Shadow AI: Riesgo emergente y habilitación

DOI: 10.29236/sistemas.n177a2

Resumen

La Inteligencia Artificial Generativa ha emergido como un catalizador de cambio, entregando agilidad al negocio, pero planteando un desafío fundamental: gobernarla con propósito y confianza. Esta democratización impulsa a los usuarios a convertirse en desarrolladores, lo que genera la *Shadow AI* (TI en la Sombra), donde las soluciones se implementan fuera del marco de gobernanza por la necesidad de velocidad. El artículo examina la *Shadow AI* de forma constructiva, argumentando que la respuesta no es prohibir, sino habilitar. Se revisan lecciones históricas de riesgos (ej. hojas de cálculo) para justificar la necesidad de un enfoque proactivo de la función de Riesgos, que debe actuar como facilitador seguro, según el Dominio 2 (ISACA CRISC, 2024), superando actitudes conservadoras que imponen controles desalineados con el costo/beneficio. Se destaca la importancia de integrar a los desarrolladores en el proceso de seguridad, mientras sus roles se transforman de la codificación rutinaria hacia la gestión de infraestructura de IA y la arquitectura de *prompts*, requiriendo recapacitación. Se concluye que la IA debe ser un facilitador del negocio, requiriendo un paraguas de gobierno centralizado para canalizar la innovación de la sombra hacia una adopción estratégica y segura. Herramientas como el CASB (*Cloud Access Security Broker*) son esenciales para lograr la visibilidad y el control efectivo en entornos *cloud*.

Palabras Claves

IA Generativa, Shadow AI, Gobierno de la IA, Riesgo Tecnológico, Habilitación de Negocio, CASB

Héctor Calderazzi

Introducción

La Inteligencia Artificial Generativa no es una simple herramienta de productividad; es un catalizador de cambio que está entregando un poder significativo al usuario de negocio, prometiendo una agilidad sin precedentes. Esta democratización, sin una adecuada canalización, genera una fricción natural con los principios de gobernanza, seguridad y ética, impactando la Confianza Digital de la organización (Moyle, 2023).

Esto me alertó sobre el escenario de riesgo creciente: la Shadow AI, que es la manifestación más reciente del concepto amplio de TI en la Sombra (Shadow TI), definido como el uso de sistemas, *software* y servicios por fuera del circuito establecido para gobernar adecuadamente el ciclo de vida de los sistemas de información y sin considerar las áreas de TI y Seguridad de la Información entre otras.

Exploraremos las motivaciones positivas detrás de la Shadow AI, analizaremos cómo las lecciones del pasado y el rol proactivo del profesional de riesgos (CRISC – *Certified in Risk and Information Systems Control*) nos obligan a buscar soluciones de habilitación en lugar de prohibición. El objetivo es claro: demostrar cómo la IA debe ser un facilitador del negocio, guiando su adopción con propósito y seguridad.

La búsqueda de agilidad y el origen de la sombra

Se observa una tendencia clara: los usuarios quieren respuestas, no datos.

Además, las propias empresas de *software*, con una estrategia pujante, vienen en forma entusiasta por más y empujan a que cada usuario sea un desarrollador. Esta combinación de demanda de agilidad y la facilidad para acceder a *software* con capacidades de IA entusiasma a los usuarios y da origen a la Shadow AI, definida por ISACA como la “Nueva Frontera

del Riesgo Empresarial" (Rajasekharan, 2025), donde la proliferación de servicios de IA en aplicaciones comerciales está agravando el uso en la sombra (Moyle, 2023). El principal riesgo es que estas soluciones operan fuera del marco de gobernanza, arriesgando la Fuga de Propiedad Intelectual, el Sesgo y el Incumplimiento Normativo.

La Shadow TI (y su evolución, la Shadow AI) no surge por intención maliciosa, sino de la necesidad urgente de velocidad del negocio.

Los empleados y gerentes implementan estas soluciones *ad hoc* porque:

- Velocidad vs. Proceso: El proceso formal de TI para aprobar herramientas es percibido como lento y burocrático.

- Funcionalidad: Las herramientas sancionadas por TI no satisfacen las necesidades específicas.

- Descentralización: La facilidad para acceder a servicios *cloud* permite a las unidades de negocio resolver sus problemas con presupuestos departamentales.

Lecciones aprendidas: análisis de patrones de riesgo histórico

Para gestionar la Shadow AI de forma constructiva, es esencial analizar el patrón de comportamiento histórico de riesgo y aprender del patrón de riesgo tecnológico pasado. La historia de TI nos enseña que la Shadow TI aparece cuando la agilidad del negocio supera la capacidad de respuesta de la gobernanza, independientemente de la tecnología en uso.

- El riesgo de las hojas de cálculo masivas:

- Tecnología: Masificación de herramientas como Excel, utilizadas como bases de datos y motores de cálculo críticos (Aplicaciones de Usuario Final - EUC). Este riesgo sigue vigente hoy.

- Riesgo: Las planillas se democratizaron sin controles de identificación, trazabilidad o integridad (Tsang et al., 2022; Rodríguez, 2019). Esto genera errores de formulación que impactan decisiones financieras y comerciales (EUSPRIG, s.f.). El riesgo aquí no era el *software* en sí, sino la ausencia de un marco de gobernanza sobre información crítica fuera de los sistemas corporativos.

- Descentralización de datos y extracción (ETL):

- Tecnología: Uso creciente de herramientas de extracción de datos y transformación de datos (similares a ETL - Extracción, Transformación y Carga o *reporting tools*). El objetivo primario fue que cada área generase sus propios reportes.

- Riesgo: La dificultad de mantener y evolucionar los procesos ETL (que requieren cambios constantes de código debido a variaciones en los sistemas de origen) genera un alto riesgo de inconsistencia de los datos (Reed et al., 2010). Por ejemplo, errores en la tabla de tasas de comisiones de ventas pueden resultar en un cálculo erróneo del importe de la comisión.

  Al descentralizar este acceso sin el *expertise* de TI, la empresa sufre por la falta de integridad y la aparición de múltiples versiones de la verdad en la reportería.

• Interacción directa del usuario con el proveedor externo:

- Tecnología: La interacción de las unidades de negocio con el proveedor externo para la adquisición directa de *software*, servicios o la contratación de desarrolladores, evitando los canales formalmente establecidos por TI.

- Riesgo: Evitar el CVDS (Ciclo de Vida de Desarrollo de Sistemas) genera debilidad en el control de cambios y pérdida de documentación (IBM, s.f.), comprometiendo la seguridad, la continuidad operativa y la sostenibilidad del sistema.

La Shadow AI amplifica estos desafíos. El riesgo ahora no es una fórmula incorrecta, sino una decisión algorítmica no validada. La lección es clara: la solución nunca ha sido la prohibición, sino la habilitación controlada. El profesional de riesgos debe ser diligente en la identificación de estas soluciones en la sombra, estudiando los flujos de trabajo reales y revisando *logs* para entender las conexiones no aprobadas, aceptando que la Shadow TI existe, según el Dominio 2 (ISACA CRISC, 2024).

La postura conservadora vs. la habilitación proactiva

La forma en que se enfrenta la Shadow AI distingue a las organizaciones. Por un lado, tenemos la actitud basada en la seguridad pura, y por el otro, la que busca la habilitación:

• Caso de la actitud conservadora (Las 20 Observaciones):
  Recientemente, un colega me compartió un caso muy ilustrativo: el equipo de TI había identificado la solución ágil a una necesidad operativa de negocio mediante la implementación de un agente de IA. Sin embargo, la respuesta del equipo de control fue una lista de 20 observaciones que, si bien estaban técnicamente justificadas, no habían sido calibradas con una evaluación del impacto de los riesgos al negocio. Este enfoque, centrado solo en el riesgo inherente, implicó que la lista de 20 controles resultara más cara de implementar que el beneficio que la nueva aplicación aportaría al negocio.

Esta desalineación entre el control y la oportunidad frenó la innovación y refuerza la percepción del área de control como un obstáculo burocrático, sin que la intención fuera detener el negocio.

- El CISO como habilitador:
  Este caso ilustra por qué el Dominio 4 (ISACA CRISC, 2024) es vital: el profesional de riesgos debe ser un facilitador seguro que equilibre los controles con el valor. Si TI es reticente, el negocio encontrará su propia solución. El rol es liderar el esfuerzo para demostrar cómo se pueden incorporar nuevas tecnologías de forma segura en lugar de rechazar su adopción.

- **Habilitación controlada y el *sandbox*:** La solución es proporcionar entornos *sandbox* (cajas de arena) para la **experimentación segura** (Ramachandran, 2025). Esto permite a los usuarios innovar y luego, si el piloto demuestra valor, se inicia un proceso de cambio controlado donde TI profesionaliza la solución.

- **Riesgo Cognitivo:** La habilitación incluye abordar el **riesgo cognitivo** (Kos'myna, 2025), fortaleciendo el **criterio humano** y el **pensamiento crítico** para evitar la **aceptación pasiva** de las respuestas de la IA.

Gobierno de la IA: hacia un modelo centralizado de facilitación

La gestión de la **Shadow AI** es una elección cultural que define la **postura de riesgo** de la organización, como se observa en la tabla No.1.

El desafío es encontrar el nivel de gris que equilibre la necesidad de competir con la responsabilidad correspondiente.

La Shadow TI es catalogada como una fuente clave de Riesgo Emergente, según el Dominio 3 (ISACA CRISC, 2024) debido al Riesgo Fuera de Apertura y el Impacto Normativo. La mitigación se basa en la

Tabla 1

Postura de riesgo de la organización frente a la Shadow AI

Actitud	Riesgo asumido	Innovación	Resultado
Conservadora	Bajo	Bajo	Seguridad y control, pero rezago competitivo.
Arriesgada	Alto	Alto	Innovación y liderazgo, pero alta exposición a riesgos (regulatorios, éticos, operacionales).

Nota: Elaboración propia.

visibilidad y la aplicación de políticas, lo que requiere el uso de herramientas de control adecuadas, según el Dominio 4 (ISACA CRISC, 2024). Entre estas herramientas para gestionar el riesgo de la sombra se encuentran las soluciones de Prevención de Pérdida de Datos (DLP), los sistemas de Monitoreo de Eventos e Información de Seguridad (SIEM) y, fundamentalmente, las herramientas especializadas en entornos *cloud*.

- El CASB como Puerta de Enlace de Seguridad:

  Para lograr la visibilidad y el control necesarios sobre las aplicaciones en la sombra, las herramientas CASB (*Cloud Access Security Broker* o Agente de Seguridad de Acceso a la Nube) son esenciales (Gartner, 2025). Un CASB actúa como un punto de aplicación de políticas de seguridad situado entre los usuarios y los proveedores de servicios cloud. Su función principal es descubrir las aplicaciones no sancionadas (Shadow TI), monitorear el comportamiento de los usuarios, aplicar políticas de DLP y garantizar el cumplimiento normativo en tiempo real.

- El Riesgo de Desplazamiento y la Integración del Desarrollador como Facilitador: Este cambio cultural implica la redefinición de roles en TI. El desafío clave es sumar a los desarrolladores como facilitadores de soluciones seguras para que acompañen en la concienciación de los usuarios e incluso brinden su apoyo para que los usuarios logren mejores soluciones, justo cuando enfrentan la incertidumbre de cómo evolucionarán sus funciones en el contexto de la IA.

- Pruebas Rigurosas: La guía de ISACA Emerging Technology (2024), referente a la Ley de IA de la UE, enfatiza la necesidad de *testing*, documentación técnica y la creación de *sandboxes* regulatorios. Ahora bien, es el ISACA CRISC (2024), a través de su *Review Manual*, el que profundiza en los requisitos de control y aseguramiento que debe aplicar el profesional de riesgos. Dicho manual detalla la metodología para la validación de modelos críticos (incluyendo lotes de prueba y análisis de resultados) y se alinea con las directrices regulatorias aplicables a modelos de riesgo financiero.

- La Calidad Continua (Desarrollo Futuro): Para garantizar que la solución se mantenga confiable, segura y sin sesgos en el tiempo, es crucial considerar disciplinas de calidad continua. Este tema es amplio y estratégico, y podría ser objeto de un desarrollo en detalle en otra columna en el futuro.

La respuesta a la Shadow AI impulsa una transformación radical en el ecosistema de roles de TI. La

codificación rutinaria migra hacia la gestión de infraestructura de IA y la función crítica de arquitecto de *prompts*, exigiendo re-capacitación general para profesionalizar soluciones y dar soporte a los usuarios que explotarán las funciones y beneficios de AI. El factor humano se confirma como insustituible: el análisis de exposición laboral (el 'iceberg' de Chopra et al., 2025) muestra que el juicio experto, la ética y la supervisión crítica no son automatizables. Precisamente, el desafío fundamental del profesional de riesgos es actuar como facilitador seguro que equilibre los controles con el valor, según el Dominio 4 (ISACA CRISC, 2024). La IA no se protege a sí misma; es el talento humano quien, con criterio y visión, debe liderar su desarrollo seguro, calidad y cumplimiento continuo (Rajasekharan, 2025).

Referencias

Chopra, A., Bhattacharya, S., Salvador, D., Paul, A., Wright, T., Garg, A., Ahmad, F., Schwarze, A. C., Raskar, R., & Balaprakash, P. (2025). *The Iceberg Index: Measuring Workforce Exposure Across the AI Economy*. arXiv. https://arxiv.org/abs/2510.25137

European Spreadsheet Risks Interest Group (EUSPRIG). (s.f.). *Investigación sobre errores en hojas de cálculo y sus consecuencias.* https://eusprig.org/research-info/horror-stories/

Gartner. (2025). *Definition: Cloud Access Security Broker (CASB)*. https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

IBM. (s.f.). *What Is Shadow IT?* https://www.ibm.com/think/topics/shadow-it#:~:text=Shadow%20IT%20is%20any%20software,department's%20approval%2C%20knowledge%20or%20oversight

ISACA CRISC. (2024). *CRISC Review Manual* (7th ed.).

ISACA Emerging Technology. (2024). *Understanding the EU AI Act: Requirements and Next Steps*. https://www.compliancehub.wiki/content/files/2024/10/ISACA_Understanding_EU-AI-Act.pdf

Kos'myna, N. (2025). *Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task*. MIT Media Lab. https://www.media.mit.edu/publications/your-brain-on-chatgpt/

Moyle, E. (2023). *Digital Trust and Adopting Generative AI*. ISACA Journal, 5. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/digital-trust-and-adopting-generative-ai

Rajasekharan KR, CISM, CDPSE, PMP. (2025). *From Shadow IT to Shadow AI: Navigating the New Frontier of Enterprise Risk*. ISACA Newsletters, 19. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-19/from-shadow-it-to-shadow-ai-navigating-the-new-frontier-of-enterprise-risk

Ramachandran, R. (2025). *Safeguarding the Future: Strategies for Protecting Generative AI, LLMs, and Agentic AI*. ISACA.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/safeguarding-the-future-strategies-for-protecting-generative-ai-llms-and-agentic-ai

Reed, C., Wang, Y., & Dutta, A. (2010). *Achieving Data Warehouse Nirvana*. ISACA Journal, 4. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/archives/journal-volume-4-2010.pdf

Rodríguez, I., C.P. (Auditor y Consultor, Diplomado en Alta Gerencia de Seguros, Especialista en Dirección Financiera y Desarrollo Organizacional). (2019). *Las hojas de cálculo y los riesgos para el Auditor*. Auditool. https://www.auditool.org/blog/auditoria-externa/las-hojas-de-calculo-y-los-riesgos-para-el-auditor

Tsang, B., Ward, S., Zhang, L., & Storey, M. (2022). *Our Approach Managing Risk of End User Computing (EUC)*. KPMG International. https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2022/10/kpmg-euc-proposition-sep-2022.pdf

Héctor Calderazzi, CISA, CRISC, CISM
Profesional de Tecnología de la Información (TI) con más de 45 años de trayectoria, cuyo expertise se ha desarrollado principalmente en entidades financieras, especializándose en Seguridad de la Información, Auditoría de Sistemas y Gestión de Riesgos (GRC). Posee un Postgrado en Innovación Empresarial (UCEMA) y una Diplomatura en Gobernanza de Datos. Es un profesional certificado por ISACA con las credenciales CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control) y CISM (Certified Information Security Manager). En su experiencia, lideró la seguridad y la gestión de riesgos en el sector financiero, destacando su participación en fusiones institucionales y proyectos estratégicos de alta complejidad. Actualmente, combina la consultoría senior en Gobierno de TI, Gestión de Riesgos y Seguridad de la Información con su rol de Mentor ISACA para capítulos a nivel global y Docente en diversas entidades académicas. Es vicepresidente de ISACA Buenos Aires Chapter.