Miradas Criticas sobre la Tecnología: Auditoria de TI y Ética en IA

Autor: Marc A. González Figueroa
Mentor: Ph.D Alfredo Cruz Triana
Departamento de Ciencia de Cómputos

Abstracto

Este artículo integra, la Auditoría en Tecnología de la Información (TI), la Ética en el uso de la Inteligencia Artificial (IA) y el impacto de estas herramientas en la ciberseguridad y en la sociedad. En primer lugar, integra los procesos de la Auditoría a los nuevos entornos de riesgo que presentan la IA. Para ello, describe la evaluación de controles, la recolección de evidencia y la presentación de hallazgos en un nuevo contexto. Hace hincapié en las auditorías de IA, en lo que se refiere a la ciberseguridad, y le da mucho peso a la integridad, la confidencialidad y la disponibilidad de los sistemas. Lo hace dentro de un marco de Ética, que no es específica de la IA, pero que se presenta como muy necesaria y obligatoria para los auditores, por las implicaciones que tiene el uso de la IA y la falta de facultades que tienen para, por ejemplo, determinar si un algoritmo es justo o no.

Introducción

La auditoría de TI evalúa los sistemas computacionales de una entidad de forma sistemática y metódica, buscando asegurarse de que estos sistemas cumplan con los estándares de integridad, disponibilidad y confidencialidad. La ética en IA se ocupa, dentro de ese contexto, de establecer principios morales que protejan la integridad de los algoritmos, asegurando que estos actúen sin sesgos y, además, que respeten la privacidad, la equidad y los derechos humanos. La unión de estos dos campos del saber favorece el surgimiento de una cultura tecnológica que vale la pena ayudar y hacer crecer.

Trasfondo

Las auditorías de TI permiten no solo identificar vulnerabilidades, sino también asegurar el cumplimiento normativo y proteger la integridad, confidencialidad y disponibilidad de los datos. Sin embargo, en muchas instituciones, esas prácticas no se realizan de forma periódica y profunda, lo que deja expuestos a los sistemas ante ciberataques, pérdida de información, y errores de configuración que podrían evitarse con un enfoque preventivo y sistemático. Tenemos el ciclo de Auditoria de TI planificación, recolección, informe y seguimiento.

El dilema ético en la toma de decisiones entre seres humanos y sistemas de Inteligencia Artificial (IA). En ella se presenta una balanza que simboliza la tensión entre la justicia, asociada a las decisiones humanas, y la precisión, representada por los algoritmos. Esta comparación gráfica resalta la tendencia de los humanos a considerar al tomar decisiones (típicamente judiciales) más factores morales, contextuales y empáticos que decisiones "automáticas" que tomarían por ejemplo una IA.

Problema

Este proyecto analiza la importancia de integrar la auditoría de TI con principios éticos en sistemas de IA. Busca concienciar sobre riesgos técnicos y morales derivados de la automatización, promoviendo controles que aseguren transparencia, equidad y responsabilidad. Además, propone herramientas para evaluar la robustez técnica y el impacto social de estos sistemas, con énfasis en la privacidad, los derechos humanos y la toma de decisiones, fomentando así una cultura tecnológica responsable.

Metodología

Fase 1: Marco Teórico y conceptual
En el Módulo 1, se establecieron los fundamentos de la auditoría de TI: principios del modelo CIA (confidencialidad, integridad, disponibilidad), tipos de auditoría, rol del auditor, auditoría interna vs. externa y la relevancia de normativas como ISO 27001 y GDPR. El Módulo 2 abordó la ética en IA, incluyendo principios como justicia, transparencia, privacidad, responsabilidad y autonomía, así como el ciclo de vida de un sistema de IA.

Fase 2: Análisis de herramientas y practicas
Se investigaron y aplicaron herramientas de auditoría tecnológica como InvGate (gestión de activos, licencias y contratos), Netwrix Auditor (seguimiento de cambios y eventos de seguridad), y Risk Cloud de LogicGate (evaluación y monitoreo de riesgos operativos).

Fase 3: Análisis ético y estudio de casos
Se analizaron casos reales: COMPAS (sistema judicial con sesgos raciales), el sistema de contratación de Amazon (discriminación de género), Tay Bot de Microsoft (contenido ofensivo), y vehículos autónomos de Uber (decisiones críticas de vida o muerte). Se promovieron debates éticos, identificación de afectados y propuestas de solución aplicando los principios aprendidos.

Fase 4: Evaluación y síntesis
Cada módulo concluyó con evaluaciones por nivel (básico, intermedio, avanzado). Se elaboraron informes de auditoría simulados con resumen ejecutivo, riesgos, impactos y recomendaciones, fomentando una comprensión crítica e integral.

Figura 1 Herramientas en la Auditoria de TI

Tabla 1 Herramientas en la Auditoria de TI

Herramienta	Funcionalidad	Uso en el modulo	Ventajas
InvGate	Gestión de inventario de activos de TI	Registro y clasificación de dispositivos	Interfaz intuitiva y fácil de usar
Netwrix Auditor	Auditoria de cambios en sistemas de TI	Monitoreo de cambios y actividad	Reportes automáticos de eventos
Logic Gate	Gestión de Riesgo	Evalúa de riesgo	Integraciones flexibles

Resultados y Discusión

El desarrollo e implementación de los módulos de auditoría y ética en inteligencia artificial ofrecieron resultados significativos en cuanto a la comprensión y la aplicación de conceptos clave, tanto en el ámbito técnico como en el ético. En el ámbito técnico, los participantes concentraron sus esfuerzos en desglosar y aprehender las fases de la auditoría de TI:

- Planificación
- Evaluación
- Recolección de evidencia
- Informe final

Estas actividades fueron llevadas a cabo por los participantes en ese mismo orden, haciendo uso de algunas herramientas que probablemente son nuevas para ellos.

Las actividades prácticas permitieron simular situaciones del mundo real donde se evaluaron los controles internos y se documentaron las vulnerabilidades. Contribuyeron a desarrollar habilidades para la elaboración de auditorías, formulando recomendaciones correctivas con base en lo que se había encontrado.

Esto en cierto modo fue un ensayo para la etapa de prácticas en el programa. En el terreno de lo ético, los estudiantes diseccionaron los sistemas de Inteligencia Artificial por el uso de los cuales se ven involucrados en dilemas morales. Y, como es de suponer, trabajaron sobre todo a partir de elucidar situaciones hipotéticas. Pero el panorama que les dibujaron las elucubraciones no pasó de ser apocalíptico. Más bien, la conclusión a la que llegaron fue que no hay solución de problemas que valga si los algoritmos no son justos, y si, además, como demuestra la experiencia, aceptan el sesgo como parte de su día a día. El reconocimiento de que es un problema de justicia lo convierte, sin duda, en un problema ético.

Figura 2 Dilemas éticos en la inteligencia artificial

Conclusión

Este proyecto demostró que la unión de la auditoría de TI con los principios éticos de la IA es pertinente y necesaria, sobre todo en el contexto digital actual. Los participantes recibieron formación técnica en procesos de auditoría y lograron adquirir competencias fundamentales para: Evaluar infraestructuras, tecnológicas, identificar vulnerabilidades, Proponer medidas correctivas, cumplir con estándares que aseguran la ciberseguridad de la organización.

Al mismo tiempo, analizar los riesgos éticos vinculados a la utilización de sistemas inteligentes hace visible lo que puede ocurrir (y ya está ocurriendo) cuando decisiones automatizadas mandan un mensaje de que esta o aquella conducta es la correcta, sin que alguien haya pensado competentemente y de antemano en qué es lo justo. Para concluir, la convergencia de auditoría y ética tecnológica es esencial para afrontar los retos actuales y anticiparse a los que planteará el futuro digital, y esto desde una perspectiva que no sólo sea crítica y preventiva, sino también humanista.

Trabajos Futuro

Como parte del desarrollo continuo de estos módulos, el trabajo futuro debe enfocarse en reforzar aún más la integración entre teoría y práctica, mediante simulaciones, laboratorios interactivos y estudios de caso actualizados. Debe implementarse más bien la propuesta de espacios donde los estudiantes auditen sistemas reales, o diseñen soluciones tecnológicas, bajo un control ético.

Por último, es necesario que haya una plataforma digital que dé soporte a la continuidad del aprendizaje de los alumnos de la materia. Esto incluiría recursos, foros, evaluaciones adaptadas y, sobre todo, actualizaciones que permitan que el conocimiento impartido evolucione al mismo ritmo que lo hace la tecnología.

Agradecimientos

Le quiero dar primero gracias a mi mentor Dr. Alfredo Cruz por guiarme y darme los consejos necesarios para poder cumplir con un trabajo de excelencias. Por ultimo, quisiera darle también las gracias a mis compañeros que fueron un pilar clave para llegar a un trabajo de excelencias.

Referencias

- InvGate, *InvGate Insight: IT Asset Management Platform*, s.f. Disponible en: https://invgate.com/es/asset-management
- Netwrix, *Netwrix Auditor Overview*, s.f. Disponible en: https://www.netwrix.com
- LogicGate, *Risk Cloud Platform*, s.f. Disponible en: https://www.logicgate.com/
- OCDE, *Artificial intelligence*, 2019. Disponible en: https://www.oecd.org/en/topics/artificial-intelligence.html
- European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence Cybersecurity Challenges*, 2020. Disponible en: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- CISA, Cybersecurity and Infrastructure Security Agency, 2023. Disponible en: https://www.cisa.gov/
- IEEE Standards Association, *Ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems*, IEEE, 2020.
- National Institute of Standards and Technology (NIST), *AI Risk Management Framework*, 2022. Disponible en: https://www.nist.gov/itl/ai-risk-management-framework