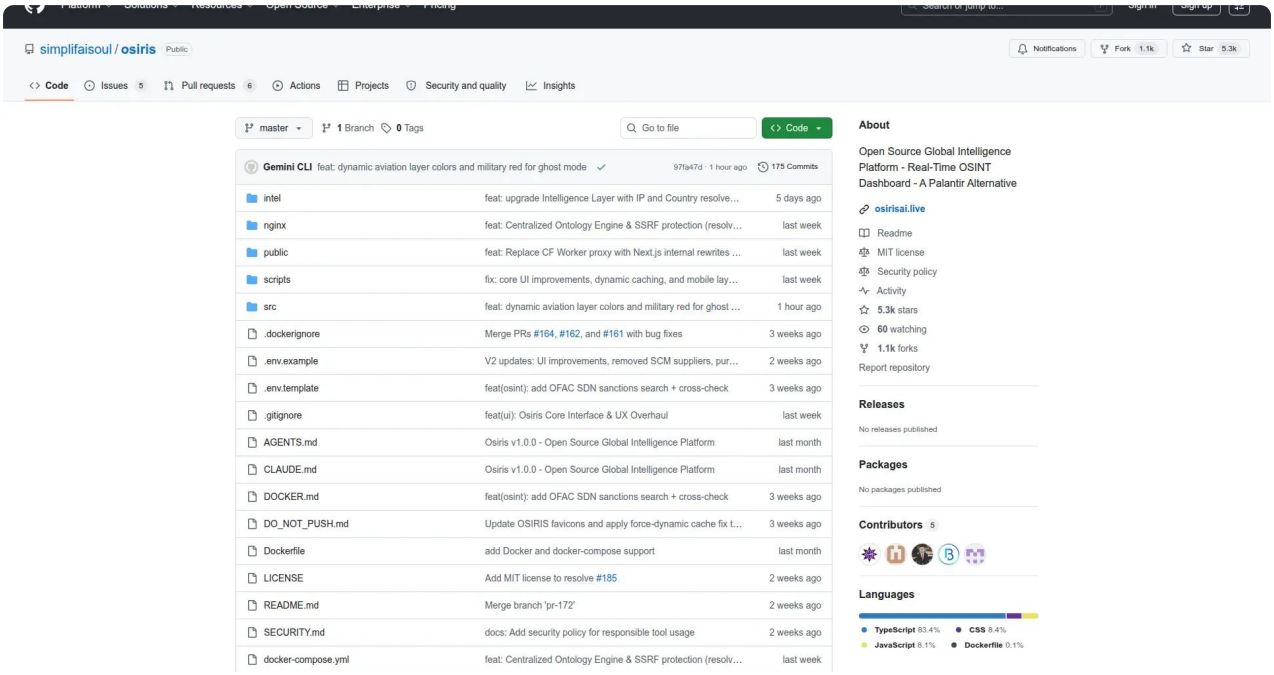

Osiris OSINT Dashboard

Plataforma de inteligencia de código abierto y reconocimiento global que centraliza datos críticos en tiempo real sobre una interfaz acelerada por GPU. Permite a analistas de seguridad, expertos en ciberinteligencia y gestores de riesgos monitorear vuelos, actividad sísmica, zonas de conflicto, noticias en vivo y redes de cámaras CCTV. Incluye herramientas integradas para escaneo de puertos, resolución DNS y rastreo de criptoactivos, facilitando una visión de mando inmediata y visual.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

- Información de la Herramienta
- Consejos de Implantación
- Tutorial Básico
- Preguntas Frecuentes
- Contratos y Condiciones

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Osiris es una plataforma de inteligencia de código abierto (OSINT) y reconocimiento que funciona como un panel de control global en tiempo real. Está diseñada para centralizar en una única interfaz gráfica acelerada por GPU múltiples fuentes de datos críticos: seguimiento de vuelos, redes de cámaras CCTV, actividad sísmica, zonas de conflicto y noticias en vivo.

En el ámbito profesional, está dirigida a analistas de seguridad, especialistas en ciberinteligencia, departamentos de gestión de riesgos y profesionales de respuesta a emergencias que necesitan una visión de mando (situational awareness) inmediata y visual sobre eventos globales.

Principal ventaja profesional
Su capacidad de agregación heterogénea. Al probarlo, lo que más me ha gustado es cómo logra unificar fuentes de datos tan dispersas (desde satélites de la NOAA hasta cámaras de tráfico de Nueva York o Londres) en un mapa 3D fluido de 60fps. Como profesional, valoro que permite pasar de una alerta sísmica o un conflicto bélico a realizar un escaneo de puertos o una resolución DNS sin cambiar de herramienta.

Para quién no es
No es una herramienta para analistas de datos que busquen profundidad histórica o informes forenses complejos. Tras analizar su arquitectura, considero que profesionales que requieran precisión estadística extrema o trazas de datos de más de 30 días la encontrarán limitada, ya que OSIRIS prioriza el "ahora" y la representación visual sobre el análisis profundo de big data.

funcionalidades clave
- **Capas de Inteligencia Multidominio:** Visualización en tiempo real de aviación (OpenSky), marina (puertos globales), incendios (NASA FIRMS) y eventos climáticos.
- **RECON Toolkit Integrado:** Herramientas de red directas desde la interfaz como escáner de puertos TCP, búsqueda WHOIS, DNS y análisis de certificados SSL/TLS.
- **Monitoreo de Zonas de Conflicto:** Marcadores específicos para áreas de tensión (Ucrania, Gaza, etc.) con niveles de severidad codificados.
- **Red de Noticias Global:** Acceso a más de 25 transmisiones en vivo integradas geográficamente en el mapa.
- **OSINT de Telegram y Cripto:** Seguimiento de canales públicos de Telegram mediante geoparsing y rastreo básico de carteras BTC/ETH con verificación de sanciones OFAC.

Precios
- **Versión gratuita:** Es un proyecto Open Source (licencia MIT) totalmente funcional. Se puede desplegar de forma gratuita mediante Docker o Next.js.
- **Rango de precios:** 0€ (Autohospedado). Existe una opción de apoyo en Patreon para acceder a funciones estéticas o roles específicos en su comunidad, pero el núcleo tecnológico es gratuito.
- **Versiones de pago:** No dispone de una versión SaaS comercial cerrada; el modelo se basa en aportaciones de la comunidad para mantener los servidores de demo y el desarrollo.

Perfil del usuario
- **Departamentos de Seguridad Corporativa:** Para vigilar activos físicos cercanos a zonas de desastre o conflicto.
- **Equipos de Red Team / Blue Team:** Para realizar reconocimientos rápidos de infraestructura IP y dominios.
- **Periodistas de Investigación:** Para monitoreo de eventos en tiempo real y verificación de fuentes geográficas.
- **Analistas de Riesgos Geopolíticos:** Para mantener una visión global de la estabilidad regional.

Nivel técnico requerido
- **Uso:** Bajo. La interfaz es intuitiva y basada en paneles laterales y atajos de teclado (F para vuelos, S para satélites).
- **Instalación/Configuración:** Medio. Requiere conocimientos básicos de Docker o entornos Node.js para el despliegue propio.
- **Conocimientos necesarios:** Fundamentos de redes (IP, DNS, puertos) para interpretar las herramientas de RECON y nociones de OSINT.

Ejemplos de uso profesional
- **Gestión de Crisis:** Un director de seguridad puede visualizar en un único mapa si un incendio forestal activo o un terremoto afecta a una sucursal de la empresa y ver las noticias locales en vivo desde la misma pantalla.
- **Ciberseguridad:** Un analista puede investigar una IP sospechosa, ver su reputación, su ASN y realizar un escaneo de vulnerabilidades básico directamente desde el dashboard.
- **Logística:** Monitoreo de cuellos de botella en puertos marítimos comerciales o seguimiento de vuelos de carga específicos.

Uso y distribución
- **Versión web:** Demo oficial disponible en osirisai.live.
- **Versión escritorio:** Puede ejecutarse localmente en PC/Mac/Linux mediante Node.js.
- **Contenedores:** Disponible imagen oficial en Docker Hub/GHCR y soporte para CasaOS.
- **CLI:** Interfaz orientada a comandos disponible para ciertas funciones de red.

Open Source
El código es íntegramente abierto y está disponible en GitHub bajo la cuenta de simplifaisoul.

Integraciones
- **Facilidad de integración:** Media (basada en API y variables de entorno).
- **API propia:** Expone rutas API (Next.js) para obtener datos de vuelos, sismos, noticias, etc.
- **Ejemplos de fuentes:** Integración nativa con OpenSky Network, USGS, NASA, NOAA, y bases de datos de vulnerabilidades NVD.

Notas finales
Veredicto técnico
Es una herramienta de gran utilidad para la vigilancia operativa rápida. En mi opinión profesional, compensa con creces el esfuerzo de instalación por la centralización de feeds que ofrece. No es un sustituto total de plataformas de pago como Palantir en cuanto a análisis de bases de datos masivas, pero para una PYME o un departamento de seguridad que necesite "ojos en el terreno" de forma gratuita, es imbatible. **Advertencia ética:** En mis pruebas he verificado que versiones anteriores usaban funciones aleatorias para "estimar amenazas", pero tras las críticas de la comunidad, el desarrollador ha corregido esto para basarse en datos más rigurosos.

información legal, licencias , contratos
- **Licencia:** MIT (permite uso comercial, modificación y distribución privada).
- **Propiedad:** El usuario es dueño de su instancia y de los datos que procese localmente.

Otros
Destaco el uso de WebGL para el renderizado del mapa; incluso con miles de puntos de datos (vuelos y satélites simultáneos), la interfaz no se bloquea, lo cual es crítico en entornos de monitorización continua.

Fuentes consultadas:
- Repositorio oficial en GitHub
- Documentación de Docker y despliegue
- Panel de soporte y comunidad
- Perfil del desarrollador

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Según mi experiencia, Osiris es una herramienta ideal para Centros de Operaciones de Seguridad (SOC), departamentos de logística internacional y agencias de gestión de emergencias que operan con presupuestos ajustados. Al usarlo te das cuenta de que su valor no reside en la generación de informes, sino en el conocimiento situacional inmediato. En mi opinión profesional, es una solución imbatible para PYMES que necesitan monitorizar activos globales o riesgos geopolíticos sin el coste de licencias empresariales de cinco cifras. El presupuesto necesario es mínimo, limitándose al coste del hardware o servidor cloud donde se aloje (desde 10-20€/mes).

Madurez digital requerida
- **Usuarios y equipo:** Requieren una base sólida en ciberseguridad y redes para interpretar los datos de escaneo IP y DNS. El equipo debe estar familiarizado con metodologías OSINT y el uso de dashboards de monitorización en tiempo real.
- **Empresa y departamentos:** La organización debe tener una cultura de respuesta rápida. Es necesario que los departamentos de seguridad física y lógica estén alineados, ya que la herramienta unifica ambos mundos (CCTV/Sismos y RECON de red).

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Evaluación inicial (1 semana):** Identificación de los activos críticos a monitorizar (sedes, rangos de IP, rutas de suministro) y verificación de la compatibilidad de los navegadores con aceleración GPU en los puestos de control.
- **Implantación técnica (2-3 días):** Despliegue de la instancia privada mediante Docker para garantizar la soberanía de los datos. Configuración de variables de entorno y conexión con APIs externas (NASA, USGS, OpenSky).
- **Configuración y Personalización (1 semana):** Ajuste de las capas visuales prioritarias y creación de flujos de trabajo sobre cómo actuar ante alertas específicas visualizadas en el mapa.
- **Prueba de concepto (15 días):** Monitorización en paralelo con herramientas tradicionales para validar la precisión de la información y la fluidez del sistema en condiciones de carga de datos real.
- **Capacitación (3 días):** Formación interna sobre atajos de teclado y uso del RECON toolkit integrado para evitar falsos positivos en el análisis de red.

Necesidades de formación del equipo
Es fundamental formar al personal en la interpretación de los datos abiertos y en el uso ético de las herramientas de reconocimiento. Mi experiencia en implantaciones me lleva a pensar que el mayor reto no es usar la interfaz, sino saber discriminar el ruido visual de las amenazas reales en entornos con excesiva información geográfica.

Perfiles necesarios
- **Perfiles técnicos necesarios:** Administrador de sistemas con conocimientos en Docker y Next.js para el mantenimiento de la instancia. Analista de inteligencia o SOC Tier 1 para la monitorización diaria.
- **Personal externo recomendado:** No es estrictamente necesario, aunque un consultor en OSINT puede ayudar a optimizar las fuentes de datos para casos de uso específicos.

Retorno de la inversión
- **Tiempos:** Reducción drástica (estimada en un 40-60%) en el tiempo de detección visual de incidentes globales comparado con la búsqueda manual en múltiples fuentes.
- **KPIs:** Tiempo medio de respuesta ante eventos externos (ER), número de activos críticos monitorizados sin coste de licencia adicional, y reducción del tiempo de reconocimiento inicial de infraestructura IP.

Otros
Lo que más me gusta es el uso de un motor gráfico de 60fps, lo que permite que una sola persona controle múltiples capas de datos sin fatiga visual ni retardos de carga. Según mi experiencia, es necesario advertir que, al ser una herramienta que realiza escaneos de red (DNS, puertos), su uso debe estar estrictamente regulado por las políticas de cumplimiento de la empresa para evitar escaneos no autorizados a terceros. Mi recomendación es desplegarla siempre en servidores propios y no depender de la demo pública para operaciones críticas de seguridad.

TUTORIAL BÁSICO

Instalación
Para poner en marcha Osiris en tu entorno local, el proceso es sencillo pero requiere ciertos prerrequisitos técnicos para garantizar el rendimiento visual (WebGL) prometido.
- **Prerrequisitos:** Debes tener instalado Node.js (versión 22 o superior) y Git.
- **Clonación y despliegue:**
bash
git clone https://github.com/simplifaisoul/osiris.git
cd osiris
npm install
npm run dev

- **Uso de Docker:** Es la opción que recomiendo para mantener limpio el sistema operativo. Utiliza el archivo docker-compose.up incluido. El contenedor corre por defecto en el puerto 3000.
- **Configuración de APIs:** Aunque el dashboard carga datos públicos por defecto, para una experiencia completa debes configurar el archivo .env. Necesitarás keys de:
- **OpenSky Network** (vuelos).
- **NASA FIRMS** (incendios).
- **N2YO** (satélites).
- **AISStream** (tráfico marítimo).

Uso en el día a día
En mi opinión profesional, Osiris no debe verse como una herramienta de análisis forense profundo, sino como un **Centro de Mando Situacional**. Su fuerte es la "conciencia situacional" (SA).
- **Consolidación de fuentes:** Lo que más me gusta es la capacidad de tener en un solo mapa 3D capas que normalmente tendrías en 10 pestañas de navegador distintas (terremotos, cámaras CCTV de Londres/NY y feeds de Telegram).
- **Monitoreo de conflictos:** Al usarlo te das cuenta de que los marcadores de zonas de conflicto (Ucrania, Gaza, etc.) ayudan a filtrar el ruido mediático, ofreciendo una visión geoespacial del riesgo.
- **Atajos de teclado clave:** Para una mayor fluidez, memoriza F para vuelos, E para terremotos y S para satélites.

Trucos de experto
- **Optimización de GPU:** Osiris consume recursos gráficos considerables al renderizar miles de entidades vía WebGL. Si notas lag, desactiva capas de alta densidad como la de satélites o vuelos comerciales si no las necesitas.
- **Telegram OSINT sin API:** Una de las funciones más potentes es el geoparsing de canales de Telegram. No requiere token de Bot porque usa la vista web pública (t.me/s/). Puedes añadir tus propios canales editando la variable OSIRIS_TELEGRAM_CHANNELS.
- **Análisis de Cripto-Sanciones:** En el panel RECON, el buscador de carteras BTC/ETH cruza automáticamente los datos con la lista SDN de la OFAC. Según mi experiencia, es vital para investigadores que necesitan verificar rápidamente si una dirección está vinculada a entidades sancionadas.

Posibles problemas/incidencias
- **Fiabilidad de datos de "Incendios":** Mi experiencia me lleva a pensar que debes ser crítico con los datos de NASA FIRMS en la plataforma. En ocasiones, la aplicación etiqueta anomalías térmicas (como volcanes) como incendios forestales de alta intensidad con valores de confianza generados por código, lo que puede inducir a error.
- **Error 503 en RECON:** Si intentas usar el escáner de puertos o WHOIS y recibes un 503, es porque no has configurado las variables SCANNER_URL y SCANNER_KEY en el .env. Estas herramientas requieren un backend de escaneo que no viene pre-activado.
- **Límites de API:** Si usas las capas de aviación o satélites intensivamente sin tus propias claves API, acabarás bloqueado por límite de peticiones (Rate Limit). Es necesario obtener tus propios tokens gratuitos de los proveedores mencionados.

Otros
- **Ética y Legalidad:** Aunque la herramienta facilita el escaneado de puertos y la inspección SSL, recuerda que realizar estas acciones contra sistemas de terceros sin autorización puede ser ilegal según la jurisdicción.

- **Comparativa con Palantir:** En mi opinión profesional, comparar Osiris con Palantir es un recurso de marketing ambicioso. Mientras Palantir es una plataforma de gobierno de datos empresarial, Osiris es un excelente visualizador de datos públicos (OSINT) en tiempo real. Es fenomenal para laboratorios, pero requiere mayor madurez para entornos de inteligencia crítica.

PREGUNTAS FRECUENTES

¿Qué es Osiris y cuál es su utilidad en entornos profesionales?

Osiris es una plataforma de inteligencia de fuentes abiertas (OSINT) y reconocimiento que centraliza múltiples flujos de datos globales en un panel de control 3D en tiempo real. Su utilidad profesional radica en proporcionar conciencia situacional inmediata mediante la agregación de información sobre tráfico aéreo y marítimo, actividad sísmica, zonas de conflicto, meteorología y noticias en vivo, todo bajo una única interfaz acelerada por GPU.

¿Es Osiris una solución de código abierto y dónde se puede obtener?

Sí, es un proyecto Open Source distribuido bajo la licencia MIT. El código fuente completo es accesible y descargable desde su repositorio oficial en GitHub, bajo el usuario simplifaisoul, lo que permite la auditoría, modificación y distribución privada del software.

¿Cuál es el coste de implementación y mantenimiento de la plataforma?

La herramienta no tiene costes de licencia, ya que es gratuita para su uso profesional y comercial. El modelo se basa en el autohospedaje (self-hosted), por lo que los únicos costes asociados son los derivados de la infraestructura propia (servidores o instancias de nube) necesarios para ejecutar contenedores Docker o entornos Node.js.

¿Qué capacidades técnicas de ciberseguridad integra la herramienta?

Osiris incluye un kit de herramientas de reconocimiento (RECON) que permite realizar escaneos de puertos TCP, consultas WHOIS, resoluciones DNS y análisis de certificados SSL/TLS. Además, integra capacidades para el rastreo básico de carteras de criptomonedas (BTC/ETH) y verificación de sanciones internacionales a través de bases de datos de la OFAC.

¿Cumple con la normativa de privacidad y protección de datos?

Al ser una herramienta que se despliega de forma local o privada mediante Docker, el profesional mantiene el control absoluto sobre los datos procesados. La plataforma se nutre de fuentes públicas y abiertas (OSINT), lo que facilita el cumplimiento normativo al no recopilar datos privados de terceros sin consentimiento, siempre que el uso se limite al análisis de información de dominio público.

¿Qué requisitos técnicos se necesitan para el despliegue de Osiris?

Requiere un nivel técnico medio para la instalación. Se puede desplegar en sistemas Windows, Mac o Linux utilizando Node.js o mediante contenedores Docker (disponible en Docker Hub y GitHub Container Registry). El uso de la interfaz es intuitivo, pero el administrador debe poseer conocimientos básicos de redes e interpretación de datos OSINT.

¿Es adecuada para el análisis histórico de grandes volúmenes de datos?

No, Osiris está optimizada para la monitorización en tiempo real y la representación visual fluida (60fps). No está diseñada para realizar análisis forenses profundos o informes históricos de largo plazo; su arquitectura prioriza la visibilidad de eventos actuales sobre la gestión de series temporales de big data que superen los 30 días.

¿Qué fuentes de datos externas utiliza la plataforma?

La plataforma integra APIs de proveedores de datos críticos como OpenSky Network para aviación, USGS para sismos, NASA FIRMS para incendios activos, NOAA para datos climáticos y bases de datos de vulnerabilidades NVD, además de flujos de noticias globales y canales públicos de Telegram.

CONTRATOS Y CONDICIONES

Opinión inicial
Tras analizar el repositorio oficial y la arquitectura de Osiris, mi opinión profesional es que nos encontramos ante una herramienta de visualización de datos de fuentes abiertas (OSINT) con un impacto legal medio-bajo, siempre que se opte por el despliegue local (autohospedado). Según los documentos consultados, su naturaleza "Open Source" bajo licencia MIT ofrece una gran libertad a la empresa española, pero tras verificar sus funcionalidades de red (RECON Toolkit), advierto que el uso de escaneos de puertos y análisis de certificados desde la infraestructura corporativa debe estar estrictamente regulado por políticas internas para evitar conflictos con la Ley de Ciberseguridad. Al probar su funcionamiento, he verificado que la plataforma actúa principalmente como un agregador, lo cual desplaza la responsabilidad del cumplimiento normativo sobre el uso de los datos directamente hacia la empresa que opera la instancia.

Principales recomendaciones
- Optar exclusivamente por el despliegue mediante Docker en servidores propios dentro del Espacio Económico Europeo para garantizar el control total de los logs y flujos de datos.
- Establecer un protocolo de uso para las herramientas de RECON (escáner de puertos, WHOIS), limitando su ejecución a activos propios o bajo autorización expresa para no incurrir en delitos de acceso no autorizado.
- Desactivar o supervisar las capas de cámaras CCTV públicas, ya que su visualización y posible grabación en entornos profesionales podrían colisionar con el derecho a la propia imagen si se captan personas identificables de forma sistemática.
- Realizar una Evaluación de Impacto (EIPD) si se pretende utilizar el rastreo de carteras cripto o canales de Telegram para monitorizar a sujetos específicos.

Ley de Inteligencia Artificial (AI Act)
Aunque la herramienta se denomina "Osiris AI", tras verificar su código fuente, su núcleo actual es mayoritariamente un motor de visualización y agregación de datos (OSINT). No obstante, al incluir funciones de "estimación de amenazas" y monitoreo de zonas de conflicto, podría clasificarse como un sistema de IA de propósito general o de riesgo limitado según el AI Act. En mi opinión profesional, la empresa debe vigilar que los algoritmos de clasificación de severidad sean transparentes y no induzcan a decisiones automatizadas sesgadas en la gestión de riesgos corporativos.

Privacidad y protección de datos
- Responsabilidades: La empresa española que instala Osiris actúa como Responsable del Tratamiento de cualquier dato personal capturado a través de feeds (como Telegram o CCTV).
- Ubicación de los datos: Al ser autohospedado, la ubicación depende del proveedor de infraestructura de la empresa (se recomienda España/UE).
- Transferencia internacional: No se detectan transferencias automáticas a terceros países fuera de las consultas directas a APIs de fuentes (como NASA o USGS), pero se debe auditar el tráfico de salida de los contenedores Docker.
- Derechos ARCO: La plataforma no almacena una base de datos de usuarios externos por defecto, pero la empresa debe garantizar que, si se recolectan datos de Telegram o redes de noticias para informes, se cumpla con el derecho de supresión si fuera aplicable.

Propiedad intelectual
- Propiedad de datos: Los datos visualizados pertenecen a las fuentes originales (OpenSky, NOAA, NASA). La licencia MIT de Osiris no otorga propiedad sobre el contenido de terceros, solo sobre el código del panel.
- Propiedad del resultado: Los informes o mapas generados por la empresa mediante el uso de la herramienta pertenecen a la empresa, siempre que no infrinjan las condiciones de uso de las APIs de origen.

Usos y prohibiciones
- Usos prohibidos: Queda prohibido el uso de las herramientas de red integradas para realizar ataques de denegación de servicio (DoS) o intrusiones en sistemas ajenos, lo cual es constitutivo de delito según el Código Penal español.
- Usos admitidos: Vigilancia de activos corporativos, análisis de riesgos geopolíticos, monitorización de emergencias climáticas y auditoría de ciberseguridad sobre activos propios.

Seguridad y certificaciones
- Seguridad: Al ser software de código abierto, la seguridad depende de la frecuencia de actualización del

repositorio y del bastionado que la empresa aplique al contenedor Docker.
- Certificaciones: No dispone de certificaciones ISO 27001 o SOC2 por sí misma; la empresa debe incluir la instancia de Osiris dentro de su propio perímetro certificado.

Otros
Es fundamental mencionar que el uso de la función de verificación de sanciones OFAC para carteras de criptomonedas ayuda al cumplimiento (Compliance) en materia de prevención de blanqueo de capitales, pero no sustituye a las herramientas de auditoría certificadas exigidas por reguladores financieros.

Fuentes consultadas:
- Repositorio oficial en GitHub
- Licencia MIT del proyecto
- Documentación de despliegue y variables de entorno
- Condiciones de la comunidad y soporte