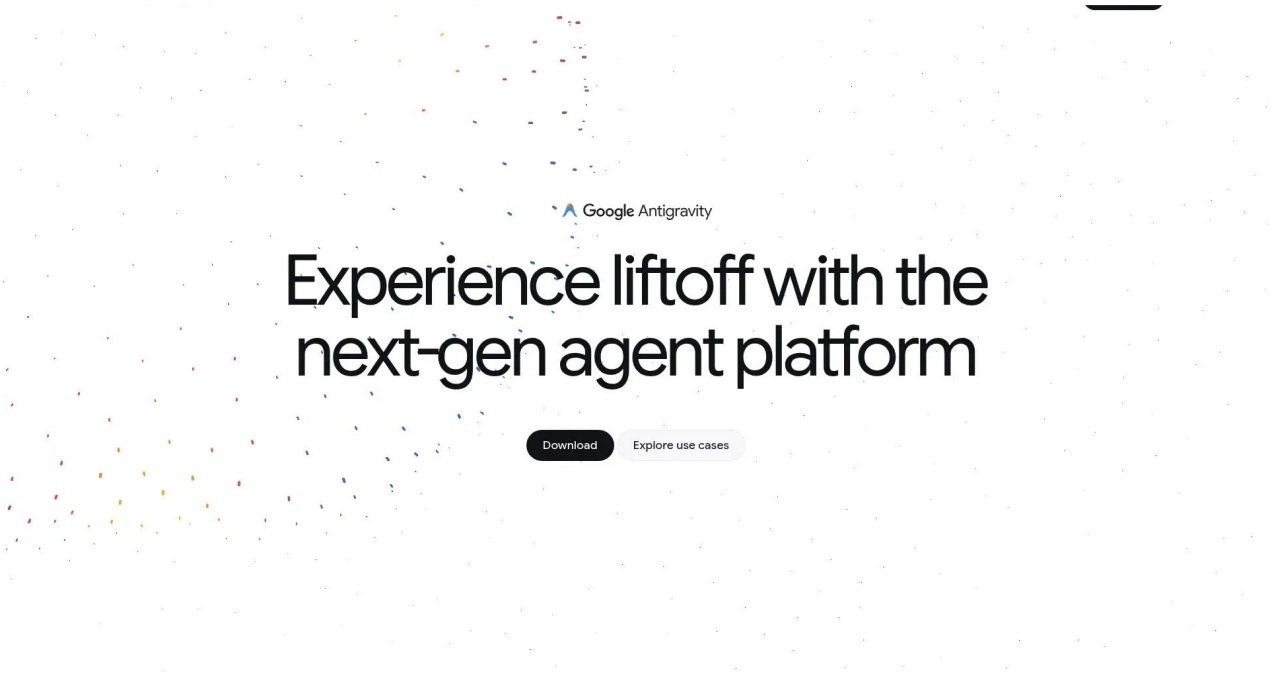

Google Antigravity

Entorno de desarrollo agentic diseñado para transformar la interacción con el software mediante agentes autónomos. Esta aplicación de escritorio nativa permite a desarrolladores senior, ingenieros de plataformas y equipos de innovación orquestar tareas complejas, navegar por sistemas de archivos y ejecutar comandos de forma independiente. Facilita la automatización de flujos de ingeniería de alto nivel, permitiendo pasar de la escritura manual de código a la supervisión estratégica de agentes.

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

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Google Antigravity es un entorno de desarrollo e investigación "agentic" (basado en agentes autónomos) diseñado para transformar la interacción con el software. A diferencia de un asistente de chat tradicional, Antigravity 2.0 es una aplicación de escritorio nativa que permite a agentes de IA orquestar tareas complejas, navegar por sistemas de archivos y ejecutar comandos de forma independiente. Está dirigido a desarrolladores senior, ingenieros de plataformas y equipos de innovación en empresas españolas que buscan automatizar flujos de trabajo de ingeniería de alto nivel y pasar de la "escritura de código" a la "supervisión de agentes".

Principal ventaja profesional
En mi opinión profesional, tras analizar sus capacidades, la razón definitiva para adoptarlo es su arquitectura orientada a la autonomía real: la capacidad de definir y lanzar "subagentes" dinámicos que trabajan en paralelo sin saturar el contexto principal. Esto permite delegar tareas completas (como una refactorización de microservicios o auditorías de seguridad en todo un repositorio) y solo intervenir en los puntos de decisión clave o revisión de artefactos.

Para quién no es
No es una herramienta para perfiles junior que aún necesitan aprender las bases del código, ni para empresas con políticas de seguridad ultra-restrictivas que no permitan la ejecución de agentes autónomos en sus máquinas. Profesionales que busquen un simple autocompletado de texto o que desconfíen de dejar que la IA maneje la terminal encontrarán esta herramienta intrusiva o excesivamente compleja para sus necesidades.

funcionalidades clave
- **Agentes Autónomos y Subagentes**: Capacidad del agente principal para crear agentes secundarios especializados en tareas específicas para mantener limpio el contexto.
- **Scheduled Tasks**: Programación de tareas recurrentes (crons) ejecutadas por agentes de IA de forma asíncrona.
- **Project-based Context**: Superación del límite del "repositorio único"; los agentes pueden acceder a múltiples directorios y carpetas bajo un concepto de "Proyecto".
- **Comandos /goal y /grill-me**: El modo /goal obliga al agente a intentar terminar la tarea sin pedir feedback constante, mientras que /grill-me fuerza a la IA a preguntar detalles antes de empezar para asegurar el alineamiento.
- **Browser-in-the-loop**: Integración nativa del navegador para que los agentes realicen tareas de investigación web o pruebas de UX de forma automatizada.

Precios
- **Versión Gratuita**: Disponible para desarrolladores individuales con límites de uso estándar.
- **AI Ultra Plan ($100 - $200 / mes)**: Escala de precios orientada a profesionales y empresas que requieren límites de cómputo hasta 20 veces superiores a los planes básicos.
- **Enterprise**: Integrado en las suscripciones de Gemini Enterprise con capacidades de administración centralizada.

Perfil del usuario
- Empresas de software con grandes bases de código (monorepos) que requieren mantenimiento automatizado.
- Departamentos de DevOps que buscan automatizar scripts de infraestructura mediante lenguaje natural.
- Equipos de QA y UX que deseen automatizar flujos de navegación real mediante agentes con acceso a navegador.

Nivel técnico requerido
- Nivel de uso: Medio. Es necesario saber guiar a un agente y entender las implicaciones de sus acciones en el sistema.
- Instalación/Configuración: Medio. Requiere configuración de workspaces y gestión de permisos de lectura/escritura en el SO.
- Competencias necesarias: Conocimiento de flujos de trabajo Git, terminal (CLI) y principios de seguridad en la ejecución de scripts.

Ejemplos de uso profesional
- **Refactorización Masiva**: Pedir al agente que actualice todas las llamadas a una API antigua en 15 servicios diferentes, ejecutando pruebas unitarias en cada uno.
- **Auditoría de Seguridad Continua**: Programar una tarea semanal para que un agente revise nuevos commits en busca de secretos expuestos o vulnerabilidades conocidas.
- **Migración de Dependencias**: Delegar el proceso de actualización de versiones de librerías críticas, incluyendo la resolución de conflictos de breaking changes.

Uso y distribución
- Versión escritorio: macOS, Linux y Windows (aplicación independiente).
- CLI: Herramienta de línea de comandos para automatizar la creación de agentes desde la terminal.
- SDK: Para desarrolladores que quieran integrar el motor de agentes en sus propios flujos de trabajo.

Integraciones
- Facilidad de integración: High Code / SDK. Requiere conocimientos de desarrollo para integraciones profundas.
- API propia: Dispone de API para conectar con el ecosistema de Google Cloud.
- Integración nativa: Conexiones directas con Google AI Studio, Firebase, Android y Google Cloud.
- Exportación: Herramienta de exportación a Google AI Studio para continuar trabajos locales en la nube.

Notas finales
Veredicto técnico
Es una herramienta de gran utilidad para empresas que ya han superado la fase de "chatbots" y buscan una verdadera automatización de la ingeniería. Sin embargo, quiero destacar que su potencia es su mayor riesgo. A principios de 2026 se detectaron vulnerabilidades críticas de ejecución de código mediante inyección de prompts en sus herramientas de búsqueda de archivos (ya parcheadas). Mi recomendación profesional es usarla siempre en entornos controlados o con el modo "Strict Mode" actualizado, tratando siempre el contenido de terceros como no confiable.

información legal, licencias , contratos
- El uso empresarial suele quedar bajo el paraguas de los contratos de Google Cloud o Gemini Enterprise, lo que asegura que los datos no se utilizan para entrenar modelos públicos en versiones corporativas pagas.

Otros
- El cambio a la versión 2.0 marca el fin de Antigravity solo como un IDE; ahora es una plataforma de agentes general que pronto se expandirá a tareas de "trabajo de conocimiento" más allá del código puro.

Fuentes consultadas:
- Sitio web oficial
- Introducing Google Antigravity 2.0
- Google launches Antigravity 2.0 at I/O 2026
- Vulnerability Report: Prompt Injection to RCE
- Technical Analysis for Chief Penetration Testers
- Security Review: Antigravity AI

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Según mi experiencia, Google Antigravity 2.0 es una herramienta diseñada específicamente para empresas tecnológicas o departamentos de IT con un volumen de deuda técnica considerable o flujos de trabajo de ingeniería complejos. Lo que más me gusta es su enfoque en la autonomía real; no es un simple asistente de completado, sino un motor de ejecución. En mi opinión profesional, es ideal para empresas que manejan monorepos o microservicios donde la coordinación manual consume demasiado tiempo de los desarrolladores Senior. El presupuesto estimado es elevado para un entorno individual (100-200 mensuales), pero el ahorro en horas de ingeniería justifica la inversión en equipos de más de 10 desarrolladores. Mi experiencia me dice que es el paso lógico tras agotar la productividad que ofrecen herramientas como GitHub Copilot, pasando de la asistencia a la delegación.

Madurez digital requerida
- Los usuarios deben ser desarrolladores senior o ingenieros de plataformas con sólidos conocimientos en CLI, Git y gestión de permisos de sistema. No es apto para perfiles que no comprendan la trazabilidad del código.
- La empresa debe contar con una cultura de automatización (DevOps/SRE) y políticas claras de seguridad de datos, ya que la herramienta interactúa directamente con el sistema de archivos y el hardware local.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Evaluación de infraestructura (1 semana): Auditoría de permisos en máquinas locales y compatibilidad con el stack tecnológico de la empresa.
- Prueba de concepto - PoC (2-3 semanas): Selección de un repositorio específico para realizar tareas de refactorización controlada o auditoría de seguridad mediante el comando /goal.
- Configuración y Strict Mode (1 semana): Implementación de capas de seguridad adicionales para evitar inyecciones de prompt en entornos locales.
- Despliegue progresivo (1 mes): Extensión del uso a equipos de QA para automatización de pruebas de navegador con Browser-in-the-loop.
- Seguimiento y revisiones (Trimestral): Auditoría de los logs de los agentes y ajuste de los límites de cómputo para optimizar el ROI.

Necesidades de formación del equipo
Es imprescindible formar al equipo en ingeniería de prompts avanzada orientada a agentes (Agentic Prompting). Al usarlo te das cuenta de que la clave no es pedir código, sino definir objetivos y criterios de aceptación claros para que el agente pueda operar sin intervención. También se requiere capacitación en seguridad para identificar posibles riesgos de ejecución de código malicioso derivado de fuentes externas.

Perfiles necesarios
- Lead Developer o Arquitecto de Software para supervisar la orquestación.
- Especialista en Ciberseguridad para configurar el entorno de ejecución "Strict Mode".
- DevOps Engineer para la integración con pipelines de CI/CD si se usa la CLI.

Retorno de la inversión (ROI)
- El retorno se empieza a percibir entre los 3 y 6 meses tras la estabilización de los flujos de agentes.
- Los KPIs principales deben ser: Reducción del tiempo de ciclo en tareas de mantenimiento (refactoring, updates), número de vulnerabilidades detectadas de forma autónoma y volumen de líneas de código bajo criterios de calidad automática cumplidos sin intervención humana.

Otros
Según mi experiencia en implantaciones, el mayor desafío no es técnico, sino cultural: los desarrolladores deben aprender a confiar en que la IA maneje la terminal. Al principio, la fricción es alta, pero una vez configurado el comando /grill-me (donde la IA pregunta hasta estar segura), la confianza del equipo aumenta drásticamente. Mi opinión profesional es que el modo asíncrono (Scheduled Tasks) es la joya oculta de esta herramienta para mantener la salud del código mientras el equipo duerme.

TUTORIAL BÁSICO

Instalación
Para comenzar con Google Antigravity 2.0 (el sucesor oficial de Gemini CLI), dispones de dos vertientes: la aplicación de escritorio (un fork de VS Code optimizado para agentes) y la herramienta de línea de comandos (CLI).
- **CLI (macOS/Linux):** Ejecuta curl -fsSL https://antigravity.google/cli/install.sh | bash.
- **CLI (Windows PowerShell):** Usa irm https://antigravity.google/cli/install.ps1 | iex.
- **Migración:** Si vienes de Gemini CLI, utiliza el comando antigravity migrate --from-gemini-cli para importar tus configuraciones y "skills" previas.
- **Autenticación:** Al terminar la instalación, ejecuta antigravity auth login. En entornos locales abrirá el navegador; en sesiones SSH remotas, te proporcionará una URL de autorización manual.
- **Checklist inicial:** Según mi experiencia, es vital verificar que tienes instalado **Go 1.21+** si planeas compilar desde fuente y contar con una suscripción activa a **Google AI Pro**, ya que el acceso gratuito está restringido en esta versión.

Uso en el día a día
La herramienta está diseñada para que el agente realice el "trabajo sucio" de navegar por el código y ejecutar pruebas.
- **Modo Meta:** Usa /goal seguido de tu tarea (ej. /goal Refactoriza el sistema de login a JWT). El agente trabajará de forma autónoma hasta finalizar, sin pedir confirmaciones constantes.
- **Comando Inline:** En el IDE, pulsa Ctrl + I (Win/Linux) o Cmd + I (Mac) para pedir cambios directos en el código o comandos de terminal en lenguaje natural. Lo que más me gusta es su capacidad para entender el contexto de todo el proyecto, no solo del archivo abierto.
- **Navegación rápida:** Aprende los atajos de teclado esenciales. Ctrl + K (o Cmd + K) es el comando universal para abrir el selector de conversación o aprobar instantáneamente los permisos que solicita un subagente.

Trucos de experto
- **Encadenamiento de subagentes:** Puedes abrir el panel /agents para monitorizar tareas que se ejecutan en segundo plano. Mi experiencia me lleva a pensar que la mejor forma de optimizar es delegar tareas de testing extensas a subagentes mientras sigues programando en el hilo principal.
- **Configuración mediante `.antigravity.yaml`:** Crea este archivo en la raíz de tu proyecto para definir el modelo (ej. gemini-3.5-flash), activar el sandbox por defecto y definir comandos de test automáticos (test_command: "npm test").
- **El comando `/grill-me`:** Úsalo antes de empezar una tarea compleja. Obliga al agente a hacerte preguntas detalladas antes de tocar una sola línea de código, evitando errores por suposiciones incorrectas.
- **Teletransporte:** En la CLI, si tienes varios procesos, usa la tecla j para "saltar" directamente a la vista detallada del subagente que está esperando tu aprobación.

Posibles problemas/incidencias
- **Vulnerabilidad de inyección indirecta:** Se ha detectado que archivos externos (como READMEs de repositorios públicos) pueden contener instrucciones ocultas en comentarios que engañan al agente para ejecutar código malicioso. En mi opinión profesional, nunca proceses repositorios desconocidos sin revisar antes el contenido de forma manual o en un entorno aislado.
- **Fallo en `/find_by_name`:** Existía una vulnerabilidad crítica que permitía saltarse el modo seguro inyectando flags como -Xsh. Asegúrate de estar usando una versión posterior a **febrero de 2026** donde este fallo fue parcheado.
- **Persistencia de configuraciones:** Cuidado con el directorio ~/.gemini/antigravity/mcp_config.json. Algunos ataques intentan modificar este archivo para crear backdoors. Si notas comportamientos extraños, revisa manualmente que no haya servidores MCP sospechosos registrados.
- **Incompatibilidades:** La versión de escritorio no es compatible con procesadores x86 en macOS; requiere obligatoriamente Apple Silicon para un rendimiento óptimo.

Otros
- **Consumo de tokens:** Al usar Gemini 3.5 Flash, la velocidad es altísima (casi 300 tps), pero el consumo de cuota en proyectos grandes puede ser elevado si el agente "escanea" recursivamente demasiados archivos. Configura adecuadamente el archivo .gitignore para que el agente no pierda tiempo indexando carpetas pesadas como node_modules o dist.

PREGUNTAS FRECUENTES

¿Qué es Google Antigravity 2.0 y en qué se diferencia de un asistente de IA convencional?

Google Antigravity 2.0 es un entorno de desarrollo e investigación basado en agentes autónomos, diseñado como una aplicación de escritorio nativa. A diferencia de los chatbots tradicionales que solo generan texto, Antigravity puede orquestar tareas complejas, navegar por sistemas de archivos, ejecutar comandos en la terminal y gestionar subagentes para trabajar en paralelo dentro de sistemas operativos macOS, Linux y Windows.

¿Cuál es el perfil profesional recomendado para utilizar esta herramienta?

Está orientada a perfiles técnicos senior, ingenieros de plataformas, desarrolladores de DevOps y equipos de innovación. Requiere un nivel técnico medio para la configuración de workspaces y gestión de permisos, además de conocimientos sólidos en flujos de trabajo Git y ejecución de scripts en línea de comandos (CLI).

¿Qué costes tiene y existen opciones para uso individual?

El sistema ofrece una versión gratuita para desarrolladores individuales con límites de uso estándar. Para profesionales que requieren mayor capacidad de cómputo, existe el plan AI Ultra (entre 100 y 200 USD mensuales). A nivel corporativo, se integra dentro de las suscripciones de Gemini Enterprise con capacidades de administración centralizada.

¿Es una tecnología segura para entornos corporativos?

Aunque es una herramienta potente, se han detectado vulnerabilidades críticas de ejecución de código mediante inyección de prompts en versiones anteriores. Se recomienda su uso en entornos controlados, activando siempre el 'Strict Mode' y tratando el contenido de terceros como no confiable. Las versiones empresariales pagas garantizan contractualmente que los datos no se utilizan para entrenar modelos públicos.

¿Qué funciones específicas ofrece para la automatización de tareas?

Incluye capacidades de 'Scheduled Tasks' para ejecutar crons asíncronos mediante IA, y comandos especializados como '/goal' para finalización autónoma de tareas y '/grill-me' para alineación previa de requisitos. También cuenta con 'Browser-in-the-loop' para realizar investigaciones web o pruebas de UX de forma automatizada.

¿Cómo gestiona la privacidad de los datos y el cumplimiento normativo?

En el entorno empresarial, el uso queda regulado por los contratos de Google Cloud y Gemini Enterprise. Esto asegura el cumplimiento de estándares de privacidad profesionales, evitando que el código propietario o la información de la infraestructura se filtre hacia el entrenamiento de modelos de lenguaje generales de Google.

¿Permite el trabajo con múltiples repositorios de forma simultánea?

Sí, mediante el concepto de 'Project-based Context', la herramienta supera la limitación del repositorio único. Los agentes pueden acceder y operar en múltiples directorios y carpetas bajo un mismo proyecto, facilitando tareas como la refactorización de microservicios o auditorías de seguridad en entornos de monorepositorios.

¿Dispone de SDK o API para integración personalizada?

Antigravity cuenta con una API propia para la conexión con el ecosistema de Google Cloud y un SDK destinado a desarrolladores que deseen integrar su motor de agentes en flujos de trabajo personalizados (High Code). Además, permite la exportación directa de trabajos locales a Google AI Studio.

CONTRATOS Y CONDICIONES

Opinión inicial
Tras verificar los contratos de servicio de Google y las condiciones específicas de la familia de productos Gemini y herramientas de desarrollo avanzadas, mi opinión profesional es que nos encontramos ante una herramienta de **impacto legal alto**. Google Antigravity 2.0 no es un simple editor, sino un entorno de agentes autónomos con capacidad de ejecución de comandos (RCE) y acceso a archivos locales. Para una empresa española, esto implica riesgos significativos bajo el RGPD y la nueva Ley de IA de la UE, especialmente por la delegación de decisiones en sistemas autónomos y la gestión de la propiedad intelectual de los resultados generados sin supervisión humana constante.

Principales recomendaciones
- Activar obligatoriamente el **Modo Estricto (Strict Mode)** para limitar la ejecución de comandos automatizados sin validación manual previa.
- Configurar el entorno exclusivamente bajo licencias **Enterprise** (Gemini Enterprise o Google Cloud) para garantizar contractualmente que los datos del código fuente no se utilicen para el entrenamiento de modelos globales.
- Realizar una Evaluación de Impacto en la Protección de Datos (EIPD) antes de permitir que los agentes accedan a bases de datos con información de carácter personal.
- Establecer una política interna que prohíba el uso de comandos como /goal en entornos de producción, limitándolo estrictamente a entornos de desarrollo y staging.
- Formar a los desarrolladores en la detección de **Inyección de Prompts Indirecta**, ya que un agente al navegar por internet o leer archivos externos puede recibir instrucciones maliciosas que comprometan el sistema local.

Ley de Inteligencia Artificial (AI Act)
- Al ser un sistema de IA de propósito general con capacidades de agente, tras verificar la clasificación del AI Act, la empresa debe asegurar que el uso de Antigravity no derive en vigilancia de empleados o toma de decisiones automatizada que afecte a derechos fundamentales.
- Existe una responsabilidad de **transparencia**: los usuarios deben ser conscientes de que están interactuando con agentes y los resultados (commits, auditorías) deben ser etiquetados como generados por IA según el Artículo 52.

Privacidad y protección de datos
- **Responsabilidades**: La empresa española actúa como Responsable del Tratamiento, mientras que Google, bajo el Addendum de Procesamiento de Datos (DPA) de Google Cloud, actúa como Encargado del Tratamiento.
- **Ubicación de los datos**: Aunque la aplicación es de escritorio, el procesamiento de los modelos Gemini ocurre en servidores de Google. Es crítico configurar la residencia de datos en la región de la UE mediante la consola de Google Cloud.
- **Transferencia internacional**: Se basa en las Cláusulas Contractuales Tipo (SCC) incluidas en los términos de Google Cloud, cumpliendo con los requisitos tras la sentencia Schrems II, siempre que se active la protección de datos empresariales.
- **Derechos ARCO**: El sistema debe permitir la exportación o eliminación de los logs de actividad de los agentes donde pueda figurar información personal del desarrollador o de terceros.

Propiedad intelectual
- **Propiedad de datos**: Según los documentos de términos de servicio de Google para suscriptores de pago, Google no reclama la propiedad de los archivos de entrada (código fuente) ni de las instrucciones (prompts).
- **Propiedad del resultado**: Los fragmentos de código generados por los agentes de Antigravity son propiedad del cliente. Sin embargo, bajo la legislación española y europea, el software puramente generado por IA sin intervención humana creativa e identificable puede carecer de protección por derechos de autor, quedando en el dominio público o bajo protección contractual limitada.

Usos y prohibiciones
- **Usos prohibidos**: Ejecución de agentes para ataques de denegación de servicio (DoS), ingeniería inversa de servicios de Google, o procesamiento de datos de categorías especiales (salud, religión) sin las medidas de seguridad adicionales de cumplimiento (como HIPAA para Google Cloud).
- **Usos admitidos**: Automatización de flujos de DevOps, refactorización de código privado, auditorías internas

de seguridad y generación de documentación técnica.

Seguridad y certificaciones
- **Seguridad**: Implementa medidas de sandboxing para el navegador integrado (Browser-in-the-loop), aunque la vulnerabilidad de inyección de prompts reportada en 2026 demuestra que el aislamiento del sistema de archivos sigue siendo un punto crítico de vigilancia.
- **Certificaciones**: Al estar integrado en el ecosistema Enterprise, se beneficia de certificaciones **ISO/IEC 27001, 27017, 27018 y cumplimiento SOC 2/3**.

Otros
Es fundamental recalcar que el uso de la versión gratuita (Free Edition) no ofrece las mismas garantías de privacidad. En la versión gratuita, las interacciones pueden ser revisadas por humanos o utilizadas para mejorar el modelo, lo que supondría una violación de secreto comercial si se procesa código propietario de la empresa.

Fuentes consultadas:
- Google Cloud Terms of Service
- Data Processing Addendum (DPA) - Google
- Gemini for Google Cloud Privacy and Security
- Vulnerability Report: Prompt Injection to RCE
- EU AI Act Compliance Guide