

Bueno ahora en esta tercera entrega le implemente las métricas de observabilidad, la latencia de ejecución, el estado de finalización, el consumo de recursos(Tokens) Análisis de registros y trazabilidad, intervención de seguridad y flujo exitoso. por último los protocolos de seguridad y ética, el filtrado local, el manejo de errores de azure, en resumen se realizó la integración de mecanismos de observabilidad y. El sistema ahora no solo ejecuta tareas complejas de investigación, sino que ofrece visibilidad sobre su propio funcionamiento y protege activamente contra usos indebidos, cumpliendo con los requisitos de un entorno de producción moderno y fiable.

Encargado de validar inputs y asegurar que el agente actúe dentro de normas éticas.

```
"""
def __init__(self):
    self.forbidden_terms = [
        "hackear", "ilegal", "delito", "malware",
        "explotar vulnerabilidad", "bomba", "arma", "explosivo",
        "atentado", "muerte", "suicidio", "veneno", "terrorismo",
        "narcotráfico", "secuestro"
    ]

    def validate_input(self, user_input: str) -> bool:
        """Valida que el input sea seguro y ético."""

-----
        except BadRequestError as e:
            logger.warning(f"[{request_id}] Bloqueo por Política de
Contenidos del Modelo (Azure/OpenAI): {e}")
            return "La solicitud fue procesada pero rechazada por el
sistema de seguridad."
```