya detectaron otras.

CATÁLOGO DE HERRAMIENTAS | TheHive

Una alerta que nadie gestiona formalmente termina siendo un **mensaje perdido en un chat** o un correo que alguien vio "**de pasada**". **TheHive** es donde cada amenaza detectada — venga de Wazuh, de MISP o de cualquier otra fuente — deja de ser una alerta suelta y **se convierte en un caso con dueño**, con pasos y con cierre.

¿Qué es TheHive?

TheHive es la plataforma donde tu equipo gestiona la respuesta a incidentes de seguridad de forma ordenada. Cuando llega una alerta, no se resuelve "de memoria" ni por WhatsApp: se abre un caso, se documenta cada acción tomada, se asigna un responsable y queda registro de cómo se cerró. Esto incluye:

- **Gestión centralizada de casos:** cada incidente de seguridad tiene un espacio propio, con toda su evidencia y su historial en un solo lugar.
- **Asignación de responsables:** se sabe siempre quién está a cargo de resolver qué, sin ambigüedad.
- **Plantillas de respuesta:** procedimientos estandarizados para los tipos de incidente más comunes, en vez de improvisar cada vez.
- **Integración directa con MISP y Wazuh:** las alertas llegan automáticamente como casos, listas para investigarse.

Beneficios de TheHive

1. **Ningún incidente se pierde ni se olvida.** Todo queda registrado desde que se detecta hasta que se cierra.
2. **Trazabilidad completa.** Si alguna vez hay que rendir cuentas de cómo se manejó un incidente, la evidencia ya está documentada.
3. **Respuesta más rápida y consistente.** El equipo sigue un proceso claro en vez de reaccionar de forma distinta cada vez.

CATÁLOGO DE HERRAMIENTAS | Cortex

Cuando se abre un caso en TheHive, alguien tiene que investigar: **¿esta IP es realmente maliciosa? ¿este archivo es peligroso?** Hacer esa verificación a mano, consultando una por una distintas fuentes externas, consume tiempo que en un incidente real no sobra. **Cortex hace ese trabajo de forma automática.**

¿Qué es Cortex?

Cortex es el motor de análisis que se conecta a los casos de **TheHive** y responde preguntas de investigación en segundos: si una **IP tiene mala reputación, si un archivo coincide con malware conocido, si un dominio está asociado a actividad fraudulenta.** En vez de que un analista busque esa información manualmente en varias fuentes distintas, **Cortex la trae automáticamente al caso**. Entre sus capacidades están:

- **Análisis automático de indicadores:** IPs, dominios, archivos y hashes se verifican contra múltiples fuentes de reputación a la vez.
- **Enriquecimiento de casos:** cada investigación en TheHive se completa con contexto adicional, sin que nadie tenga que salir a buscarlo.
- **Reducción del tiempo de análisis:** lo que antes tomaba consultas manuales dispersas, ahora ocurre en el mismo flujo de trabajo.
- **Extensible:** se pueden sumar nuevos analizadores según las necesidades específicas de la institución.

Beneficios de Cortex

1. **Investigaciones más rápidas.** El contexto que un analista necesita llega solo, en vez de tener que salir a buscarlo.
2. **Menos margen de error humano.** El análisis automático es consistente, no depende de qué tan minucioso estuvo el analista ese día.
3. **Cierra el ciclo completo.** Con Cortex, la cadena MISP > Wazuh > TheHive > Cortex queda funcionando de punta a punta, sin pasos manuales sueltos.

RESULTADOS COMPROBADOS

Esta arquitectura no es una propuesta teórica — ya opera en una entidad del Estado boliviano, donde se implementó sobre servidores distribuidos por función: monitoreo, correlación de eventos, gestión de casos e inteligencia de amenazas, y automatización de tareas.

Qué mejoró, medido durante 3 meses de operación continua:

ASPECTO EVALUADO	RESULTADO
Funcionalidad del sistema	87,5%
Fiabilidad (continuidad del monitoreo)	95,3%
Usabilidad para el equipo técnico	79,4%
Seguridad (controles ISO/IEC 27001)	82,1%
Calidad total del sistema	86,08%

Lo que esto significó en la práctica:

- El monitoreo se mantuvo activo incluso ante la caída de nodos individuales, gracias a la tolerancia a fallos del sistema — la institución dejó de depender de un solo punto de falla.
- El personal técnico pudo operar los tableros del sistema con una curva de aprendizaje corta, sin necesidad de capacitación externa prolongada.
- Los tiempos de reacción ante incidentes se redujeron de forma medible, al pasar de detección manual y dispersa a alertas centralizadas y automáticas.
- La institución pasó de no tener visibilidad estructurada de su infraestructura a contar con un sistema evaluado formalmente bajo normas internacionales (ISO/IEC 25010 e ISO/IEC 27001).

CÓMO SE IMPLEMENTA

Fases y tiempos

La implementación sigue un ciclo de mejora continua (Planificar–Hacer–Verificar–Actuar), aplicado ya en un despliegue real:

PLANIFICAR

Relevamiento de la infraestructura actual, definición de servidores críticos a monitorear, y ajuste del alcance según el tamaño de la institución.

HACER

Instalación y configuración del núcleo: monitoreo (Zabbix + Grafana), detección (Wazuh), y después inteligencia de amenazas y respuesta a incidentes (MISP + TheHive + Cortex)

VERIFICAR

Pruebas de conectividad, validación de alertas, ajustes finales y evaluación funcional del sistema completo.

ACTUAR

Mejora continua: ajuste de reglas, incorporación de nuevas fuentes de monitoreo, y acompañamiento técnico.

Qué necesitamos de tu equipo

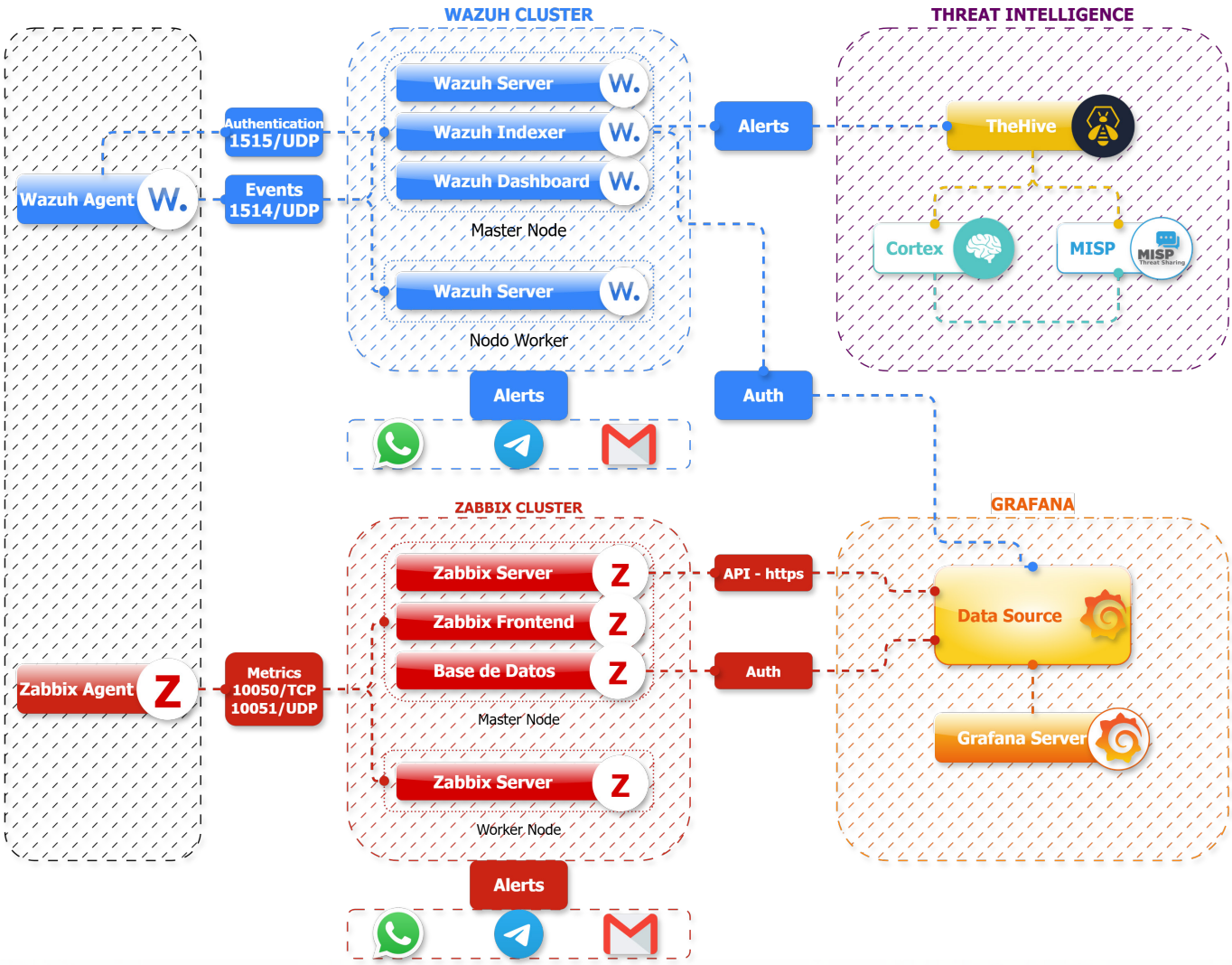
Segmentación de servidores según tamaño de la institución

Nivel	Endpoints	Servidores necesarios	Recursos por servidor
Básico	Hasta 50	1 servidor consolidado (todas las herramientas juntas)	**S_1:** 4 vCPU · 8 GB RAM · 120 GB
Intermedio	Hasta 100	2 servidores: (1) monitoreo, (2) detección + respuesta	**S_1:** 2 vCPU · 4 GB RAM · 80 GB **S_2:** 2 vCPU · 8 GB RAM · 100 GB
Avanzado	Hasta 150-200	3 servidores: (1) Monitoreo (2) SIEM principal (3) HA + respuesta e inteligencia	**S_1:** 2 vCPU · 4 GB RAM · 80 GB **S_2:** 2 vCPU · 8 GB RAM · 100 GB **S_3:** 2 vCPU · 4 GB RAM · 80 GB

El nivel Avanzado corresponde exactamente a la configuración ya validada en una entidad pública boliviana durante 3 meses de operación continua — no es una estimación teórica.

EL ECOSISTEMA COMPLETO

Cada herramienta que viste en el catálogo **no opera de forma aislada.** Así es como se conectan entre sí, procesan la información y la entregan al equipo.



1. **Clúster Wazuh.** Recibe eventos y datos de autenticación desde los agentes instalados, y envía alertas directamente a Threat Intelligence.
2. **Threat Intelligence (TheHive, Cortex, MISP).** Recibe las alertas de Wazuh, las enriquece y organiza como casos gestionables.
3. **Clúster Zabbix.** Monitorea métricas de infraestructura y las entrega a Grafana como fuente de datos.
4. **Grafana.** Centraliza la información de ambos clústeres en paneles visuales únicos.
5. **Notificaciones.** Cada alerta relevante llega automáticamente por WhatsApp, Telegram o correo electrónico, sin que nadie tenga que estar revisando pantallas de forma constante.

INVERSIÓN

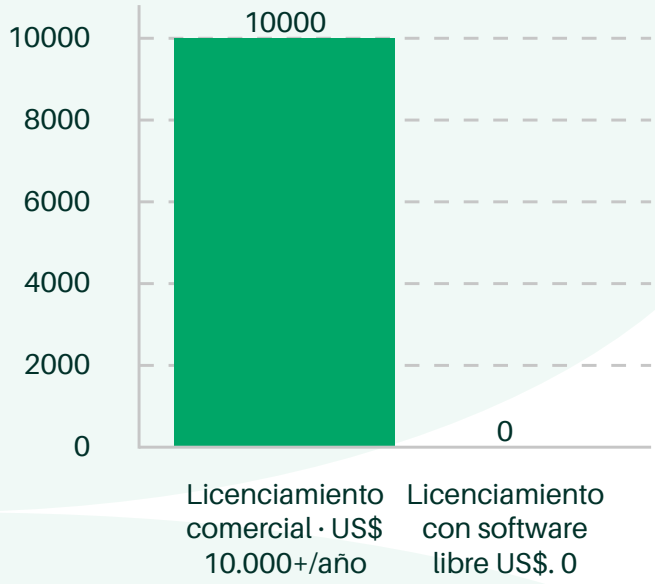
Esta arquitectura entrega la misma capacidad de monitoreo y detección que una solución comercial, sin el costo de licenciamiento que normalmente representa la mayor parte del presupuesto de un proyecto de este tipo.

Licencias

Software incluido: Zabbix, Grafana, Wazuh, MISP, TheHive, Cortex — licenciamiento: Bs. 0, sin límite de eventos por segundo ni de endpoints.

Referencia del mercado: un SIEM comercial de entrada cuesta entre Bs. 69.000 y Bs. 276.000+ anuales, solo en licencias

COMPARACIÓN DE COSTO ANUAL DE LICENCIAMIENTO



Licenciamiento comercial · US$ 10.000+/año → Licenciamiento con software libre US$. 0

AHORRO DEL 100% EN LICENCIAMIENTO

Costo del servicio

El costo de esta arquitectura no está en el software, sino en la implementación y el acompañamiento técnico especializado — la inversión real que garantiza que el sistema funcione como debe.
La inversión varía según el nivel de la institución (Básico, Intermedio o Avanzado) y se define tras el diagnóstico inicial sin costo.
Contáctanos para recibir una propuesta económica personalizada.

HIGH LEVEL

2026

SIGAMOS

El siguiente paso no es decidir si esta arquitectura funciona — es ver cómo se aplica a tu institución.

Diagnóstico inicial sin costo: evaluamos tu infraestructura actual y qué nivel (Básico, Intermedio o Avanzado) te corresponde. Sin compromiso.

El plazo del PISLEA ya corre — empezar antes es la única ventaja que se puede elegir.

---

lcumara@outlook.com

Ing. Limber Cumara

+591 68007247

linkedin.com/in/lcumara