E3 CreaTIC

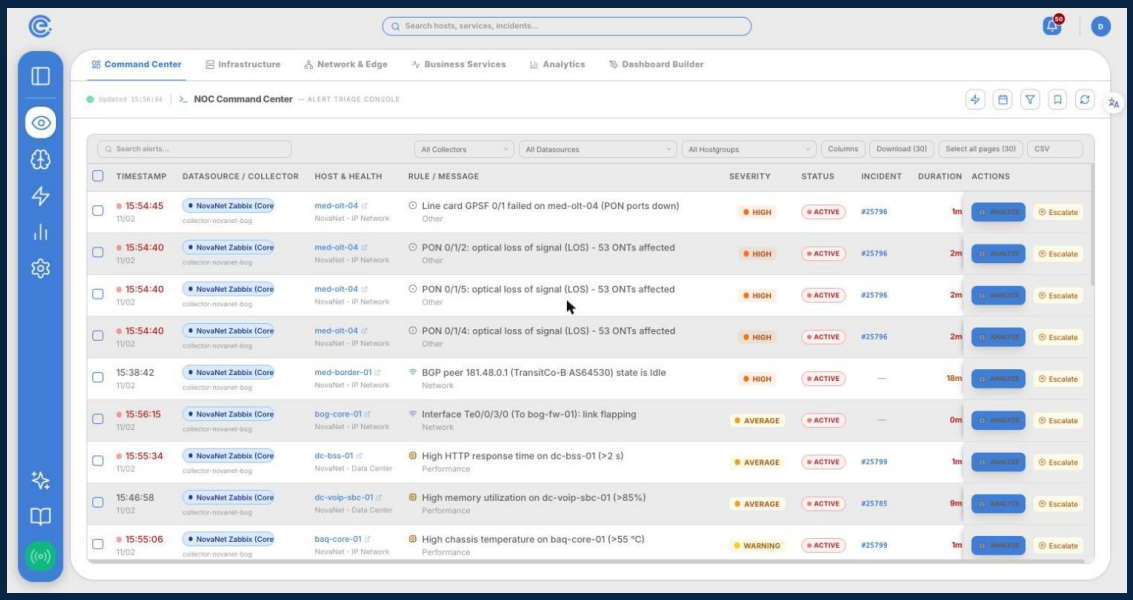
FICHA TÉCNICA · 2026

PLATAFORMA DE AIOPS Y OBSERVABILIDAD

EVA AIOps

Operaciones inteligentes y soporte proactivo

Conecta todas tus fuentes de monitoreo y telemetría, convierte miles de alertas en pocos incidentes con su causa probable y orquesta la respuesta.



Colección multifuente · Correlación · Anomalías · Causa raíz · IA generativa · Orquestación

Del ruido de alertas a incidentes accionables

Reduce el MTTR, operando con menos ruido, diagnósticos más precisos y acciones concretas de notificación y/o solución.

El reto de la operación

Los centros de operación y soporte de servicios tecnológicos conviven con miles de alertas al día, repartidas entre varias herramientas de monitoreo, logs, traps y flujos de red. La mayoría son síntomas repetidos de un mismo problema, y el equipo pierde tiempo valioso decidiendo qué mirar primero mientras el servicio ya está degradado.

Las herramientas de monitoreo saben **que algo falló**; lo difícil es entender **qué falló primero, a quién afecta y qué hacer ahora**. Esa respuesta suele depender de la experiencia de quien esté de turno, y se traduce en tiempos de detección (MTTD) y de resolución (MTTR) más largos de lo necesario.

En resumen

EVA AIOps es la capa de inteligencia que se ubica entre tu monitoreo y tu equipo. Recolecta datos con **EVA Collector** (SNMP, Syslog, NetFlow, OpenTelemetry, agentes, APIs) o se conecta con las plataformas que ya tienes: **Zabbix, PRTG, SolarWinds, Prometheus/Grafana, Elastic, Splunk** y otras fuentes.

Normaliza y enriquece los eventos con la CMDB, los agrupa en incidentes, detecta anomalías, ordena los candidatos a causa raíz con su evidencia visible, calcula el impacto en el negocio y dispara flujos que notifican, abren tickets y ejecutan acciones de remediación sin escribir código.

Una plataforma, cuatro capas

EVA AIOps organiza el ciclo completo de la operación: del dato crudo a la acción.

01
Colección de datos e integración
Recolecta información de múltiples fuentes, plataformas y tecnologías mediante conectores e infraestructura propia.
- EVA Collector
- Conectores con plataformas de monitoreo

02
Procesamiento inteligente de eventos
Normalización, deduplicación, correlación, enriquecimiento y análisis inteligente de eventos con algoritmos de IA/ML.

03
AIOps y observabilidad
Identificación de incidentes, detección de anomalías, análisis de patrones, identificación de posibles causas raíz y visibilidad operacional.

04
Automatización y orquestación
Integración con plataformas ITSM, notificaciones, generación de tickets, ejecución de acciones y procesos de autorremediación.

Resultados comprobados

69 %
reducción del ruido de alertas

56 %
mejora en la respuesta a incidentes

36 %
mejora del MTTR en el primer año de implementación

+100k
activos gestionados

Cifras de despliegues de EVA en clientes de telecomunicaciones, validadas por caso de éxito; el piloto de lanzamiento alcanzó un 97,9 % de reducción de ruido. Los resultados dependen del volumen operativo y la infraestructura de cada cliente.

Resultados para la operación

Menos ruido
Las alertas duplicadas y relacionadas se agrupan en un solo incidente priorizado. El indicador de reducción de ruido lo mide de forma continua.

Menor MTTR
Detección temprana por anomalías, causa probable en segundos y respuesta automatizada: menos tiempo entre la alerta y la solución.

Diagnóstico explicable
Cada causa raíz muestra la evidencia que la sustenta. El operador entiende por qué, no solo qué.

Visión de negocio
Para cada servicio de negocio que modelas en EVA: su salud, los usuarios potencialmente afectados, los ingresos en riesgo por hora y el cumplimiento del SLA.

CAPA 1 · COLECCIÓN DE DATOS E INTEGRACIÓN

EVA Collector: colección multiprotocolo

EVA Collector es el componente de colección y normalización de EVA. Se despliega en la red del cliente (datacenter, sedes o nube) y captura telemetría de cualquier fuente con el mecanismo que mejor se ajuste a cada componente, sin depender de una herramienta de monitoreo de terceros.

Mecanismo	Estándares y protocolos	Qué cubre
Con agente	Agente EVA Collector a nivel de sistema operativo con eBPF (extended Berkeley Packet Filter, tecnología del núcleo de Linux para observar el sistema con bajo impacto) o tecnología equivalente	Servidores físicos y virtuales y nodos de contenedores: métricas, logs, eventos y trazas
Sin agente	SNMP v1/v2c/v3 (sondeo y traps), SSH, WMI y Syslog (RFC 3164 / 5424)	Equipos de red y seguridad, almacenamiento, impresoras, UPS, aires acondicionados de precisión y demás dispositivos con SNMP, entornos heredados y plataformas que generan logs
Flujos de red	NetFlow, sFlow e IPFIX	Tráfico, ancho de banda y conversaciones en los enlaces de red
Estándares abiertos	OpenTelemetry (OTLP) y exportadores Prometheus / OpenMetrics	Aplicaciones instrumentadas, contenedores, clústeres Kubernetes y bases de datos
APIs y archivos	APIs REST de nubes y fabricantes, webhooks entrantes y archivos de log	Nubes públicas (Azure, OCI, AWS), consolas de fabricantes y aplicaciones propias

DESPLIEGUE

Listo en minutos

- Contenedor Docker con comando de instalación generado por la consola
- Solo conexiones salientes cifradas (HTTPS 443): no se abren puertos de entrada en tu red
- Configuración administrada centralmente

RESILIENCIA

No se pierde información

- Búfer local persistente de hasta 100.000 eventos ante cortes
- Envío solo de cambios
- URLs de respaldo

SEGURIDAD

Protegido desde el origen

- Enrolamiento con secreto, aprobación del administrador y token renovable
- TLS 1.2/1.3 y mTLS; VPN IPsec opcional
- Revocación e identidad de hardware

Integración con las plataformas de monitoreo que ya tienes

Si tu organización ya invirtió en una o varias plataformas de monitoreo, EVA **no las reemplaza: las une y les agrega inteligencia**. Sus conectores consumen alertas, eventos, métricas e inventario de cada herramienta y los procesan en un único modelo de incidente, para que el equipo trabaje desde una sola consola y con una sola verdad.

Plataforma	Datos que EVA consume	Método de integración
Zabbix	Problemas y alertas, métricas e históricos, inventario y grupos de hosts, proxies para diagnóstico remoto	API nativa
PRTG Network Monitor	Alarmas y estados de sensores, dispositivos y grupos, valores de canales	API y notificaciones por webhook
SolarWinds	Alertas activas, nodos, interfaces y estado de los elementos	API (SWIS) y webhook
Prometheus / Grafana	Alertas de Alertmanager y de las alertas de Grafana, series de métricas	Receptor de webhook y API de consultas
Elastic	Alertas de reglas, logs y eventos	API y conector webhook
Splunk	Alertas de búsquedas programadas y eventos notables	Acción de alerta por webhook y API REST
Otras fuentes	Nagios, Icinga y cualquier sistema que emita Syslog, traps SNMP o webhooks, o exponga una API REST	EVA Collector y conectores genéricos

Así reduce EVA el MTTR sobre tu monitoreo actual

DETECTAR
Antes y con menos ruido
Anomalías frente a la línea base de cada métrica y alertas de todas las fuentes correlacionadas en un incidente.

DIAGNOSTICAR
Causa probable en segundos
Candidatos a causa raíz con evidencia, topología, incidentes similares y resumen generado por IA.

ESCALAR
Al equipo correcto
Prioridad según el servicio afectado; ticket y notificación automáticos con el contexto completo.

RESOLVER
Con un clic o sin él
Diagnósticos remotos y flujos de remediación; cierre automático cuando no quedan alertas activas.

CAPA 2 · PROCESAMIENTO INTELIGENTE DE EVENTOS

Del evento crudo al incidente

Cada evento se normaliza, se enriquece con contexto y se correlaciona con los demás para que al equipo solo lleguen incidentes reales. Las decisiones de agrupación se toman con reglas y evidencias auditables.

Normalización y enriquecimiento

- **Modelo común de evento** para todas las fuentes: severidad, equipo, servicio, categoría y entorno homologados.
- **Clasificación automática** por palabras clave y entorno (producción, pruebas, desarrollo) y tabla de excepciones por patrón de nombre.
- **Contexto CMDB**: dueño, contrato, SLA, servicios soportados y clientes impactados desde InvGate Asset Management u otra CMDB por API.
- **Datos históricos**: líneas base, recurrencia e incidentes similares de los últimos 90 días.

Deduplicación, correlación y reducción de ruido

1 incidente, no 50 alertas. El motor de correlación por etapas transforma miles de alertas en pocos incidentes accionables.

- **Deduplicación** de alertas repetidas y asociación de nuevas alertas al incidente abierto del mismo equipo.
- **Reglas propias** con prioridad, alcance, condiciones, ventana de tiempo y plantilla de título; **extractores por patrón (expresiones regulares)** para agrupar por ubicación, nombre del dispositivo, servidor o aplicación, par BGP, puerto PON, OLT o cualquier otra clave.
- **Agrupación multidimensional con IA/ML**: equipo, vecindad topológica, similitud de mensajes, cercanía temporal, categoría y entorno.
- **Indicador de reducción de ruido**: alertas crudas frente a incidentes generados, por regla y por etapa.

CAPA 3 · AIOPS Y OBSERVABILIDAD

Inteligencia AIOps explicable

Cada motor responde una pregunta distinta de la operación y entrega su resultado con el razonamiento detrás, para que el operador decida con confianza. La IA generativa explica y acelera; no decide sin evidencia.

Identificación y gestión de incidentes

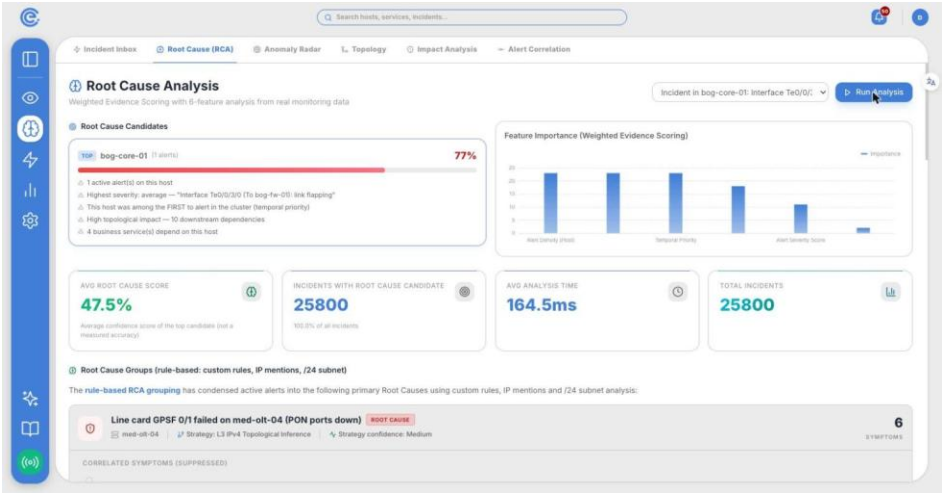
- Incidentes priorizados (P1 a P3) con ciclo de vida completo: asignación, reconocimiento individual o masivo, notas, línea de tiempo y cierre automático cuando ya no quedan alertas activas.
- Búsqueda avanzada sobre campos del incidente, la CMDB y la correlación; vistas guardadas y compartidas por el equipo.

Radar de anomalías

- Arquitectura multicapa: **puntuación Z (Z-Score) y rango intercuartílico (IQR)** contra la línea base de cada métrica, **tendencia adaptativa (media móvil exponencial)** y **explicación con IA generativa**.
- CPU, memoria, disco, swap, carga, tráfico de interfaces, latencia y pérdida de paquetes, entre otras.
- Detecta degradaciones antes de que crucen un umbral fijo; se resuelve sola al normalizarse y puede disparar automatizaciones.

Causa raíz con puntuación ponderada de evidencias

- Lista priorizada de candidatos con seis evidencias ponderadas: **severidad, densidad de alertas, profundidad topológica, prioridad temporal, criticidad del servicio y diversidad de síntomas**, con el aporte de cada una a la vista.
- Agrupación de síntomas por reglas, IP mencionadas y subred; árbol de causa raíz, incidentes similares y mapa de recurrencia 7×24.



Análisis de causa raíz: candidato principal y su evidencia ponderada

Topología e impacto en el negocio

- Grafo de dependencias con relaciones declaradas en la CMDB e inferidas (co-ocurrencia, cadenas de incidentes, subred, servicios).
- Radio de afectación, servicios impactados, usuarios estimados, **ingresos en riesgo por hora** y cadena de propagación desde la causa raíz.

IA generativa aplicada a la operación

- **Asistente conversacional** que consulta datos en vivo de tu entorno y **narrador con IA** que genera el resumen ejecutivo de la vista en curso.
- **Resumen de incidente** con causas probables y soluciones sugeridas; análisis de alertas y explicación de anomalías en lenguaje natural.

- Independiente del modelo: **local con Ollama** o cualquier API compatible con OpenAI, con el cliente en control de sus datos.

Observabilidad de aplicaciones y experiencia digital

Extiende la visibilidad de EVA desde la infraestructura hasta la aplicación y el usuario final, con los mismos motores de correlación, anomalías y causa raíz.

Capacidad	Alcance
Monitoreo del desempeño de aplicaciones (APM)	Trazas distribuidas con OpenTelemetry (instrumentación automática para Java, .NET, Node.js, Python y Go); mapa de servicios; tasa de peticiones, errores y duración por servicio y por transacción; explorador de trazas; relación entre trazas, logs y métricas de infraestructura.
Monitoreo de usuario real (RUM)	Componente ligero para aplicaciones web que mide carga de páginas, Core Web Vitals, errores de JavaScript y llamadas a servicios, por navegador, dispositivo y ubicación, y las enlaza con las trazas del servidor.
Monitoreo sintético	Pruebas programadas desde los EVA Collector ubicados en distintas sedes: HTTP/HTTPS (código, contenido y vencimiento de certificados), DNS, TCP, ICMP, APIs de varios pasos y transacciones de navegador grabadas; disponibilidad y tiempo de respuesta frente a SLA.

Visibilidad para cada rol

Vista	Qué responde
Centro de mando	Consola en tiempo real para el centro de operaciones y soporte a servicios: todas las alertas de todas las fuentes, filtros, salud por recurso, análisis con IA y escalamiento a incidente.
Bandeja de incidentes	Incidentes correlacionados y priorizados, con su causa probable, contexto CMDB e historial.
Infraestructura y red	Salud de servidores y equipos de red: indicadores, mayores consumos, tráfico por interfaz, latencia y pérdida.
Servicios de negocio	Salud de cada servicio de negocio, componentes, MTTR, SLA e incidentes que lo afectan.
Analítica y reportes	Tendencias, componentes más ruidosos, MTTR/MTBF, disponibilidad frente a SLA, reducción de ruido; exportación a PDF, CSV y JSON.
Explorador de eventos	Búsqueda de Syslog, traps SNMP, flujos y webhooks recibidos por los colectores, con contexto CMDB y contenido original.
Constructor de tableros	Tableros a la medida con indicadores, gráficas, medidores y tablas en tiempo real.

CAPA 4 · AUTOMATIZACIÓN Y ORQUESTACIÓN

Del diagnóstico a la acción

Diseñador visual de flujos **sin código** sobre un motor de ejecución durable, con reintentos por paso y pasos de compensación.

- **Disparadores**: eventos de alertas, incidentes y anomalías con condiciones; webhook entrante firmado (HMAC) y programación periódica.
- **Modo automático o manual**: cada regla ejecuta su flujo en segundo plano o publica un botón de acción en la consola.
- **Acciones**: escalar, priorizar, reconocer, comentar y resolver incidentes; diagnósticos remotos (ping, traceroute, puertos, DNS, HTTP) y acciones de autorremediación.
- **Lógica**: condiciones, bifurcación y unión, ciclos, esperas y lectura de datos. Historial con el detalle de cada paso.

Tipo	Conectores
Notificación	Microsoft Teams, Telegram, Slack y correo (SMTP)
ITSM	Permite crear, comentar, actualizar y consultar tickets en cualquier ITSM con API REST
CMDB	InvGate Asset Management y otras CMDB por API
Genéricos	Servicio web (Bearer, básica, API key, OAuth2) y webhook saliente

Casos de uso

TELECOMUNICACIONES E ISP
Operación de red y acceso
Correlación de fallas de OLT, BNG, BGP y red troncal; impacto en suscriptores y servicios residenciales.

TI CORPORATIVA
Operación de TI
Una sola consola sobre varias herramientas de monitoreo, con CMDB, SLA y tickets automáticos.

SERVICIOS GESTIONADOS
Operación multicliente
Instancias dedicadas por cliente, colectores remotos y reportes de SLA y desempeño.

Especificaciones técnicas

Fuentes de monitoreo	Zabbix, PRTG, SolarWinds, Prometheus/Grafana, Elastic y Splunk; otras fuentes por Syslog, traps SNMP, webhooks y API REST.
EVA Collector	Agente (eBPF o equivalente); sin agente: SNMP v1/v2c/v3, SSH, WMI, Syslog; NetFlow, sFlow, IPFIX; OpenTelemetry (OTLP), Prometheus/OpenMetrics; APIs de nube (Azure, OCI, AWS) y fabricantes; archivos de log.
Despliegue del colector	Contenedor Docker en la red del cliente; solo conexiones salientes HTTPS (443); enrolamiento con secreto, aprobación y token renovable; búfer persistente de hasta 100.000 eventos; URLs de respaldo.

Procesamiento y AIOps	Correlación por etapas (reglas, expresiones regulares, IA/ML), radar de anomalías (Z-Score, IQR, media móvil exponencial), causa raíz por puntuación ponderada de evidencias, topología e impacto en el negocio.
IA generativa	Ollama (local) o cualquier API compatible con OpenAI; parámetros e instrucciones configurables.
Integraciones de salida	Teams, Telegram, Slack, SMTP, InvGate Service Desk y Asset Management, servicio web y webhook genéricos.
Seguridad y acceso	Control de acceso por roles de sistema y personalizados (recurso:acción); contraseñas bcrypt y sesiones JWT; auditoría exportable; TLS 1.2/1.3, mTLS con colectores, HSTS y secretos enmascarados.
Modelo de despliegue	Instancia dedicada por cliente con datos aislados: SaaS dedicado en AWS o en la infraestructura del cliente.
Aplicaciones y experiencia digital	APM con trazas OpenTelemetry, monitoreo de usuario real (RUM) y monitoreo sintético desde los colectores.
Plataforma	Servicios en Python (FastAPI), PostgreSQL, Redis, Kafka, OpenSearch, Neo4j, MinIO y Temporal; interfaz web en React con zona horaria por usuario.

Cómo empezar

01
Conecta
Registra tus plataformas de monitoreo e instala EVA Collector en tu red.

02
Ajusta
Modela tus servicios de negocio, conecta la CMDB y define reglas de correlación.

03
Automatiza
Diseña los flujos de respuesta: tickets, notificaciones y remediación.

Acerca de E3 CreaTIC

E3 CreaTIC es una empresa colombiana, fundada en 2012, que desarrolla software e integra soluciones de AIOps, observabilidad, monitoreo, ITSM e ITAM para operaciones de red y de TI. Hemos desplegado proyectos en más de 16 países de Latinoamérica y más de 200 automatizaciones e integraciones. Somos Delivery Partner de Zabbix y Partner Gold de InvGate. **EVA AIOps es nuestro producto: lo diseñamos, lo desarrollamos y lo soportamos.**

Web e3creatic.com · **Correo** sales.latam@e3creatic.com · **Teléfono** +57 324 399 3791

Oficina Av. El Dorado #92-32, Of. 5-131 · Bogotá, Colombia

Demo en vivo demo-eva.e3creatic.com · **Manual de usuario** e3creatic.com/es/productos/eva-aiops/docs · **Soporte** support.e3creatic.com

© 2026 E3 CreaTIC. Todos los derechos reservados. EVA AIOps es un producto de E3 CreaTIC. Zabbix, PRTG, SolarWinds, Nagios, Icinga, Prometheus, Grafana, Elastic, Splunk, InvGate, Microsoft Teams, Telegram, Slack, OpenAI, Ollama y las demás marcas mencionadas pertenecen a sus respectivos titulares y se citan solo con fines de identificación. Las capacidades descritas pueden evolucionar sin previo aviso.