No. 176 Julio - Septiembre DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tecnologías emergentes y disruptivas a 2030

Oportunidades y retos para Colombia

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

CURSOS ONLINE

Nos enfocamos en que tu aprendizaje
sea accesible y efectivo.

GERENCIA DE PROYECTOS

INTELIGENCIA ARTIFICIAL

MEJORES PRÁCTICAS

INGENIERÍA DE SOFTWARE

SEGURIDAD INFORMÁTICA

PLATAFORMAS

¡ Mejora tus habilidades !

www.acis.org.co
3015530540 - 3043463413
cursos@acis.org.co

ACIS

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Julio - Septiembre 2025
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

CONECTA CON NOSOTROS

@Comunidadacis

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

www.acis.org.co

Tecnologías emergentes y disruptivas a 2030 - Oportunidades y retos para Colombia

DOI: 10.29236/sistemas.n176a1

Emir Hernando Pernet Carrillo

Maria Mercedes Corral Strassmann

En esta edición se exploran diferentes tecnologías emergentes y disruptivas con mayor potencial de aplicación y desarrollo hacia el año 2030. A través de la entrevista, la investigación, el foro y el articulo se busca evidenciar las oportunidades, expectativas y riesgos que deben ser objeto de análisis y valoración por parte de las empresas, la

academia y el gobierno, con el ánimo de evaluar la viabilidad de su adopción en Colombia. De igual forma, la información y los elementos críticos expuestos pueden ayudar a establecer las condiciones que éstas pueden considerar para el logro de sus objetivos empresariales y el beneficio de sus grupos de interés.

La entrevista en esta edición es con Félix Rodríguez, vicepresidente adjunto de riesgos no financieros y control interno en el Banco Promerica de República Dominicana. Félix nos comparte su perspectiva de las nuevas tecnologías desde el punto de vista de la gestión de riesgos, auditoría y gobierno. Adicionalmente, identifica las tecnologías que para él son las más relevantes y aplicables en nuestro contexto nacional, señalando los retos y limitaciones que se pueden presentar en su implementación, y los tres puntos principales en los que las organizaciones no se deben equivocar en la selección y despliegue de nuevas tecnologías, para no poner en riesgo el cumplimiento de la promesa de valor a sus clientes.

La investigación se basa en la publicación de la IEEE, Predicciones Tecnológicas 2025, enfocándose, en primer lugar, en las tres tecnologías más maduras a la fecha y con mayor perspectiva de adopción a 2030, adicionalmente, en las tres tecnologías con mayor impacto en la sostenibilidad. Además de presentar los retos y las oportunidades para las seis tecnologías, se extraen las recomendaciones más relevantes de la IEEE para los sectores de la industria, el gobierno, la academia, las organizaciones profesionales, los usuarios finales, los desarrolladores, los CxO, y los inversionistas.

En el espacio tradicional del foro para la sección Cara y Sello, se contó con la participación especial de la Ingeniera Sandra Lascarro Mercado, reconocida conferencista sobre tendencias tecnológicas y gestión de la información. Dentro del foro se debatieron temas como el dilema entre las ventajas competitivas o los riesgos que conllevan la adopción de tecnologías disruptivas, la aplicabilidad de dichas tecnologías dentro del contexto local, los criterios de selección, diseño e implementación que deben considerarse con las nuevas tecnologías, la preparación requerida por los gestores del riesgo que deben tomar decisiones sobre las mismas, y los aspectos culturales y humanos para tener en cuenta.

Finaliza esta edición con el artículo del Ingeniero Jeimy José Cano PhD, director de la revista Sistemas, y experto en Seguridad, en el cual plantea la necesidad de actualizar las estrategias de ciberseguridad en las organizaciones, con base en una mayor comprensión y aprovechamiento de las inestabilidades y los inciertos en favor del logro de sus objetivos estratégicos. En su artículo, el Doctor Cano pre-

senta nuevas soluciones estratégicas que se alejan un poco de las tradicionales, mediante la implementación de procesos de aprendizaje y de evolución, haciendo más dinámicos y vigilantes los mecanismos de defensa cibernéticos.

El mensaje que deseamos transmitir a las organizaciones, la academia y el gobierno, es la importancia de contar con una visión prospectiva de las tecnologías emergentes y disruptivas, ya que dicha visión ayuda a orientar la toma de decisiones, aportando la identificación temprana de riesgos y oportunidades, y una adecuada gestión de ventajas competitivas y de estrategias de defensa.

***Emir Hernando Pernet Carrillo**, DBA. Asesor en Negocios de Tecnología. Ingeniero de Sistemas y Computación de la Universidad de los Andes, Colombia, y MBA de ese mismo centro educativo. Master of Computer Science de Arizona State University, USA. Doctor of Business Administration de Newport University, USA. Experiencia de más de 20 años como Asesor de Soluciones Tecnológicas del Departamento de Sistemas de Información del Banco de la República, y Subdirector de Computación Corporativa del Departamento de Tecnología Informática del Banco de la República.*

***Maria Mercedes Corral Strassmann**, PhD. Ingeniero de Sistemas y Computación de la Universidad de Los Andes; Maestría en Comunicación de datos, University College London de la Universidad de Londres; Programa de Desarrollo Directivo - PDD de Inalde; y Doctorado de Comunicación, Lenguajes e Información en la Universidad Javeriana. Experiencia, como director de Proyectos en el Banco de la República; Gerente de TI de CIFIN - Asobancaria; vicepresidente de Tecnología de Deceval. Experiencia de más de 20 años como Profesor Universitario en áreas de Ingeniería de software, y Gerencia de proyectos, Maestría y Especialización de Ingeniería de Sistemas en la Universidad Javeriana.*

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

¡AFILIATE YA!

Y DISFRUTA DE ESTOS BENEFICIOS

- Actualización en formación profesional y académica de manera constante.
- Candidatura a participación profesional en proyectos de ACIS.
- Candidato a Director o CoDirector de Grupo de Interés (GI).
- Candidatura a participar en consultorías solicitadas a ACIS por el sector privado y público.
- Candidatura a participar en eventos nacionales o internacionales como delegado de ACIS.
- Candidato a Miembro de Consejo Editorial de la Revista Sistemas.
- Descuentos especiales en cursos y eventos exclusivos en el área de las TIC.
- Referencia profesional para vinculación como Perito en procesos de arbitraje.
- Referencia para participación en Juntas Directivas.
- Inclusión en el gremio de Ingenieros de Sistemas más importante del país.
- Recepción trimestral de la revista SISTEMAS en formato digital.
- Acceso diferido a la base de Webinars de ACIS.
- Acceso exclusivo a oportunidades laborales a través de nuestro portal de empleo.
- Participación como conferencista o participante en las charlas semanales.
- Correo personal con @acis.org.co
- Asista a las funciones del Teatro Nacional con un 20% de descuento. Consulte la Programación y solicite el descuento a cursos@acis.org.co.
- 30% de descuento en los libros de la Casa Editorial ALFAOMEGA, consulte el Catálogo

Afiliación General

Afiliación + Precio de estudio de formulario

$ 323.400 + $ 60.000

Afiliación para recién egresados

Descuento de 20% para recién egresados, (2 años) + Precio de estudio de formulario

$ 258.800 + $ 60.000

301 5530540 suscripciones@acis.org.co www.acis.org.co

Tecnologías disruptivas y emergentes

Félix Rodríguez, experto en gestión de riesgos, auditoría y gobierno, entre otros asuntos, se pronunció al respecto.

DOI: 10.29236/sistemas.n176a2

Con más de quince años de experiencia en sectores financieros y tecnológicos, nuestro entrevistado, Félix Rodríguez, dio respuesta a cada una de las inquietudes formuladas, advirtiendo: “Las respuestas aquí ofrecidas reflejan exclusivamente mi experiencia y criterio profesional, y no representan necesariamente la posición institucional ni oficial de la organización en la que actualmente laboro”.

Revista Sistemas: *Considerando las diferentes tecnologías disruptivas y emergentes disponibles a la fecha, ¿cuáles serían en su opinión las más relevantes para su aplicación en el país y por qué?*

Félix Rodríguez: En mi opinión, las tecnologías que de manera general tienen, y continuarán teniendo, un relevante impacto son la Inteligencia Artificial y la analítica avanzada.

Esto se alinea a mi pensar que estas tecnologías se han venido desarrollando para apoyar de manera directa a la transformación integral, principalmente para sectores clave como salud, educación, agroindustria y la banca. Dentro de estas también destaco la computación en la nube y el edge computing, que democratizan el acceso a infraestructura digital y aceleran la transformación, principalmente para las PYMES.

Adicionalmente, no puedo dejar de mencionar la conectividad 5G y el blockchain, los cuales representan una oportunidad para mejorar la agilidad, transparencia y la confianza, especialmente en trazabilidad y servicios financieros inclusivos.

RS: *En su práctica empresarial, ¿qué retos y limitaciones ha observado para la implementación ágil y detallada de las tecnologías emergentes y disruptivas que se han seleccionado?*

FR: He identificado dos grandes retos que, con los años, he tenido la oportunidad de observar y gestionar; El primero es la escasez de talento especializado en áreas clave como inteligencia artificial, ciberseguridad y ciencia de datos, temas que cada día cobran mayor relevancia para la sostenibilidad y competitividad de las organizaciones.

El segundo gran desafío es la resistencia cultural al cambio. Muchas organizaciones todavía operan con estructuras rígidas y tradicionales, y esto no se debe únicamente a limitaciones financieras, sino más bien a la forma en que los profesionales de tecnología, seguridad y gestión de riesgos comunicamos el valor y la relevancia de estas disciplinas. Cuando no logramos transmitir con claridad su impacto estratégico, la adopción se ralentiza.

Adicionalmente, enfrentamos grandes retos regulatorios significativos. A pesar de los esfuerzos que realizan los entes reguladores y gubernamentales por mantenerse alineados y generar marcos de supervisión aplicables a estos tiempos, no siempre pueden avanzar al mismo ritmo que la innovación. A todo esto, se suma la capacidad de inversión desigual, que deja a muchas empresas en desventaja, especialmente las medianas y pequeñas.

Finalmente, considero fundamental el reto de la madurez en la gobernanza de datos, donde son pocas las organizaciones que han desarrollado enfoque o metodologías claras, así como sus estructuras dedicadas a gestionar los datos como un activo estratégico para la generación de valor integral.

RS: *¿En qué no se pueden equivocar las empresas en Colombia para seleccionar y desplegar tecnologías disruptivas y emergentes de cara a la promesa de valor para sus clientes?*

FR: Desde mi óptica y experiencia, las empresas no pueden equivocarse en tres aspectos clave. 1) la innovación debe centrarse en el cliente: la tecnología no es un fin en sí mismo, sino un medio para generar valor, confianza y experiencias diferenciadas, 2) no se puede pasar por alto el cumplimiento, principalmente la ética y la confianza digital, porque un mal manejo del marco regulatorio aplicable, así como la privacidad y la transparencia puede destruir la reputación de la empresa, y 3) se deben garantizar la alineación estratégica: no se trata de adoptar tecnologías por capricho o moda, sino de poder integrarlas a los objetivos de negocio y su propuesta de valor.

RS: *¿Cómo ha sido su relación con el área de auditoría y ciberseguridad al diseñar e implementar iniciativas digitales con tecnologías emergentes y disruptivas? ¿Buscan acompañar y comprender los retos? ¿Son reacios a dichas innovaciones? ¿Comparten el reto y buscan opciones?*

FR: En mi más de catorce años de recorrido profesional, he vivido diversas experiencias, donde en los casos donde se genera el mayor éxito es cuando la función de auditoría interna, ciberseguridad y gestión de riesgos se convierten en aliados estratégicos, donde desde sus funciones participando desde el inicio para garantizar que la innovación se despliegue de manera segura y en cumplimiento con las regulaciones.

Pero no siempre pasa de esta forma, en otras experiencias la historia es otra, donde he percibido cierta resistencia inicial, motivada por temores a vulnerabilidades o por desconocimiento del potencial de las tecnologías. Pero en general, cuando logramos establecer un diálogo constructivo, y como siempre digo "*una conversación basada en una cultura en gestión de riesgos*", ambas áreas entienden que su rol no es frenar la innovación, sino asegurar que ésta sea sostenible, confiable y segura para todos los actores involucrados

RS: *¿Cómo deberían definir las organizaciones su apetito de riesgo*

digital para balancear la promesa de valor, los retos empresariales y las iniciativas digitales?

En las organizaciones siempre es importante gestionar los riesgos basado en una declaración formal del apetito de riesgo, sobre todo bajo el enfoque digital.

Para esto se puede sugerir partir de tres importantes aspectos: 1) la promesa de valor al cliente: si una innovación genera confianza y diferenciación, vale la pena asumir un mayor nivel de riesgo. 2) la capacidad interna de gestión, es decir, nuestra madurez en la combinación para la gestión de riesgos, ciberseguridad, continuidad de negocio, talento y gobernanza. Y 3) la sostenibilidad empresarial, buscando un equilibrio entre la estabilidad actual y la competitividad futura.

En resumen, y sin intención de decir algún nunca dicho o pensado; se trata de asumir riesgos calculados y conscientes, con marcos de control, estrategias de mitigación y una gobernanza digital sólida.

Predicciones Tecnológicas IEEE 2025

DOI: 10.29236/sistemas.n176a3

Emir Hernando Pernet Carrillo

Maria Mercedes Corral Strassmann

Resumen

Con base en las predicciones tecnológicas del 2025 presentadas por la IEEE (IEEE Computer Society, 2025), este articulo explora las nuevas tecnologías con un horizonte de adopción comercial de los próximos cinco años. Para cada tecnología se presenta una descripción básica y las predicciones correspondientes. Posteriormente se realiza un análisis más detallado de las tres tecnologías que registran las mejores evaluaciones en cuanto al Éxito de la Tecnología en 2025, el Grado de Adopción en el Mercado, y el Grado de Madurez, identificando sus problemas/demandas, oportunidades e impactos. Para las tres tecnologías con mayor impacto en sostenibilidad se identifican sus oportunidades de negocio, habilitadores e inhibidores. Para las seis tecnologías (tres mejor evaluadas, y tres con mayor impacto en sostenibilidad) se exponen las recomendaciones más relevantes de la IEEE dirigidas a diferentes sectores como la industria, el gobierno, la academia, las organizaciones profesionales, los usuarios finales, los desarrolladores, los CxO, y los inversionistas.

Palabras clave

IEEE, Predicciones Tecnológicas, Horizonte de Adopción Comercial, Sostenibilidad, Inteligencia Artificial, Automatización, LLM Development, Drone Adoption, AI Agents, IT Energy Convergency, Smart AG, Sustainable Computing.

Introducción

Para el año 2025, la IEEE presentó un documento con las predicciones tecnológicas del 2025 (IEEE Computer Society, 2025). Las tecnologías tratadas en dicho documento tienen un horizonte de adopción comercial que está entre los próximos 2.54 y 9,60 años. La IEEE conformó un equipo de Predicciones Tecnológicas integrado por 54 miembros de 17 países que cubren todos los continentes. De América participaron 1 de Brasil, 1 de Uruguay, 2 de Canadá y 32 de los Estados Unidos. La distribución por género fue de 15 mujeres y 39 hombres. En cuanto a los sectores a los que pertenecen los 53 miembros, 23 son de la Academia, 25 de la Industria, 5 del Gobierno y 1 de Organizaciones Profesionales. Con referencia a las áreas de tecnología con mayor representación dentro del Equipo se encuentran Information Technology, Wearables, Artificial Intelligence, Data Management, Knowledge Management, Edge Computing, y Autonomous Vehicles.

Predicciones

En términos generales sus predicciones fueron las siguientes:

• Crecimiento acelerado en muchas facetas de la IA, lo que requiere la recapacitación de la fuerza laboral.

• Disminución del interés en la sostenibilidad, centrada en EE. UU., debido a las nuevas presiones económicas y sociopolíticas (aunque no a nivel mundial).

• Automatización cada vez mayor en muchas dimensiones, lo que sienta las bases para nuevas oportunidades de IA.

• Rápido desarrollo de la biotecnología, aunque discreto (p. ej., "descubrimiento de fármacos asistido por IA", "diagnóstico médico basado en IA").

Metodologia

Identificación de predicciones

Cada miembro del equipo podía plantear hasta 2 predicciones. En total se presentaron 88 predicciones iniciales.

Se realizó un proceso de preselección donde cada autor podía votar por 16 tecnologías. Después de esta votación, el número se redujo a 22 predicciones. Posteriormente se hizo una cuidadosa integración de algunas predicciones.

Evaluación

Se le asignó una calificación a cada tecnología, dependiendo de varios criterios, los cuales se detallan a continuación.

- Calificación de A+ a F- para los criterios
  - Éxito de la tecnología en 2025
  - Impacto en la Humanidad
  - Predicción del grado de adopción en el mercado en 2025
- Calificación del Grado de Madurez [Muy temprana, Prototipo,

Incubación, Emergente, Maduro, Comercialización] para el criterio de Madurez.
- Calificación del tiempo de adopción [1 año, 3 años, 5 años, 10 años, 15 años} para el criterio de Horizonte de Adopción Comercial.

Calificación

Para cada tecnología se identificaron sus problemas/demandas, oportunidades, impactos, soluciones sostenibles, y oportunidades de negocio.

Análisis de la información

Para el análisis de la información se consideraron los criterios de evaluación:

- Horizonte de Adopción Comercial
- Éxito de la Tecnología en 2025
- Grado de Adopción en el Mercado
- Grado de Madurez
- Impacto en la Humanidad

Considerando que en esta Edición de la Revista SISTEMAS se busca identificar las tecnologías emergentes a 2030, de las 22 tecnologías tratadas en la publicación de la IEEE, se centró el análisis en aquellas 17 cuyo horizonte de adopción comercial es anterior al año 2031. A continuación, se presenta la lista de estas tecnologías ordenadas de forma ascendente por el criterio del Horizonte de Adopción Comercial.

Descripciones y Predicciones de las Tecnologías.

LLM Development

Descripción:

LLM o modelos de lenguaje de gran tamaño, son modelos muy grandes de aprendizaje profundo pre-entrenados con grandes cantidades de datos. El transformador

Tecnologia	Horizonte de Adopcion Comercial (Años)	Éxito de la Tecnologia en 2025	Grado de Adopcion en el Mercado	Grado de Madurez	Impacto en la Humanidad
LLM Development	2,54	A-	A/B	B	A/B
Drone Adoption	2,83	A/B	B+	B	A/B
AI Agents	3,15	A/B	B+	B-	A/B
Mis/Disinformation	3,69	B	B	B/C	B
Wereables/biomarkers	3,75	B+	B	B-	B+
Augmented AI	4,06	B+	B	B/C	B+
AI-Enhanced Robotics	4,25	B+	B-	B-	B+
Next-gen Cyberwarfare	4,58	B-	B-	B/C	B-
Funct Safety / Autonomous Vehicles	4,73	B	B	B/C	B
AI – Based Medical Diagnosis	4,75	B	B-	B/C	B
Smart Ag	4,77	B+	B-	B/C	B+
Tools and Policies for AI Regulation	4,79	B/C	B/C	C+	B/C
Autonomous Driving	4,83	B+	B	B-	B+
Data Feudalism	4,9	B-	B-	C+	B-
IT/Energy Convergence	5,06	B+	B-	C+	B+
AI Assisted Drug Discovery	5,21	B	B-	B/C	A
Sustainable Computing	5,6	B	B-	C+	A/B

Tabla 1- Tecnologías Emergentes 2030.
Fuente: (IEEE Computer Society, 2025)

subyacente es un conjunto de redes neuronales que consta de un codificador y un decodificador con capacidades de autoatención. El codificador y el decodificador extraen significados de una secuencia de texto y comprenden las relaciones entre las palabras y las frases que contiene (Amazon, 2025).

Predicción:
Veremos implementaciones de nuevos tipos de modelos de lenguaje, como modelos de lenguaje pequeños y modelos exóticos para propósitos especiales.

Drone Adoption
Descripción:
Un vehículo aéreo no tripulado, comúnmente conocido como dron, es un vehículo sin tripulación, capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido(Ferrovial, 2025).

Predicción:
Drone-as-a-Service (DaaS) redefinirá la logística, la agricultura y la respuesta ante desastres, ofreciendo soluciones confiables, de bajo costo y rápidas respuestas en diversas industrias.

AI Agents
Descripción:
Un AI Agent o agente de inteligencia artificial se refiere a un sistema o programa que es capaz de realizar tareas de forma autónoma en nombre de un usuario o de otro sistema mediante el diseño de su flujo de trabajo y el uso de las herramientas disponibles(IBM, 2025).

Predicción:
Los agentes de IA que combinan LLM, modelos de aprendizaje automático (ML) y sistemas basados en reglas proporcionarán soluciones autónomas y altamente especializadas para operaciones financieras, de fabricación y venta minorista.

Wereables/Biomarkers
Descripción:
Las tecnologías de sensores portátiles son cada vez más relevantes en la investigación sanitaria, especialmente en el contexto del manejo de enfermedades crónicas. Generan datos de salud en tiempo real que pueden traducirse en biomarcadores digitales, que pueden proporcionar información sobre nuestra salud y bienestar(NPJ, 2025).

Predicción:
Los wearables rastrearán biomarcadores para la detección temprana de enfermedades y el bienestar proactivo, expandiéndose más allá del seguimiento del estado físico al monitoreo de grado médico para enfermedades crónicas.

Augmented AI
Descripción:
La Inteligencia Artificial Aumentada se refiere a la integración de la inteligencia y las capacidades humanas con tecnologías de inteligencia artificial (IA) para mejorar la toma de decisiones, la resolución de pro-

blemas y la productividad. Se centra en el uso de la IA para complementar y potenciar las capacidades humanas, en lugar de sustituirlas por completo(Subex, 2025).

Predicción:
La IA aumentada redefinirá la colaboración entre humanos y máquinas, combinando la precisión de las máquinas con la supervisión humana para lograr soluciones inclusivas y éticas en los ámbitos de la atención médica, las finanzas y la educación.

AI-Enhanced Robotics
Descripción:
La robótica mejorada con IA está transformando la fabricación y el almacenamiento, gracias a una combinación de tecnologías de vanguardia. Estas tecnologías permiten a los robots operar de forma autónoma, adaptarse a entornos cambiantes y colaborar fluidamente con los trabajadores humanos (Profile Tree, 2025).

Predicción:
La inteligencia incorporada permitirá a los robots percibir, aprender y colaborar en entornos dinámicos, logrando una autonomía sin precedentes y una adaptabilidad similar a la humana.

Smart Ag
Descripción:
"Smart Ag" se refiere a la agricultura inteligente, un enfoque de la agricultura que utiliza tecnologías avanzadas y datos para optimizar la producción y la sostenibilidad. Implica la aplicación de sistemas informáticos y electrónicos para la toma de decisiones, el control y la automatización de las operaciones agrícolas(IBM, 2025).

Predicción:
Los sistemas impulsados por IA mejorarán el rendimiento de los cultivos, la gestión de los recursos y la sostenibilidad, abordando la seguridad alimentaria mediante el monitoreo del suelo y el clima en tiempo real.

Autonomous Driving
Descripción:
La conducción autónoma, también conocida como conducción automatizada o vehículo autónomo, se refiere a la capacidad de un vehículo para conducirse a sí mismo sin la intervención humana. Utiliza una combinación de sensores, inteligencia artificial y sistemas de navegación para percibir su entorno, tomar decisiones y controlar sus movimientos(MD, 2025).

Predicción:
Los vehículos autónomos reducirán las emisiones, mejorarán la seguridad y transformarán la logística urbana, pero su adopción generalizada depende de las aprobaciones regulatorias y la confianza pública.

IT/Energy Convergence
Descripción:
La convergencia IT/energía, también conocida como convergencia

IT/OT (Tecnología de la Información/ Tecnología Operacional) en el contexto energético, se refiere a la integración de los sistemas informáticos (IT) con los sistemas de tecnología operativa (OT) dentro del sector energético. En esencia, implica la conexión y el análisis de datos de dispositivos OT (como sensores, medidores inteligentes, sistemas de control) a través de sistemas IT (como software de análisis, planificación de recursos empresariales, gestión de relaciones con clientes) (Energy Sustainability Directory, 2025).

Predicción:
La transformación digital de la energía reflejará la evolución de la TI, permitiendo redes sustentables, integración de energías renovables y un crecimiento exponencial de la IA para un suministro eficiente de energía.

Mis/Disinformation
Descripción:
Los sistemas avanzados de IA pueden analizar patrones, uso del lenguaje y contexto para ayudar en la moderación de contenidos, comprobar si las noticias son falsas y detectar información errónea y desinformación (World Economic Forum, 2025).

Predicción:
Las herramientas de IA detectarán y mitigarán la desinformación, contrarrestando su rápida difusión en las redes sociales para proteger la opinión pública y la confianza.

Funct Safety / Autonomous Vehicles
Descripción:
La seguridad funcional en vehículos autónomos (FA) se refiere a la capacidad del vehículo para operar de manera segura, incluso ante fallos en sus sistemas electrónicos y eléctricos. Se centra en prevenir o mitigar situaciones peligrosas que puedan surgir debido a errores en el funcionamiento de estos sistemas, garantizando la seguridad tanto de los ocupantes como de otros usuarios de la vía (Synopsys, 2025).

Predicción:
Los marcos de seguridad avanzados garantizarán que los vehículos autónomos funcionen de forma confiable en los sectores público y comercial, ganando confianza para una adopción más amplia.

AI – Based Medical Diagnosis
Descripción:
Mediante sistemas de diagnóstico médico con IA, los profesionales sanitarios podrán desarrollar tratamientos personalizados basados en grandes cantidades de datos de pacientes. Estas herramientas pueden identificar patrones entre pacientes y extraer conclusiones sobre el tratamiento más adecuado para cada persona (NIX, 2025).

Predicción:
La IA mejorará la precisión diagnóstica, particularmente en radiología y patología, mejorando los resultados de los pacientes y redu-

ciendo la carga de trabajo de los médicos.

Next-gen Cyberwarfare

Descripción:

La ciberguerra es una serie de ataques cibernéticos estratégicos contra un estado-nación, lo que causa un daño significativo. Este daño podría incluir la interrupción de los sistemas informáticos vitales hasta la pérdida de vidas. La ciberguerra generalmente se define como un conjunto de acciones por parte de una nación u organización para atacar los sistemas de red informáticos de países o instituciones con la intención de interrumpir, dañar o destruir la infraestructura por virus informáticos o ataques de denegación de servicio. Y la esperanza es que las herramientas efectivas de inteligencia frente a ciber amenazas puedan reducir los daños causados por estos ataques (Fortinet, 2025).

Predicción:

Las ciberdefensas basadas en IA contrarrestarán las amenazas en constante evolución. Los desafíos incluyen la colaboración internacional, la velocidad de respuesta y la defensa contra ataques cada vez más potenciados por la IA.

Data Feudalism

Descripción:

El "feudalismo de datos" o "feudalismo digital" es un concepto que describe la situación en la que las grandes empresas tecnológicas, como Google, Amazon o Meta, tienen un control significativo sobre los datos y, por lo tanto, sobre las personas y las sociedades en la era digital. Es similar al feudalismo histórico, donde los señores feudales poseían la tierra y tenían poder sobre los siervos, pero en este caso, las plataformas digitales poseen los datos y ejercen influencia sobre los usuarios (Medium, 2025).

Predicción:

Nuevas herramientas permitirán a los usuarios recuperar el control sobre sus datos. Los desafíos incluyen garantizar un acceso equitativo y armonizar los marcos regulatorios globales.

Tools and Policies for AI Regulation

Descripción:

La gobernanza de la inteligencia artificial (IA) se refiere a los procesos, estándares y medidas de seguridad que ayudan a garantizar la seguridad y la ética de los sistemas y herramientas de IA. Los marcos de gobernanza de la IA orientan la investigación, el desarrollo y la aplicación de la IA para garantizar la seguridad, la equidad y el respeto de los derechos humanos (IBM, 2025).

Predicción:

Surgirán marcos para la ética y la gobernanza de la IA. Los desafíos incluyen la armonización de estándares globales y la garantía de mecanismos de aplicación eficaces.

AI-Assisted Drug Discovery
Descripción:
Las técnicas de IA, en particular el aprendizaje automático y el aprendizaje profundo, han revolucionado el descubrimiento de fármacos mediante el análisis de grandes conjuntos de datos, la predicción de propiedades moleculares y la identificación de posibles fármacos candidatos. Los algoritmos de IA pueden realizar un cribado virtual de bibliotecas de compuestos para identificar las moléculas con mayor probabilidad de unirse a dianas específicas, lo que reduce el tiempo y el coste del cribado experimental. Los modelos de IA pueden predecir las propiedades farmacocinéticas y farmacodinámicas de los compuestos, lo que ayuda a los investigadores a priorizar los candidatos más prometedores para su posterior desarrollo(NIH, 2025).

Predicción:
Los avances en IA acelerarán el descubrimiento de fármacos, identificando nuevos compuestos y tratamientos, aunque persisten obstáculos regulatorios y relacionados con la calidad de los datos.

Sustainable Computing
Descripción:
La computación sostenible implica diseñar, desarrollar, usar y desechar sistemas informáticos de forma respetuosa con el medio ambiente. Esto incluye el uso de hardware y software energéticamente eficientes, la reducción de residuos electrónicos y la reducción de las emisiones de carbono. También promueve soluciones tecnológicas para el clima para los usuarios finales mediante el uso de computación acelerada e IA(Nvidia, 2025).

Predicción:
Los centros de datos adoptarán hardware energéticamente eficiente, gestión inteligente de recursos y energía renovable, aunque ampliar las prácticas de sostenibilidad sigue siendo un desafío.

Tecnologías Mejor Evaluadas
Las tres tecnologías que tienen un horizonte de adopción más cercano y mejores evaluaciones en tres de los otros cuatro criterios (Éxito de la Tecnología en 2025, Grado de Adopción en el Mercado, y Grado de Madurez) son: LLM Development, Drone Adoption, y AI Agents.

A continuación, para estas tecnologías se presenta un análisis de los Problemas/Demandas, Oportunidades, e Impactos identificados por la IEEE.

LLM Development
Problemas/Demandas
Parte de los problemas de esta nueva tecnología están relacionados con temas de sostenibilidad. Solamente algunas pocas iniciativas toman en consideración la sostenibilidad en TI, con un poco entendimiento de como medirla.

Otros problemas tienen que ver con el uso eficiente de la energía, en particular con el uso apropiado de

los recursos computacionales lo que genera un alto consumo de energía; la falta de herramientas y técnicas para la computación sensible al carbono; y la generación de basura electrónica. También se presentan dificultades en la preservación de privacidad por parte de algunos modelos LLM.

Oportunidades
Los LLM permiten generar Small Language Models (SLM) más efectivos, los cuales en sus versiones Open Source generan oportunidades para afinar modelos y utilizarlos con propósitos específicos.

Adicionalmente, los LLM ayudan a argumentar análisis y detecciones, a resolver problemas computacionales a partir de descripciones de texto, y a generar recomendaciones. Los problemas de privacidad mencionados en el aparte anterior pueden ser tratados mediante modelos personalizados.

Impactos
El aumento en la disponibilidad de los LLM está creando mayores oportunidades para la implementación de ideas innovadoras y casos de uso específicos, para el desarrollo de agentes de IA, para la detección de alucinaciones mediante la validación cruzada de modelos, para la protección de datos, y para la validación de la verdad. Sin embargo, las nuevas generaciones pueden perder sus habilidades, y también se puede perder creatividad en nuevos contenidos, principalmente si estos se generan a partir de otros modelos.

Drone Adoption
Problemas/Demandas
Se ha generado un aumento en la demanda de soluciones apalancadas en drones para campos como la Agro-Tecnología (Gestión de cultivos, monitoreo de ganado, aplicación de fertilizantes y pesticidas, captura de datos sobre la salud de los cultivos, nivel de nutrientes y necesidades de riego, y apoyo al conformado de precisión), la extinción de incendios (monitoreo en tiempo real, mapeo del perímetro del incendio, y la identificación de puntos críticos), las aplicaciones cartográficas, de planeación urbana, de detección de artefactos explosivos y de estudios ambientales de precisión, las aplicaciones de entretenimiento, cinematográficas y estratégicas, y las entregas asistidas por drones en zonas urbanas y rurales.

En cuanto a los retos se encuentran obstáculos regulatorios, preocupaciones éticas y de privacidad, duración limitada de la batería y autonomía de vuelo.

Oportunidades
Esta tecnología ofrece oportunidades para el desarrollo de robots colaborativos avanzados (Cobots) con funciones mejoradas de percepción y seguridad para diversas aplicaciones industriales, innovaciones en robótica sanitaria para cirugía, rehabilitación y asistencia en

el cuidado personal, incremento de la productividad y seguridad en entornos peligrosos, integración en ciudades inteligentes para una mejor gestión de infraestructuras, y el uso potencial de la robótica de consumo en la educación, el hogar y el entretenimiento.

Impactos
El uso de esta tecnología se puede ver reflejado en una reducción significativa de lesiones y errores laborales, en una mejora de la calidad de vida mediante cuidados asistenciales y rehabilitación, en ahorro en los costos y aumento en la eficiencia operativa en todos los sectores, en una aceleración de la sinergia entre humanos e IA en el lugar de trabajo y el hogar, y en una mejora de la respuesta ante desastres y la mitigación de riesgos.

AI Agents
Problemas/Demandas
Los AI Agents encuentran una mayor demanda en la ejecución de tareas repetitivas que requieren un bajo nivel de conocimientos especializados y/o creatividad, en el uso por parte de pequeñas empresas que requieren expandirse pero que no pueden contratar personal calificado para realizar tareas específicas, en usuarios que requieren interactuar con agentes que entiendan su lenguaje humano preferido, incluyendo expresiones flexibles o informales, y en soluciones que requieren obtener información relevante basada en un contexto o tema determinado.

Oportunidades
Los AI Agents permitirán la realización de tareas complejas con una mínima intervención humana, a partir de una descripción de dichas tareas. De igual forma, estos agentes aumentaran la eficiencia laboral ya que realizaran las mismas tareas que un humano, pero en menor tiempo y con menos errores. Pequeñas empresas podrán crecer sin necesidad de contratar trabajadores mejores calificados. Las nuevas oportunidades laborales se centrarán alrededor del desarrollo y mantenimiento de AI Agents. Los IA Agents podrán desarrollar su propia lógica de acuerdo con sus necesidades. Estos agentes se convertirán en aliados e impulsores del desarrollo de actividades sostenibles. Se podrán desarrollar AI Agents que se desempeñen como tutores que ayuden al desarrollo de una educación más accesible y personalizada.

Impactos
El mayor impacto de los AI Agents se reflejará en la evolución de los empleos, en la medida en que los agentes asuman tareas especializadas, se crearán oportunidades para nuevos roles, como también la necesidad de mejorar algunas habilidades, y se requerirá mayor capacitación para los trabajadores sobre cómo colaborar con AI Agents. En cuanto a las pequeñas empresas, estas podrán escalar más rápido con la implementación de AI Agents, con una baja inversión en mano de obra.

Tecnologías Sostenibles
Dentro de las tecnologías innovadoras con un horizonte de adopción comercial anterior al año 2031, se identificaron tres, con un mejor impacto en sostenibilidad: IT Energy Convergency, Smart AG, y Sustainable Computing.

A continuación, para estas tecnologías se presenta un análisis de sus Soluciones Sostenibles / Oportunidades de Negocio, Habilitadores e Inhibidores identificados por la IEEE.

IT Energy Convergency
Un tema para tener en cuenta desde la sostenibilidad y las tecnologías será la transformación de la energía la cual impactará posteriormente en la evolución de estas, lo anterior llevará a contar con redes sustentables, y con energías renovables que permitirán un potencial crecimiento de la IA, el cual se verá tangible en el suministro eficiente de la energía.

Soluciones sostenibles / Oportunidad de negocio
Algunas soluciones que se pueden vislumbrar para esta tecnología son: la energía nuclear y la posibilidad de generar energía cerca al consumo, así mismo la energía gestionada con ayuda de la IA habilitaría el aprendizaje por refuerzo multiobjetivo.

Habilitadores / Inhibidores
Existen algunos habilitadores de las anteriores soluciones, entre estos se presentan, por ejemplo, los recursos distribuidos, la gestión moderna de la oferta y demanda de la energía, como también la cadena de suministro que integra componentes físicos con sistemas informáticos, y adicionalmente el mejoramiento de la seguridad de los recursos energéticos distribuidos. Y como inhibidores están los cumplimientos normativos y regulatorios, la fragmentación que existe en el mundo en cuanto a la energía producida y la requerida por Internet, y el mejoramiento de la seguridad y protección en las áreas expuestas a ataques.

Smart AG
Los sistemas inteligentes de agricultura impulsados por IA permitirán el mejoramiento y rendimiento de los cultivos, y ayudarán a la gestión de los recursos y la sostenibilidad, sin olvidar la importancia de la seguridad alimentaria y el monitoreo del suelo y clima en tiempo real.

Soluciones sostenibles / Oportunidad de negocio
Desde las tecnologías Smart AG, se plantean soluciones como la existencia de estándares para un pasaporte alimentario digital y global que permita el seguimiento de la cadena de aprovisionamiento, así como sistemas de gestión de inventarios con la utilización de IoT en la cadena de suministro de alimentos, enfocados directamente en el consumidor con aplicaciones que utilizan la identificación de ra-

dio frecuencias (RFID) móvil que permita gestionar menús e inventarios y a la vez ayude a reducir desperdicios.

Otra propuesta es contar con las tecnologías Lab-on-a-chip + Blockchain que ayude a la verificación segura de la salud del ganado. Las tecnologías Edge & IoT en "cloud" para gestionar la aplicación de correctores para el riego y el uso de fertilizantes que se conecte a sistemas locales de gestión ambiental.

Habilitadores / Inhibidores
Existen algunos habilitadores para estas soluciones como el IoT Alimentario que utiliza sensores, robótica, e IA entre otras tecnologías que se conectan a través de datos, aplicaciones y aprendizaje. Otro habilitador es la nutrición y menús personalizados con IA para el consumidor, las etiquetas estandarizadas para los alimentos, y finalmente sensores implantados.

Como inhibidores, está la cultura, el acceso limitado a la tecnología, principalmente la de bajo costo, los intereses económicos y nacionalismos que no permiten el uso de estándares globales y el intercambio de datos.

Sustainable Computing
Los centros de datos deben adoptar hardware energéticamente eficiente, así como gestión inteligente de recursos y energía renovable, sin olvidar que la adopción y ampliación de las prácticas de sostenibilidad sigue siendo un desafío, para todos los sectores y la sociedad.

Soluciones sostenibles / Oportunidad de negocio
Desde la Computación Sostenible, se plantean el uso de tecnologías para poder ofrecer certificaciones de sostenibilidad, y poder dar una ventaja competitiva sobre quienes no puedan contar con soluciones sostenibles y finalmente permitir un ahorro financiero.

Habilitadores / Inhibidores
Algunos habilitadores son el poder contar con iniciativas sostenibles en todo el mundo, una mayor participación de las personas en los temas de sostenibilidad, y finalmente el compromiso de los altos ejecutivos; sin olvidar las regulaciones establecidas por los gobiernos.

Dentro de los inhibidores está un posible aumento de precios; la complejidad que requiere la gestión, y finalmente las dificultades que se presentan para cambiar la mentalidad y la cultura de la sociedad.

Recomendaciones

El artículo de la IEEE presenta varias recomendaciones enfocadas a diferentes sectores como la industria, el gobierno, la academia, las organizaciones profesionales, los usuarios finales, los desarrolladores, los CxO, y los inversionistas. Presentamos algunas recomen-

daciones a las tres tecnologías con horizontes de adopción más cercanos y probables (LLM Development, Drone Adoption, AI Agents), y a las tres tecnologías con mayor impacto en sostenibilidad (Smart AG, Sustainable Computing, IT-Energy Convergence).

En cuanto a las tecnologías con horizontes de adopción más cercano, para LLM Development, se recomienda a la Industria la exploración de nuevas facetas de esta tecnología, en particular la de los Small LM; a los CxO, por su parte, se les sugiere modernizar sus empresas mediante el uso de nuevos tipos de LLMs. Por otro lado, la recomendación para la industria en cuanto a Drone Adoption, consiste en la validación de casos de uso de drones en entornos y modelos de negocio seleccionados, mientras que a los inversionistas se les invita a explorar nuevos modelos de transporte con drones y en el espacio. En el caso de los AI Agentes, a la industria se le pide su implementación en las áreas donde se puede complementar la labor humana; a los CxO se les recomienda modernizar sus empresas mediante su adopción; y a los usuarios finales se les llama a considerar cómo debe ser su interacción con estos agentes.

Para las tecnologías con mayor impacto en sostenibilidad, en el caso de Smart AG se considera responsabilidad del Gobierno su regulación, patrocinio y fomento, mientras que la de los inversionistas es la identificación de oportunidades sustanciales para su aplicación. Para Sustainable Computing, se le propone a la Industria su implementación de extremo a extremo para todos sus productos y servicios, y a la Academia se le solicita aumentar los planes de estudio Inter tecnológicos en informática sostenible. En cuanto a IT-Energy Convergence, se le recomienda al Gobierno promover la inversión en esta tecnología en los principales sectores industriales.

Para las nuevas tecnologías se invita a las organizaciones profesionales a desarrollar estándares adaptables (plug-and-play), que induzcan economías de escala competitivas, con niveles de credibilidad apoyados en información estadística. A los desarrolladores, por su parte, se les recomienda incrementar la automatización mediante la adopción de nuevos modelos y mejores prácticas de desarrollo (DevOps), y considerar que el consumo de energía se propaga no solo durante la operación, sino también en el desarrollo del código mismo.

Conclusión

Todos estos esfuerzos para lograr unos beneficios importantes de las nuevas tecnologías requieren la participación integral y activa de los diferentes actores y sectores de la sociedad, quienes finalmente son los beneficiarios de los avances tecnológicos. De igual forma, se debe tener en cuenta los aportes

que se pueden lograr entre las diferentes tecnologías, con el propósito de potenciar al máximo sus resultados e impacto en la humanidad. Las futuras investigaciones que se realicen sobre todos estos temas deben considerar una visión sistémica e integral orientada por propósitos de bienestar común y focalizado en el logro de los objetivos de desarrollo sostenible (ODS) (Naciones Unidas, 2025). Otro punto de vista que puede ser interesante analizar son las repercusiones de estas nuevas tecnologías en las transformaciones de los seres humanos como personas y de la sociedad en su conjunto, dentro de la perspectiva de lo que la IEEE denomina “Ciencias para la vida”.

Referencias

Amazon. (10 de 09 de 2025). AWS. Obtenido de https://aws.amazon.com/es/what-is/large-language-model/#:~:text=Los%20modelos%20de%20lenguaje%20de%20gran%20tama%C3%B1o%2C%20tambi%C3%A9n%20conocidos%20como,decodificador%20con%20capacidades%20de%20autoatenci%C3%B3n

Energy Sustainability Directory. (10 de 09 de 2025). IT/OT Convergence in Energy. Obtenido de https://energy.sustainability-directory.com/term/it-ot-convergence-in-energy/#:~:text=From%20an%20academic%20perspective%2C%20the,autonomy%2C%20resilience%2C%20and%20sustainability

Ferrovial. (10 de 09 de 2025). Drones. Obtenido de https://www.ferrovial.com/es-la/innovacion/tecnologias/drones/#:~:text=Un%20veh%C3%ADculo%20a%C3%A9reo%20no%20tripulado,de%20vuelo%20controlado%20y%20sostenido

Fortinet. (10 de 09 de 2025). ¿Qué es la ciberguerra? Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/cyber-warfare#:~:text=La%20ciberguerra%20es%20una%20serie,da%C3%B1os%20causados%20por%20estos%20ataques.

IBM. (10 de 09 de 2025). ¿Qué es la agricultura inteligente? Obtenido de https://www.ibm.com/mx-es/think/topics/smart-farming#:~:text=La%20agricultura%20inteligente%2C%20tambi%C3%A9n%20conocida,sustentabilidad%20en%20la%20producci%C3%B3n%20agr%C3%ADcola

IBM. (10 de 09 de 2025). Que son los AI Agents? Obtenido de https://www.ibm.com/mx-es/think/topics/ai-agents#:~:text=Un%20AI%20agent%20o%20agente,cu%C3%A1ndo%20recurrir%20a%20herramientas%20externas

IBM. (10 de 09 de 2025). What is AI governance? Obtenido de https://www.ibm.com/think/topics/ai-governance

IEEE Computer Society. (10 de 09 de 2025). 2025 Technology Predictions. Obtenido de IEEE Computer Society: https://www.computer.org/resources/2025-top-technology-predictions

MD. (10 de 09 de 2025). Conducción autónoma. Obtenido de https://www.md-elektronik.com/es/conduccion-autonoma/#:~:text=El%20t%C3%A9rmino%20%C2%ABconducci%C3%B3n%20aut%C3%B3noma%C2%BB%2

0se,desplazan%20solos%20y%20los%20robots

Medium. (10 de 09 de 2025). Data Feudalism: Transitioning from Serfdom to Digital Autonomy in a Decentralized Landscape. Obtenido de https://medium.com/@julia.galmiche/data-feudalism-transitioning-from-serfdom-to-digital-autonomy-in-a-decentralized-landscape-d2ce605815e5

Naciones Unidas. (10 de 09 de 2025). Objetivos de Desarrollo Sostenible. Obtenido de https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

NIH. (10 de 09 de 2025). Artificial intelligence as a tool in drug discovery and development. Obtenido de https://pmc.ncbi.nlm.nih.gov/articles/PMC11372739/#:~:text=Emergence%20of%20AI%20in%20drug,of%20AI%20in%20pharmaceutical%20research

NIX. (10 de 09 de 2025). Cómo el diagnóstico médico con IA está transformando la industria: beneficios y ejemplos. Obtenido de https://nix--united-com.translate.goog/blog/how-ai-medical-diagnosis-changes-the-industry-benefits-examples/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

NPJ. (10 de 09 de 2025). NPJ Digital Medicine. Obtenido de https://www.nature.com/articles/s41746-024-01151-3#:~:text=Abstract,these%20processes%20are%20currently%20lacking

Nvidia. (10 de 09 de 2025). Sustainable Computing. Obtenido de https://resources.nvidia.com/l/en-us-sustainable-computing

Profile Tree. (10 de 09 de 2025). 5 Ways AI-Enhanced Robotics is Revolutionising Manufacturing and Warehousing: Boosting Productivity for a Powerful Future. Obtenido de https://profiletree.com/ai-enhanced-robotics-manufacturing-warehousing/

Subex. (10 de 09 de 2025). Inteligencia Aumentada. Obtenido de https://www-subex-com.translate.goog/article/augmented-intelligence/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

Synopsys. (10 de 09 de 2025). ¿Qué es la seguridad funcional del hardware automotriz? Obtenido de https://www-synopsys-com.translate.goog/glossary/what-is-automotive-hardware-functional-safety.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

World Economic Forum. (10 de 09 de 2025). Tecnologías emergentes - Cómo combatir la desinformación de la IA y proteger la verdad en el mundo digital. Obtenido de https://es.weforum.org/stories/2024/06/como-combatir-la-desinformacion-de-la-ia-y-proteger-la-verdad-en-el-mundo-digital/

***Emir Hernando Pernet Carrillo**, DBA. Asesor en Negocios de Tecnología. Ingeniero de Sistemas y Computación de la Universidad de los Andes, Colombia, y MBA de ese mismo centro educativo. Master of Computer Science de Arizona State University, USA. Doctor of Business Administration de Newport University, USA. Experiencia de más de 20 años como Asesor de Soluciones Tecnológicas del Departamento de Sistemas de Información del Banco de la República, y Subdirector de Computación Corporativa del Departamento de Tecnología Informática del Banco de la República.*

***Maria Mercedes Corral Strassmann**, PhD. Ingeniero de Sistemas y Computación de la Universidad de Los Andes; Maestría en Comunicación de datos, University College London de la Universidad de Londres; Programa de Desarrollo Directivo - PDD de Inalde; y Doctorado de Comunicación, Lenguajes e Información en la Universidad Javeriana. Experiencia, como director de Proyectos en el Banco de la República; Gerente de TI de CIFIN - Asobancaria; vicepresidente de Tecnología de Deceval. Experiencia de más de 20 años como Profesor Universitario en áreas de Ingeniería de software, y Gerencia de proyectos, Maestría y Especialización de Ingeniería de Sistemas en la Universidad Javeriana.*

Defensa cibernética

Tecnologías de engaño y defensa de blanco móvil

DOI: 10.29236/sistemas.n176a5

Resumen

En la dinámica actual de las organizaciones y sus retos para avanzar en medio de las tensiones nacionales e internacionales, se hace necesario actualizar las estrategias de ciberseguridad empresarial para entender y aprovechar las inestabilidades e inciertos en favor del logro de sus objetivos estratégicos. En este entorno asimétrico y disruptivo, donde las certezas escasean y los ciberataques conllevan asimetrías inherentes relacionadas con información, capacidades, riesgos, oportunidades y regulaciones, el reto ya no es solo proteger, sino defender y anticipar escenarios, adoptando una postura estratégica que complemente las prácticas tradicionales. De esta forma, las tecnologías de engaño (*Deception Technologies*) y las defensas de blanco móvil (*Moving Target Defense - MTD*) emergen como soluciones estratégicas fundamentales para invertir estas asimetrías a favor de los profesionales de seguridad/ciberseguridad y habilitar nuevas capacidades cibernéticas que permitan aprender continuamente los patrones de ataque y evolucionar los señuelos para desviar los recursos del adversario. La adopción de estas tecnologías representa un cambio de paradigma hacia una defensa cibernética más dinámica y vigilante, orientada a crear confusión estratégica y jugar ahora en el mismo terreno del adversario: distracción y engaño.

Palabras clave

Tecnologías de engaño, disuasión, defensa, asimetrías, ciberseguridad

Introducción

La dinámica del mundo actual y la acelerada transformación digital establece un escenario asimétrico y disruptivo que reta cualquier estrategia corporativa. En este contexto, las tensiones internacionales y los desarrollos tecnológicos emergentes establecen el nuevo referente de las empresas para mantenerse y permanecer en el largo plazo, sin perjuicio de las diferentes posturas que una organización pueda tener para tratar de sortear los embates de cambios súbitos o mareas tecnológicas que puedan afectar la esencia de su negocio o transformar el sector donde opera (Bax & Jaggi, 2025).

En este contexto, el reto de la ciberseguridad no está en proteger y asegurar la operación de la empresa, sino en defender y anticipar los escenarios posibles y probables que puede enfrentar la organización, y desde allí, avanzar en el desarrollo y actualización de las capacidades cibernéticas que le permitan dar cuenta de su promesa de valor para sus clientes. Por tanto, es un imperativo estratégico que las empresas situadas ahora en un ecosistema digital de negocios, de forma regular, exploren y analicen las propuestas y servicios tecnológicos de seguridad para enfrentar las asimetrías propias de los ciberataques actuales (Cano, 2024).

Si bien tecnologías recientes y altamente publicitadas como la inteligencia artificial son de consulta obligada para revisión, otras alternativas, como la gestión continua de exposición a amenazas (*Continuous Threat Exposure Management* – CTEM, en inglés), las tecnologías de engaño (*Deception Technologies*, en inglés) y las defensas de blanco móvil (*Moving Target Defense* - MTD, en inglés) deben ser consideradas como parte fundamental de la actualización y adaptación de las capacidades cibernéticas disponibles en las organizaciones, que buscan distraer, demorar, confundir y disuadir a los posibles adversarios de la empresa en el contexto actual.

Las organizaciones que buscan anticipar los movimientos de sus posibles atacantes, no sólo deben estar al día en sus prácticas básicas de gestión de la seguridad, sino que permanentemente deben cuestionar lo que han aprendido hasta el momento, desconectar los fundamentos propios de su modelo de seguridad y control, para crear nuevas conexiones con las tendencias y señales débiles identificadas en el entorno, y así proponer nuevas distinciones que permitan una actualización del panorama de amenazas potenciadas con tecnologías emergentes y disruptivas (Day & Schoemaker, 2019).

En consecuencia con lo anterior, se desarrolla esta reflexión con el fin de analizar algunas tecnologías emergentes y disruptivas aplicadas al reto de anticipar en la gestión de la ciberseguridad empresarial, no como un ejercicio exclusivamente técnico, sino como una lectura estratégica que las organizaciones deben desarrollar, no solo proteger y asegurar la operación, sino para crear valor y nuevas experiencias en sus clientes, que hoy demandan soluciones creativas, identificar tendencias emergentes y generar ideas viables que transformen la manera de hacer las cosas.

Múltiples denominaciones para el entorno actual

Todos los reportes internacionales coinciden en que las organizaciones si hay algo que deben hacer en la actualidad, es navegar en entornos inciertos e inestables donde la premisa es que las certezas escasean y las turbulencias abundan. Por tanto, reconocer y ajustar sus planteamientos estratégicos es una tarea que en muchos casos dependerá si se enfrenta a una disrupción (afectación estructural del mercado o sector) o perturbaciones (causadas por crisis globales, desastres naturales o accidentes). En este sentido, se han presentado diversas formas de entender la realidad actual del mundo con acrónimos que buscan sugerir marcos de acción y análisis para que las empresas logren entender y superar sus propios miedos y avanzar con paso firme hacia el logro de sus objetivos estratégicos (Verweire, 2023).

A continuación, se presenta en la tabla 1 un breve resumen de los acrónimos más utilizados a nivel global en la actualidad.

Tabla 1

Acrónimos para entender el mundo actual

Acrónimo	Detalle	Fuente
VUCA - *Volatile, Uncertainty, Complexity, Ambiguity*	Volátil, Incierto, Complejo, Ambigüo	1980 – Escuela de Guerra de EE.UU.
TUNA - *Turbulent, Uncertainty, Novelty, Ambiguity*	Turbulento, Incierto, Novedoso, Ambigüo	2016 - Ramírez, R. & Wilkinson, A. (2016). *Strategic reframing. The Oxford Scenario Planning Approach*. Oxford, UK. Oxford Press
BANI - *Brittle, Anxious, Non-linear, Incomprehensible*	Frágil, Ansioso, No-lineal, Incomprensible	2020 - Instituto para el Futuro (Centro de Pensamiento) ubicado en Palo Alto, CA. USA
NAVI – *Nonlinear, Accelerated, Volatile, Interconnected*	No-lineal, Acelerado, Volátil, Interconectado	2025 – EY – Bax, H. J. & Jaggi, G. (2025). What if disruption isn't the challenge, but the chance? *EY*. https://www.ey.com/en_gl/megatrends/what-if-disruption-is-not-the-challenge-but-the-chance

Nota: Elaboración propia.

Cualquiera de las lecturas que se tenga o se elija para comprender el mundo la incertidumbre, la volatilidad y la No-linealidad, son parte inherente de las características que las organizaciones deben atender. En esta misma línea, los riesgos cibernéticos se hacen parte de estas características las cuales se exacerban por cuenta de las tensiones geopolíticas internacionales y la evolución natural de las amenazas digitales. Por lo tanto, las empresas del siglo XXI deben procurar mantener un sistema de vigilancia estratégica cibernética que le permite advertir los cambios y tendencias en el contexto digital para prepararse y sortear las amenazas emergentes que se puedan generar (Bodji et al., 2025).

Entender la dinámica del mundo, resulta siendo la base conceptual y práctica de la gestión del riesgo cibernético, que no busca "predecir" lo que va a ocurrir, sino establecer los distintos escenarios posibles y probables que resulten de interés para la compañía, y de esta forma, tomar las decisiones claves y las acciones estratégicas que reconozcan cómo se puede propagar dicho riesgo y disminuir sus impactos.

Asimetrías de un ciberataque

Para enfrentar los retos que implica entender, atender y superar un ciberataque, es necesario comprender las asimetrías inherentes que este evento conlleva. En este ejercicio, cinco temas resultan claves como fundamento de las reflexiones y las exigencias que se tienen tanto hacia las organizaciones y su relación con el entorno, como desde la perspectiva del atacante como actor clave que busca generar incierto, inestabilidad y caos. A continuación, se detallan en la tabla 2.

Entender estas asimetrías en el escenario actual, es lo que permite a la organización establecer algunos referentes de revisión y análisis para tratar de anticipar los futuros movimientos de sus adversarios. Ignorar esta asimetría en los análisis actuales del panorama de amenazas, implica generar nuevos puntos ciegos en los modelos de seguridad y control, y abrir mayores espacios de maniobra a los atacantes, que buscan cada vez más mimetizarse utilizando la niebla de los conflictos, la diversidad de efectos y la sorpresa como fundamento de su agenda de desestabilización.

Tecnologías emergentes y disruptivas para la gestión del riesgo cibernético

Las asimetrías mencionadas y contextualizadas en la incertidumbre, la volatilidad y la No-linealidad del mundo actual, crean "tormentas digitales adversas" que las organizaciones deben tratar de identificar, anticipar y atender para tener una mejor preparación y limitar los impactos de sus posibles efectos en las organizaciones.

Para ello, actualmente adicional a las tecnologías tradicionales que

Tabla 2
Asimetrías de un ataque cibernético

ASIMETRÍAS	EXPLICACIÓN	IMPACTOS
Asimetría de **información**	El adversario tiene un **mayor nivel de conocimiento** de la infraestructura tecnológica objetivo que la organización.	Generar mayores puntos ciegos que el adversario puede aprovechar. (***Objetivo:*** *Generar sorpresa*)
Asimetría de **capacidades**	El adversario conoce mejor que la organización **el tiempo y los recursos necesarios para acceder al objetivo** (y llevar a cabo actividades de seguimiento).	Implementar de forma acelerada técnicas, tácticas, procedimientos y herramientas novedosas para concretar el ataque. (***Objetivo:*** *Crear inestabilidad*)
Asimetría de **riesgos**	El adversario tiene un **mayor nivel de comprensión del riesgo** que implica llevar a cabo determinadas operaciones cibernéticas en comparación con la organización.	Mejorar la inteligencia para planear y ejecutar con éxito la acción adversa contra la organización. (***Objetivo:*** *Aumentar efectividad*)
Asimetrías de **oportunidades**	El adversario tiene **un mayor nivel de comprensión de la información que puede adquirir y/o la capacidad de disrupción, denegación, degradación y destrucción** en comparación con la organización.	Diseñar y ejecutar escenarios con mayor capacidad de daño y exposición para la organización. (***Objetivo:*** *Diversidad de efectos*)
Asimetría de **regulaciones**	El adversario puede **entrar en conflicto o no con las normativas o iniciativas de regulación global o nacional** para generar amenazas emergentes e innovadoras.	Generar de tensiones entre Estados y particulares que reten los límites tradicionales de las regulaciones y tratados nacionales e internacionales. (***Objetivo:*** *Aumentar las inestabilidades nacionales y globales*)

Nota: Adaptado de: Smeets, 2022, p. 159

operan en las organizaciones como son firewalls de nueva generación, EDR (*Endpoint Detection and Response*), XDR (*eXtended Detection and Response*), SOC (*Security Operation Center*) analíticos, SOAR (*Security Orchestration, Automation, and Response*) y demás siglas que sugieren los proveedores, la práctica muestra que es necesario avanzar en los temas de disuasión como factor determinante para complementar las estrategias actuales de seguridad y control que tienen las empresas.

La disuasión implica crear un entorno donde se inviertan las asimetrías del ciberataque a favor de los profesionales de ciberseguridad / seguridad, con el fin de degradar la gestión de riesgos del adversario y su inteligencia previa, para que cambie de objetivo (no de intención) y que, la organización inicialmente seleccionada ya no sea de

su interés (Burton, 2018). Lograr este resultado, implica que la organización ha alcanzado un nivel de madurez en la gestión de su infraestructura de seguridad y control, donde ahora el reto no es la protección sino la defensa: distraer, demorar, confundir y engañar.

Para ello, han venido evolucionando dos alternativas como las tecnologías de engaño (*Deception Technologies*) y las defensas de blanco móvil (*Moving Target Defense*) como alternativas interesantes para entrar en el mismo juego del adversario: distracción y engaño como fundamento de su acción. A continuación, en la tabla 3 se hace un resumen de estas dos propuestas sus ventajas y limitaciones con el fin de motivar una mejor comprensión de las mismas.

A pesar de que la implementación de estas tecnologías tiene sus retos particulares investigaciones recientes revelan hallazgos que muestran su viabilidad y efectividad para las organizaciones: (Ferguson-Walter et al., 2021)

- La implementación de tecnologías de engaño defensivo son eficaces, incluso si un atacante es consciente de su uso.
- El ciberengaño es eficaz si el atacante simplemente cree que puede estar en uso, aunque no lo esté.
- Las herramientas cibernéticas defensivas y el engaño psicológico impiden a los atacantes penetrar en los sistemas informáticos para filtrar información.

A la fecha se tienen tecnologías de engaño adaptativas basadas en inteligencia artificial (*honeypot* adaptativos) que son sistemas señuelo inteligentes que imitan activos críticos de la red, utilizando IA (Inteligencia Artificial) y aprendizaje automático (ML) para: (Datta & Acton, 2025)

- Atraer y engañar al malware basado en inteligencia artificial generativa (GenAI).
- Aprender continuamente los patrones de ataque y comportamientos del adversario.
- Evolucionar sus señuelos para mantener al atacante comprometido y distraído, y así, desviar sus recursos.

Y como todo sistema de basado en inteligencia artificial hay que considerar sus limitaciones propias como son: (Datta & Acton, 2025)

- Sesgo de datos o Modelo / Alucinaciones.
- Reentrenamiento continuo y diligente de los sistemas de IA de defensa para mantener su eficiencia y resiliencia.
- Baja confianza especialmente con “vectores de ataque novedosos”, lo que genera un posible retraso en la respuesta.

Conclusiones

En el arte y la ciencia de anticipar en la gestión del riesgo cibernético,

Tabla 3
Tecnologías de engaño y tecnologías de blanco móvil

Característica	Tecnologías de engaño (*Cyber Deception*)	Tecnologías de blanco móvil (*Moving Target Defense* - MTD)
Descripción	Buscan confundir y desinformar activamente a los atacantes, influenciando sus decisiones con información falsa (ej. *honeypots*, *honeytokens*, *honeyfiles*, vistas de red engañosas)	Buscan aumentar la incertidumbre y complejidad para el atacante mediante el cambio dinámico y continuo de las configuraciones del sistema o red (ej. mutación de IP, anonimización, diversificación de configuración)
Ventajas	• Nivelan asimetrías atacante-defensor. • Corrompen la toma de decisiones del atacante (desvío, distorsión, agotamiento de recursos). • Recopilan inteligencia valiosa sobre TTPH (Técnicas, Tácticas, Procedimientos y Herramientas) del atacante. • Habilitan la adaptación de las capacidades cibernéticas de forma proactivas y estratégica. • Complementan defensas tradicionales al ser evasivas.	• Aumentan la incertidumbre y complejidad para el atacante. • Invalidan el reconocimiento y la inteligencia base del atacante. • Hacen más difícil el aprendizaje de las reglas de detección por parte del atacante. • Confunden las herramientas automatizadas de reconocimiento del atacante. • Altera la vista de la superficie de ataque del adversario dificultando la ingeniería de exploits confiables y su persistencia en el sistema(s) objetivo.
Limitaciones	• Riesgo de detección por atacantes sofisticados. • La mutación y falsa representación pueden ser costosas o descubiertas. • Riesgo de divulgación accidental y alerta al atacante. • Preocupaciones éticas y legales (fraude, engaño, intrusión).	• Limitaciones por infraestructura física (subredes, conexiones estáticas). • Espacios de IP limitados en ciertos entornos. • Las soluciones basadas en *Software Defined Networking* (SDN)[1] pueden ser costosas y pueden requerir cambio de switches de red. • El mantenimiento de la consistencia en entornos dinámicos es un desafío.

Nota: Basado en Jajodia et al, 2016; Heckman et al., 2015

la tecnología juega un papel importante, no sólo en la implementación, sino en su comprensión y entendimiento de sus posibilidades y alcances. En este sentido, las organizaciones no sólo deben reconocer las bondades de los avances técnicos disponibles, sino situar las mismas en el ejercicio permanente de retar lo que se conoce, y en la capacidad y versatilidad de los atacantes modernos.

[1] Soluciones para generar direcciones IP aleatorias por flujo y crear vistas de red engañosas, permitiendo un control granular sobre las comunicaciones de dispositivos individuales.

En este sentido, la disuasión como control renovado en un escenario donde se privilegia el engaño y la distracción, resulta de interés para incorporar y actualizar en las estrategias actuales de seguridad y control de las empresas (Huang & Zhu, 2023). Por lo tanto, no sólo es entrar en la misma dinámica del adversario, sino saber jugar el juego y no dejarse sorprender por el posible ejercicio de contrainteligencia que ahora va a desarrollar el atacante, al ver que lo que antes era estático y conocido, ahora será dinámico y muchos veces incierto o desconocido.

El ejercicio de inteligencia para reconocer al adversario se hará ahora más intenso y retador para los profesionales en ciberseguridad, que más allá de caracterizar patrones y tendencias relevantes, deberá interpretar y movilizar sus análisis para visualizar lo que está ausente o no se ve, asumir la ambigüedad como la base de sus reflexiones y reconocer en las anomalías la esencia del ejercicio de defensa (Martin, 2019). Esto es, evolucionar de una vista técnica y aplicada (que seguirá siendo importante y relevante) hacia el desarrollo de habilidades para interpretar los cambios del entorno y las asimetrías propias de los ataques para encontrar las señales débiles que sugieran transformaciones claves que lleven a posibles alteraciones del panorama de amenazas.

De esta forma, la defensa cibernética no sólo será empujada a un siguiente nivel de evolución donde se habilitan capacidades para confundir, desviar y agotar los recursos de los atacantes, mientras se obtiene inteligencia estratégica sobre sus TTPH (Técnicas, Tácticas, Procedimientos, Herramientas) y posibles intenciones, sino que se plantea un cambio de paradigma hacia una postura vigilante, dinámica y más consciente del adversario, donde el juego infinito de defensa y ataque entra en nuevo nivel: crear confusión significativa en el descubrimiento y ataque de activos digitales en tiempo real, de forma automatiza y, ahora como servicio.

Referencias

Bax, H. J. & Jaggi, G. (2025). What if disruption isn't the challenge, but the chance? *EY*. https://www.ey.com/en_gl/megatrends/what-if-disruption-is-not-the-challenge-but-the-chance

Bodji, A., Glaser, G. & Teixeira, T. (2025). Resilience through transparency. How the midstream is key for more resilient supply chains. *Arthur D'little Insights*. https://www.adlittle.com/en/insights/viewpoints/resilience-through-transparency

Burton, J. (2018). Cyber Deterrence: A Comprehensive Approach? NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Cano, J. (2024). The Virtuous Circle of the Adversary: Challenges and

Threats for Modern Organizations. *ISACA Journal*. 3. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/challenges-and-threats-for-modern-organizations

Datta, P. & Acton, T. (2025). Promises and Perils of Generative AI in Cybersecurity. *MIS Quarterly Executive*. *24*(2). 167-184. https://aisel.aisnet.org/misqe/vol24/iss2/5/

Day, G. & Schoemaker, P. (2019). *See soon, act faster. How vigilant leader thrive in an era of digital turbulence*. Cambridge, MA. USA: MIT Press.

Ferguson-Walter, K. J., Major, M. M., Johnson, C. K. & Muhleman, D. H. (2021). Examining the Efficacy of Decoy-Based and Pyschological Cyber Deception. *30th USENIX Security Symposium (USENIX Security 21)*. 1127–1144.

Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., & Tsow, A. W. (2015). *Cyber denial, deception and counter deception: A framework for supporting active cyber defense* (1a ed.). Springer International Publishing.

Huang, L., & Zhu, Q. (2023). *Cognitive security: A system-scientific approach*. Springer International Publishing.

Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (Eds.). (2016). *Cyber deception: Building the scientific foundation* (1a ed.). Springer International Publishing.

Martin, P. (2019). *The rules of security. Staying safe in a risky world*. Oxford, UK. Oxford University Press.

Smeets, M. (2022). *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force*. USA: Oxford University Press.

Verweire, K. (2023). *Strategy in Turbulent Times: How to Design a Strategy that is Robust and Future-Proof*. Lannoo.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Tecnologías disruptivas en tiempos turbulentos

DOI: 10.29236/sistemas.n176a4

En el marco del encuentro fueron tratados los asuntos más relevantes relacionados con el entorno actual sobre el tema en cuestión.

María Mercedes Corral y Emir Pernet, editores técnicos de esta edición, dieron la bienvenida a los participantes y abrieron el debate formulando la primera pregunta.

En tiempos turbulentos de perturbaciones y disrupciones globales ¿son las tecnologías disruptivas y emergentes una opción para avanzar hacia el encuentro de nuevas ventajas competitivas o de escenarios de nuevos riesgos para entender y superar? ¿Las dos cosas? ¿por qué?

Sandra Lascarro Mercado
En mi opinión son las dos cosas. Son muchas las ventajas de usar tecnología para automatizar procesos, ganar tiempo y trabajar para escalar servicios; no es lo mismo hacerlos masivos sin ese recurso. Pero también veo varios riesgos en la gobernanza y en el objetivo para soportar al ser humano. Existen

problemas éticos, asuntos legales, manejo de desperdicio electrónico, gasto energético. Especialmente, en las nuevas generaciones porque la tecnología está presente en sus tareas de colegio.

Jeimy J. Cano M.
Director Revista Sistemas

Los primeros estudios realizados sobre los impactos de la IA tanto en las organizaciones como en las universidades hablan de la descarga cognitiva. Es decir, la dependencia de la IA que reduce la capacidad de los profesionales para realizar análisis críticos independientes y resolver problemas sin apoyo tecnológico. El otro riesgo se plantea alrededor del cuidado del planeta particularmente en los Estados Unidos, en donde los asuntos relacionados con los objetivos sostenibles no son parte de su agenda política actual, especialmente en lo relacionado con el medio ambiente.

Y si esta gran potencia no está sintonizada con los temas de sostenibilidad, pues muy seguramente se van a adoptar tecnologías disruptivas que pueden poner en peligro el futuro de nuestro planeta o el futuro de nuestra sociedad.

Sandra Lascarro M.
Ese es otro de los riesgos que tenemos que mirar cómo lo manejamos, cómo lo controlamos, cómo lo mitigamos y cuáles son las diferentes estrategias para manejo de riesgos.

Un asunto adicional a lo ya mencionado, que poca importancia tiene y queda como "detrás de cámaras", es el manejo de los desperdicios electrónicos. Un ejemplo concreto es el de los páneles solares y la gente que está metiéndose en esa línea no se pregunta, cuando termine su vida útil ¿qué va a pasar?

Jeimy J. Cano M.
Hoy, esos paneles solares son más contaminantes. Y son temas que hay que tener en cuenta como una parte del ecosistema digital que se ha desarrollado precisamente para acelerar las cosas y el desarrollo tecnológico.

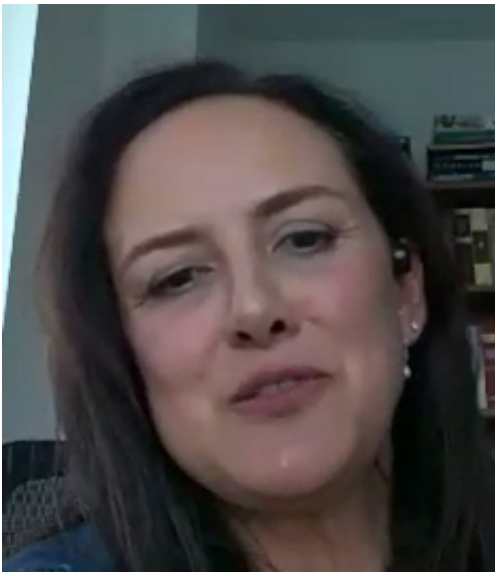
Sandra Lascarro M.
Estamos como en plan Terminator, yendo derecho a perder el control de nuestras vidas. La AI ahora es la puerta de entrada a cualquier empresa, son los porteros de los edificios. Cuando voy a un lugar y me

atiende un robot en lugar de una persona pues a veces no tienen el criterio y demoran más al cliente en lugar de agilizar, personalmente pienso que una persona debe tener aún la autoridad y el criterio para ayudar a otro ser humano inicialmente, si es una tera sencilla lo atiende un robot, si no, lo atiende otro humano… Es un avance, pero entre comillas. Pero me voy a Manhattan a la conferencia Smart Cities, comiéndome una manzana del metro hasta el muelle. Cuando la voy a botar, no encontraba caneca para hacerlo, por ninguna parte hasta después de 20 minutos y estaba cerrada y sellada. Bajé una app para abrirla, una cosa absurda, pues luego uno tiene que decir qué es lo que va a botar en la caneca para poder o no abrirla, no están todas las opciones claras. Duré exactamente 12 minutos en el proceso de abrirla y no fue posible. Yo le explicaba que era una manzana, que era una semilla y me decía que ahí no podía botarla. Pienso que es lo más absurdo que se han inventado.

Jeimy J. Cano M.
Me imagino que ellos pretendían evitar que la gente botara desperdicios, pero se les olvidó que es un ser humano el que está usando la caneca. Surge entonces el tema de la funcionalidad. La solución natural era disponer de un pedal físico y listo.

Emir Pernet
Pasamos a la segunda pregunta. Y es: dentro de ese conjunto variado, de tecnologías disruptivas y emergentes que están disponibles, ¿cuáles podemos aprovechar hoy en día?. ¿Cuáles son las más relevantes que se pueden aplicar en nuestro país o en nuestro contexto, y ¿por qué?

Sandra Lascarro M.



Hablando de sostenibilidad, creo que se pueden aplicar todas, mientras mantengan la democracia de la información completa y que todo el mundo pueda tener acceso. Que la calidad de la información sea buena, me parece fundamental. Disponer por ejemplo de los datos abiertos que en Colombia están muy bien legalizados, aunque todavía falta implementación y que los datos publicados sean relevantes

Que la ciudadanía pueda tener acceso a los datos, tener indicadores claros de gestión de las ciuda-

des y que la gente pueda usarlos. Y pienso que donde más se deben aplicar es precisamente en gobierno, porque es donde más se necesitan, donde más hace falta automatizar cosas, donde más hace falta hacerle seguimiento a la información. Creo que automatizar los servicios públicos, por ejemplo, tener predicciones en salud, seguridad, poder disponer de internet de las cosas para monitoreo ambiental. No es lo mismo poner cámaras en todas partes, sin tener ningún análisis y sin que los ciudadanos estén enterados de que no tienen acceso a nada de eso. No dudo en que cualquier tecnología es viable, mientras exista una solución real que afecte positivamente a las personas.

Y mientras haya educación, porque aquí uno ve, por ejemplo, los robotcitos de Uber Eats. que andan solos por la calle, nadie se lo roba, nadie lo destapa y se roba lo que hay adentro, o sea, es un tema cultural Es impresionante. Los carros no los atropellan, ellos cruzan la calle, esperan el semáforo. Yo pensaba esto en Colombia no dura un segundo. Si, aquí en Manhattan hay problemas con las bicicletas eléctricas y los scooters… pero existe también el dinero para reemplazar los que se pierden o se dañan. Así que el problema no es tecnológico, es cultural y educativo.

Sí, porque fíjense que llegan nuevas tecnologías que permiten, por ejemplo, los temas de economía social, como Uber, Waze, como B&B, que son aplicaciones que realmente ayudan a resolver problemas y a compartir recursos. Y fíjense todo el problema que tienen de adaptabilidad al país. O sea, muchos países los adaptaron sin ningún problema, es más, les crearon parqueaderos, espacios para que se trabajaran y en Colombia no. En Colombia ha sido muy difícil este ingreso de muchas tecnologías porque terminan afectando a algunos pocos. Entonces, en lugar de buscar que realmente les cambie la vida a muchas personas, terminan es trabajando sus propios intereses.

Emir Pernet

¿Cuáles elementos se deben considerar para la selección, diseño e implementación de iniciativas digitales con tecnologías emergentes y disruptivas?

Sandra Lascarro M.
En mi opinión tiene que ver con el hecho del problema que resuelve, o sea, tener un propósito claro al respecto. Eso es un elemento muy importante. ¿A cuántas personas realmente afecta esta solución? Porque no se trata de resolverle el problema a tres personas, sino realmente afectar la mayor cantidad de gente posible.

Y eso es algo que uno ve mucho en la industria. Otro aspecto a tener en cuenta es si realmente las personas están dispuestas a adoptar estos cambios y no se está haciendo tampoco gestión del cambio, lo cual tiene que realizarse siempre que se va a adoptar una tecnología de estas, sobre todo cuando es disruptiva y realmente va a generar un cambio drástico.

Jeimy J. Cano M.
Hay un elemento importante allí, Sandra, que es clave y que es una palabra que he venido escuchando en la perspectiva que tú planteas, que es una perspectiva muy de negocio, a propósito del libro Verweire, K. (2023). *Strategy in Turbulent Times: How to Design a Strategy that is Robust and Future-Proof*. Bélgica: Lannoo. Estrategia en tiempos turbulentos. Lo primero es ¿Qué problema vamos a resolver? Si usted no tiene claro el problema que va a resolver, no avance. De hecho, tener clara la pregunta de investigación o el problema a resolver, es la solucionar la mitad del problema.

Lo segundo, a propósito del último comentario, es generar confianza digital. Ese es el elemento articulador que al final permite que una tecnología, emergente o disruptiva, por lo menos avance a un siguiente estado. Presentar una prueba de concepto puede ser un buen inicio para construir esta confianza y no llegar a improvisar.

Lo digo por la experiencia concreta que viví en una visita al ecosistema de ciberseguridad de la República Checa. Una persona, un equipo de trabajo y un estudiante de tesis doctoral resolvieron un problema específico relacionado con el análisis de los paquetes anormales en un tráfico de red. Se dedicaron 5 años a eso y desarrollaron un producto que se volvió parte después de una suite de un producto más grande.

Ahora, existen otros escenarios, en los cuales las tecnologías disruptivas pueden potenciar soluciones ya existentes. Es decir, hay problemas que tienen una solución vigente que utilizan cierto tipo de tecnología, pero que se puede optimizar adoptando otras tecnologías novedosas, sin partir desde cero.

Jeimy J. Cano M.
Casos concretos hay. Sí, sí, sí. Pero también ahí pues que tan lista están las organizaciones, que tan lista está su recurso humano, que tan listo está. Sí, muchas cosas, las normas, las leyes, la parte legal. Sí, o sea que ahí es donde cae todo

otra vez. Entonces De hecho Está todo, pero no, no sale.

Sandra Lascarro M.
De hecho, el Foro Económico Mundial en una publicación de 2017 dijo, "¿Cuáles son las cinco cosas que son claves para la transformación digital?". Entonces, unas, las que son hacia afuera, las que van a afectar los grupos de interés. El tema de seguridad y privacidad, en eso no puede fallar. Y hacia dentro, la cultura. Ese es el segundo elemento. O sea, de los cinco en esos dos, las organizaciones no se pueden equivocar. Ese es el modelo de negocio. En eso se puede equivocar. Otro es la infraestructura; y finalmente, el último elemento es el de la financiación. Los capitales de riesgo.

Jeimy J. Cano M.
Dice el Foro Económico Mundial en su reporte sobre la transformación digital en 2017, “En todo eso se pueden equivocar, pero en lo que no se pueden equivocar es en el tema de seguridad y privacidad, que es la afectación hacia afuera con sus grupos de interés y hacia dentro el desarrollo de una cultura digital”.

Emir Pernet
Abordamos ahora el tema de los ejecutivos: ¿Estos equipos están preparados para definir y para detallar el apetito al riesgo digital que supone la implementación de tecnologías disruptivas y emergentes en una organización?. ¿Están preparados? Totalmente, parcialmente? Y si la respuesta es no, o si es parcialmente, ¿qué tendrían que hacer o qué se debería hacer para acompañar a esos equipos y apoyarlos en sus deficiencias?

Sandra Lascarro M.
El riesgo digital es todavía un concepto relativamente nuevo en una alta dirección, o sea, casi que no se no se ha empezado a medir realmente como debería. Todavía falta mucha formación a niveles directivos acerca de ética, de la gobernanza digital y de los riesgos.

Emir Pernet
también encontramos que muchas veces las organizaciones no tienen la capacidad interna para poder ayudar a sus directivos a considerar y a medir esos riesgos digitales. Pero existen firmas consultoras con experiencia en algunos sectores de la industria, que pueden apoyar a las organizaciones a desarrollar las capacidades requeridas en sus directivos.

Es decir, no necesariamente todo tiene que ser con recurso interno. Claro, definitivamente necesitan la participación de gente de muchas áreas. Internamente hay que generar el diálogo, pero también hay que generar estos diálogos con la academia, y con consultores externos para poder realizar un análisis más amplio. No es lo mismo una mirada desde el interior que desde el exterior.

Sandra Lascarro M.
Pero también yo creo que ahí hay un punto y es de cuánto recurso dispone la organización para esas cosas. Recursos no financieros, es gente, es plata, obviamente, es tiempo, ¿sí? O sea, de cuánto se está hablando para poder llegar a ese tipo de temas, así es. Otro asunto está relacionado con las juntas directivas, mi foco durante los últimos casi nueve años. La gente cree que a sus integrantes no les interesa el tema, pero no es así.

Entonces, lo primero que yo encuentro es una barrera que muchas veces ponemos nosotros mismos cuando hablamos con nuestros ejecutivos que es el lenguaje.

Jeimy J. Cano M.
Eso me llevó a escribir un libro para los ejecutivos, donde no hay un solo término técnico en ese texto, solo ciberseguridad mirada desde el negocio. Entonces, primera cosa, es un tema de lenguaje. Lo segundo, el tema es que ellos, los ejecutivos, quieren aprender. Eso se llama alfabetización digital. Y mirando varios modelos, al día de hoy eso se resume en el marco ABC cuadrado. Analítica, es decir, cómo van a usar los datos. Segundo, negocio (*Business*), entender el negocio en el contexto digital y la promesa de valor. Tres, el código, es decir, la infraestructura, las plataformas, claro, no se va a volver experto, sino que conozcan cómo se habilitan capacidades en esas plataformas. Y finalmente la ciberseguridad que es lo que atraviesa precisamente todo el ejercicio anterior desde la analítica hasta el código. Y si ellos están entrenados por lo menos en esos cuatro temas, las conversaciones son distintas.

Emir Pernet
Última pregunta. ¿Cuáles elementos debemos tener en cuenta en una organización para evaluar y seleccionar nuevas tecnologías disruptivas de cara al futuro?, ¿Cómo debemos tratar y entender los riesgos digitales emergentes?

Sandra Lascarro M.
Ese es uno de los riesgos que definitivamente se tiene que trabajar. Es necesario estar atentos a que la información no esté manipulada y que no haya tampoco dependencia tecnológica. Ese es otro riesgo digital muy grande. Se trata de lograr que realmente el usuario se empodere y pueda resolver también ciertas cosas. Tales riesgos hay que tenerlos en cuenta para las evaluaciones, pero también hay que considerar todo el impacto social. O sea, si realmente se está haciendo inclusión o si solamente se está generando más división entre los que sí saben usar la tecnología y quiénes no.

Jeimy J. Cano M.
Entonces es un tema de percepción y de apetito de riesgo. Un ejemplo concreto. Tú has visto cuando llega el momento de actua-

lizar o colocarle un parche a tu equipo. Microsoft te dice, “Hay que actualizar un parche”. Y tú dices, “No lo actualizo”, ahí estás aceptando un riesgo. Esto es, estás aceptando que al no tener el parche, el atacante pueda tomar control de tu máquina o hacer lo que sea con esa vulnerabilidad que se iba a corregir con ese parche. Ese es tu apetito.

Emir Pernet

Después de todos estos temas que hemos que hemos visto de riesgos, de tecnologías disruptivas, de alfabetización, y de cultura,. ¿Qué reflexiones finales podemos traer? ¿Qué valor agregado podemos darle a nuestros lectores con respecto a la mejor forma de sacar provecho de las nuevas tecnologías en entornos tan volátiles?

Sandra Lascarro M.

En mi opinión, el mensaje es siempre tener de primero al ser humano como centro y objetivo, además de acordarse que todas estas nuevas tecnologías están para soportar el desarrollo del ser humano y para ayudarnos a vivir mejor; la idea es conseguir soluciones disruptivas que realmente ayuden a resolver los problemas que tenemos.

Yo pienso que ese es como el objetivo principal y fundamental de cualquier proyecto tecnológico en el que nos embarquemos. Y entre más disruptivo sea, pues más gestión de cambio, más educación, más planeación.

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

¡ Pongase al día en sus cuotas !

Recuerda que te da derecho a participar en un evento virtual

Comuniquese con nuestro equipo de atención al cliente.
suscripciones@acis.org.co
o al télefono 3015530540

Para más información
www.acis.org.co/