OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Declaración de Capacidades

Evaluación adversarial para sistemas de IA científica.

Los modelos de lenguaje científicos, agentes de investigación y flujos de datos sensibles se evalúan mediante pruebas autorizadas de alcance definido e informes con evidencia.

Desde $10,000 por proyecto

Competencias principales

Evaluación de sistemas de IA científica
Evaluación autorizada de modelos de lenguaje científicos, procesos de evaluación y agentes co-científicos dentro del alcance aprobado por el cliente.

Aseguramiento de datos científicos sensibles
Revisión de flujos de datos biológicos, químicos y otros datos sensibles, incluidos límites de acceso, controles y prácticas de manejo.

Riesgo y corrección basados en evidencia
Hallazgos documentados, evidencia reproducible y recomendaciones priorizadas para responsables científicos, de seguridad y cumplimiento.

A quiénes apoyamos

Organizaciones de investigación y equipos que desarrollan u operan sistemas de IA científica, agentes de investigación y procesos con datos científicos sensibles.

https://tortzal.com · contact@ozcorp.io

© All Rights Reserved

OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Evaluación de modelos y sistemas de prueba

Evaluar el comportamiento declarado, los límites de confiabilidad y los controles de supervisión de modelos científicos.

Alcance del trabajo

- Definición del sistema y su uso previsto
- Cobertura de evaluación y criterios de aceptación
- Revisión de limitaciones y supervisión documentadas
- Hallazgos priorizados para responsables del sistema

Proceso de trabajo

01 **Definir autorización y alcance**
Confirmar sistema, uso previsto, métodos permitidos y límites de evaluación.

02 **Establecer criterios**
Acordar requisitos observables, medidas de éxito y evidencia esperada.

03 **Realizar evaluación controlada**
Evaluar el sistema dentro del entorno y alcance aprobados.

04 **Revisar resultados y límites**
Contrastar observaciones con criterios y documentar incertidumbres.

05 **Informar hallazgos**
Entregar evidencia y recomendaciones a responsables del sistema.

Aplicaciones
Modelos de lenguaje científicos, procesos de evaluación y sistemas de supervisión.

Nota de alcance
La evaluación es autorizada y delimitada. Los resultados describen el alcance probado y no garantizan el comportamiento futuro.

Equipos participantes
Tortzal, Science

NAICS sugerido

541690 Otros servicios de consultoría científica y técnica
541511 Programación informática personalizada
541990 Otros servicios profesionales, científicos y técnicos.

PSC sugerido

B524, B529 y B544 estudios y análisis científicos
AJ11 servicios de I+D en ciencia y tecnología.

© All Rights Reserved

OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Aseguramiento de agentes y herramientas de investigación

Revisar la interacción de agentes de investigación con herramientas, datos y puntos de aprobación humana en sistemas autorizados.

Alcance del trabajo

- Inventario de flujos de agentes y acceso a herramientas
- Revisión de supervisión y límites de autorización
- Evaluación controlada frente a requisitos acordados
- Hallazgos asignados a responsables y prioridades correctivas

Proceso de trabajo

01 **Mapear el flujo del agente**
Documentar tareas previstas, herramientas, datos y decisiones humanas.

02 **Revisar permisos y límites**
Evaluar controles de acceso, aprobaciones y responsabilidades.

03 **Evaluar requisitos acordados**
Realizar comprobaciones controladas en los sistemas y métodos autorizados.

04 **Documentar observaciones**
Registrar resultados, evidencia, límites y contexto operacional.

05 **Priorizar mejoras**
Asignar próximos pasos a los equipos responsables del sistema.

Aplicaciones
Agentes de investigación, herramientas científicas y procesos con supervisión humana.

Nota de alcance
Las pruebas se limitan a sistemas y acciones autorizados explícitamente para el proyecto.

Equipos participantes
Tortzal, InfraOps, Ozcorp Scientific

NAICS sugerido

541511 Programación informática personalizada
541519 Otros servicios relacionados con informática
541690 Otros servicios de consultoría científica y técnica.

PSC sugerido

D307 Estrategia y arquitectura de TI
B524 y B529 estudios y análisis científicos.

© All Rights Reserved

OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Revisión de flujos con datos científicos sensibles

Evaluar sistemas con datos científicos sensibles, incluidos movimiento de datos, accesos, retención y responsabilidad operacional.

Alcance del trabajo

- Clases de datos y límites de los procesos
- Revisión de controles de acceso y manejo
- Documentación de riesgos y evidencia
- Recomendaciones para los equipos responsables

Proceso de trabajo

01 **Definir datos y alcance**
Identificar clases de datos, sistemas, propósitos y límites de revisión.

02 **Mapear el movimiento de datos**
Documentar fuentes, transformaciones, almacenamiento y accesos.

03 **Revisar salvaguardas**
Evaluar acceso, retención, validación y responsables operacionales.

04 **Registrar riesgos y evidencia**
Describir controles observados y su contexto de apoyo.

05 **Recomendar medidas correctivas**
Priorizar mejoras para los equipos responsables del manejo de datos.

Aplicaciones
Flujos con datos biológicos, químicos y otros datos científicos sensibles.

Nota de alcance
La revisión no sustituye determinaciones legales, de privacidad, bioseguridad o regulatorias del cliente.

Equipos participantes
Tortzal, Science, InfraOps

NAICS sugerido

541690 Otros servicios de consultoría científica y técnica
541519 Otros servicios relacionados con informática
541990 Otros servicios profesionales, científicos y técnicos.

PSC sugerido

B524, B529 y B544 estudios y análisis científicos
D307 Estrategia y arquitectura de TI.

© All Rights Reserved

OZCORP SCIENTIFIC LLC
7 Calle Tabonuco Ste 105
Guaynabo, PR 00968

Paquete de evidencia e informe de decisión

Convertir una evaluación aprobada en hallazgos claros y próximos pasos para equipos técnicos, científicos y de gobernanza.

Alcance del trabajo

- Resumen ejecutivo de hallazgos
- Catálogo de escenarios y resultados
- Paquete de evidencia reproducible
- Hoja de ruta correctiva priorizada

Proceso de trabajo

01 **Consolidar registros**
Reunir alcance, métodos, observaciones y evidencia aprobados.

02 **Validar hallazgos**
Comprobar que las conclusiones estén respaldadas por resultados.

03 **Evaluar impacto y prioridad**
Organizar hallazgos por importancia, responsables y medidas correctivas.

04 **Preparar el informe**
Comunicar hallazgos y límites a equipos técnicos y de liderazgo.

05 **Entregar el paquete**
Proveer registros acordados y una hoja de ruta práctica.

Aplicaciones
Revisión técnica, decisiones de gobernanza, planificación correctiva y comunicación de riesgos.

Nota de alcance
Los informes reflejan el alcance probado, la evidencia disponible y los criterios acordados.

Equipos participantes
Tortzal, Ozcorp Scientific

NAICS sugerido

541690 Otros servicios de consultoría científica y técnica
541990 Otros servicios profesionales, científicos y técnicos.

PSC sugerido

B524, B529 y B544 Estudios y análisis especiales.

© All Rights Reserved