VOLUMEN XIII
ISSN:2015-5392

CPIC
COLEGIO DE PROFESIONALES EN INFORMÁTICA Y COMPUTACIÓN

TECHNOLOGY inside

AGRADECIMIENTOS

COMITÉ EDITORIAL

Ing. Francisco Vargas Navarro
Ing. Modesto Jara Porras
Federico Jiménez Molina
Josué Estrada Solano

AUTORES Y CO-AUTORES

Mtr. Ricardo Aguirre Morice
Ministerio de Educación Pública. Ingeniería Informática, Seguridad de la Información.
Dr. Juan Carlos Sandí-Delgado
Informático, Profesor Catedrático, UCR
Mag. Steven Cruz-Sancho
Informático, Académico Campus Sarapiquí, UNA
Bach. Samuel Jones-Chaves
Informático, estudiante Universidad de Costa Rica
Bach. Xavier Gómez-López
Informático, estudiante Universidad de Costa Rica
Mba. José Andrés Fernández Marmolejo
Coordinador, Comisión de Inteligencia Artificial, CPIC
J. Alonso Solano Segura
Autor. Docente Universitario
Licdo. Joseph Rodríguez Marín
MAP., Autor

REVISIÓN FILOLÓGICA

Margarita Chaves Bonilla
Filólogos de Costa Rica

MAQUETACIÓN

Franciny González Coto
Josué Estrada Solano
Juan Pablo Arias Morales

DIVULGACIÓN

Departamento de Comunicación y Relaciones Públicas
Colegio de Profesionales en Informática y Computación (CPIC)

PRODUCIDO POR

Colegio de Profesionales en Informática y Computación (CPIC)
2025

TABLA DE CONTENIDO

ISSN: 2015-5392

EDITORIAL

Estimados lectores,

Es un honor para el Comité Editorial de Technology Inside presentarles la decimotercera edición de nuestra revista, la cual refleja el dinamismo, la innovación y el compromiso ético de nuestra comunidad frente a los retos de la era digital.

En esta entrega, exploramos cómo la inteligencia artificial ya está transformando las aulas, el panorama regional de América Latina y el Caribe, y los desafíos en gobernanza, equidad y soberanía tecnológica. Asimismo, abordamos la importancia de una ciberseguridad sólida en el sector educativo y el papel de las metodologías ágiles como motor de cambio cultural y eficiencia.

También dirigimos la mirada hacia tecnologías emergentes como los gemelos digitales, que combinan IA, IoT y Big Data para revolucionar procesos industriales y abrir oportunidades en sectores como la medicina, con beneficios potenciales en eficiencia, calidad y reducción de costos.

Estos temas recuerdan que la tecnología, por sí sola, no garantiza el progreso. Este requiere principios éticos, formación continua y una visión humanista que coloque a las personas en el centro. Como profesionales, corresponde liderar esta transformación con conocimiento, criterio y compromiso social.

Atentamente,

Comité Editorial de Technology Inside
CPIC

ISSN: 2015-5392 VOLUMEN XIII

ANÁLISIS CRÍTICO DE LA POLÍTICA DE CIBERSEGURIDAD DEL MEP: RETOS Y OPORTUNIDADES PARA SU OPTIMIZACIÓN

Mtr. Ricardo Aguirre Morice
Ministerio de Educación Pública de Costa Rica. Ingeniería Informática, Seguridad de la Información. Ciberseguridad.
ricardoaguirremorice@hotmail.com

RESUMEN

Este artículo evalúa la Política de Ciberseguridad del Ministerio de Educación Pública de Costa Rica (MEP) en relación con estándares internacionales como ISO 27001 y NIST CSF. Se identificaron fortalezas en su alineación con normativas nacionales, pero también brechas en áreas críticas como capacitación, gestión de incidentes y continuidad del negocio. A través de un enfoque comparativo y metodológico, se propone un plan de mejoras para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

ABSTRACT

This article evaluates the Cybersecurity Policy of Costa Rica's Ministry of Public Education (MEP) in relation to international standards such as ISO 27001 and NIST CSF. Strengths were identified in its alignment with national regulations, but also gaps in critical areas such as training, incident management, and business continuity. Through a comparative and methodological approach, an improvement plan is proposed to ensure the confidentiality, integrity, and availability of institutional information.

Palabras clave: Ciberseguridad, políticas educativas, ISO 27001

INTRODUCCIÓN

El Ministerio de Educación Pública (MEP) de Costa Rica constituye una de las instituciones más extensas del país en términos de estructura administrativa y volumen de información gestionada. Según datos del MEP (2019), cuenta con aproximadamente 88 000 funcionarios públicos, distribuidos entre las oficinas centrales -incluido el despacho de la ministra-, 27 direcciones regionales ubicadas a lo largo del territorio nacional, cerca de 206 circuitos escolares y alrededor de 4825 centros educativos.

A partir de estas cifras, puede inferirse que el MEP es una organización con una alta superficie de exposición y un volumen significativo de datos bajo su gestión. Esta magnitud se incrementa aún más al considerar la población estudiantil. De acuerdo con Sibaja (2024), en el año 2023 se registró una matrícula de 1 123 964 estudiantes. Con base en esta información, se puede extrapolar que el MEP administra datos personales correspondientes al 24,03 % de la población nacional, al sumar tanto al personal funcionario como al estudiantado.

Esto significa que casi una cuarta parte de los datos personales del país se encuentra almacenada en los sistemas del MEP, sin contar los registros históricos acumulados por la institución. Se trata, por tanto, de una cantidad considerable de información concentrada en una sola organización, lo que la convierte en una verdadera mina de oro de datos, susceptible de ser explotada por quienes sepan cómo acceder y utilizar adecuadamente dicha información.

JUSTIFICACIÓN

Con base en los datos presentados con anterioridad, se justifica la necesidad de cuantificar el potencial que posee el MEP y, paralelamente, analizar el riesgo inherente que enfrenta desde una perspectiva estratégica. Costa Rica, como país con un sistema educativo público y obligatorio en los niveles de primaria y secundaria, garantiza que todos los ciudadanos, en algún

 ISSN: 2015-5392

momento de sus vidas, transiten por esta institución mediante sus diversas unidades descentralizadas. Esta característica posiciona a la educación nacional como una infraestructura crítica, dada su función esencial en la formación ciudadana y su alta exposición a riesgos de seguridad.

El MEP, al gestionar información personal sensible -tanto de menores de edad como de administradores de fondos públicos y funcionarios de la institución-, enfrenta riesgos significativos en términos de filtración de datos. Este panorama convierte a la organización en un posible objetivo de interés para actores maliciosos. Por tanto, resulta imperativo integrar elementos de ciberseguridad, ciberinteligencia y seguridad de la información en la estructura primaria del MEP, no solo como una medida de protección, sino también como una estrategia para fortalecer la resiliencia institucional frente a amenazas potenciales. Esta integración tiene como fin mitigar riesgos y garantizar la continuidad operativa, destacando la importancia de incorporar estos componentes dentro de las políticas y estrategias nacionales de protección de infraestructura crítica.

OBJETIVO:

Evaluar la Política de Ciberseguridad del Ministerio de Educación Pública (MEP) y proponer una modificación estructurada que optimice la protección de datos y fortalezca su capacidad de respuesta ante amenazas cibernéticas.

ANTECEDENTES:

Según Moreno (2019), la educación es un derecho de las personas a lo largo de su vida y constituye una responsabilidad del Estado, el cual debe garantizar tanto la alfabetización digital como el uso de las tecnologías de la información y la comunicación en los procesos educativos. Como señala el autor, la educación es la piedra angular de muchas naciones, y uno de los elementos fundamentales que la sostiene es la seguridad. Surge entonces la pregunta: ¿qué tipo de seguridad provee el Estado a las instituciones educativas?

En términos generales, se puede hablar de una seguridad jurídica y física, expresada en medidas como la instalación de alambrado, cercas perimetrales o la presencia de personal capacitado para salvaguardar la integridad de quienes asisten a estos centros. Esta concepción corresponde a una noción de seguridad entendida como “el conjunto de métodos que promueven un entorno seguro y protegido que permite a las personas desarrollar sus actividades cotidianas” (Purpura, 2006, p. 20).

A partir de esta descripción, puede afirmarse que la seguridad es uno de los pilares esenciales para el funcionamiento de cualquier sociedad que aspire a una vida cotidiana estable. Esta idea es respaldada por el filósofo humanista Abraham Maslow, quien en su teoría de la motivación humana sitúa la necesidad de seguridad y protección en el segundo nivel de su jerarquía, justo después de las necesidades fisiológicas básicas . Maslow plantea que el ser humano debe avanzar progresivamente desde la base de dicha pirámide hasta alcanzar la autorrealización.

Fig. 1. Pirámide de Maslow.

Si se considera que las instituciones educativas albergan tanto a personas en proceso de formación como a cientos de profesionales comprometidos con ese fin, resulta evidente que todos los actores deben velar por la seguridad de la comunidad educativa. Sin embargo, esta seguridad no puede limitarse únicamente al ámbito físico o tradicional; también debe extenderse al entorno digital.

[1]La pirámide de Maslow es una teoría psicológica que organiza las necesidades humanas en cinco niveles jerárquicos: fisiológicas (alimento, agua, sueño), de seguridad (protección, estabilidad), sociales (amor, pertenencia), de estima (reconocimiento, respeto) y de autorrealización (desarrollo personal, creatividad). Cada nivel debe satisfacerse parcialmente antes de avanzar al siguiente.

Desde finales del siglo XX, con la expansión del acceso a Internet, se ha producido una creciente digitalización de los espacios educativos. Este fenómeno se ha intensificado en cada década, y cobró especial relevancia tras la pandemia global de COVID-19, la cual sumió al mundo en una interconexión y dependencia aún mayores de las tecnologías digitales. Como consecuencia, aumentó de forma significativa la exposición a los riesgos asociados a este entorno, haciendo urgente una revisión de las estrategias de protección y resiliencia institucional.

La tecnología, en la vida moderna, ha incrementado significativamente los riesgos en materia de seguridad de la información. Los ciberataques -como el robo de datos, el ransomware y el phishing- se han convertido en amenazas constantes que buscan explotar vulnerabilidades en sistemas y redes con el fin de obtener acceso no autorizado a información sensible. La expansión del Internet de las Cosas (IoT) ha agravado esta problemática, ya que muchos dispositivos conectados, a menudo desprotegidos o mal configurados, representan nuevos puntos de entrada para los atacantes. Asimismo, la creciente dependencia de servicios en la nube y de soluciones de almacenamiento digital ha expuesto tanto a empresas como a individuos a fallos de seguridad asociados con accesos indebidos y configuraciones erróneas.

La seguridad de la información también enfrenta un desafío crítico relacionado con el factor humano, el cual continúa siendo una de las principales vulnerabilidades. La falta de concienciación sobre prácticas seguras, el uso de contraseñas débiles y la susceptibilidad a técnicas de ingeniería social son problemáticas recurrentes que facilitan la explotación de datos confidenciales. Paralelamente, la cantidad masiva de información personal almacenada en plataformas digitales ha generado crecientes preocupaciones sobre la privacidad, incluyendo riesgos de seguimiento no autorizado, uso indebido de datos y su comercialización sin consentimiento.

Por todo lo anterior, se hace imprescindible añadir una capa adicional de protección a las ya existentes, especialmente en sectores estratégicos como la educación. Es necesario, incluso, replantear la jerarquía de necesidades de Maslow, incorporando la seguridad de la información como un componente esencial para resguardar la infraestructura crítica del sistema educativo. Proteger los datos de los ciudadanos que acceden a estos servicios es indispensable para la formación integral de quienes construirán el futuro de la nación.

La creación de una cultura de seguridad de la información en la sociedad -y particularmente en los entornos educativos- es fundamental, dada la centralidad de la tecnología en la vida cotidiana y los riesgos emergentes que se presentan en escenarios catastróficos o altamente tecnologizados. En un contexto donde la información personal está digitalizada y la identidad puede ser manipulada o incluso robada, emergen amenazas como el otorgamiento indebido de una identidad a terceros o a humanos digitales. Esto podría derivar en accesos no autorizados a recursos críticos, en decisiones legales erróneas o incluso en la suplantación total de una identidad digital.

En el ámbito educativo, donde los datos de estudiantes y docentes son especialmente vulnerables, la falta de medidas de seguridad incrementa el riesgo de estas amenazas. La posibilidad de clonar o reutilizar una identidad educativa con fines maliciosos -como el fraude académico o el acceso indebido a recursos institucionales- constituye un peligro real.

Una cultura sólida de seguridad de la información también es clave para prevenir el uso indebido de identidades digitales y garantizar la integridad de los datos en una sociedad cada vez más interconectada. Sin una formación adecuada en prácticas seguras, las personas son más susceptibles a ataques sofisticados capaces de usurpar su identidad no solo en redes sociales o plataformas financieras, sino también en entornos digitales avanzados, donde humanos artificiales pueden simular comportamientos, voces o decisiones de individuos reales.

Este tipo de amenazas plantea implicaciones éticas y legales profundas, ya que una identidad comprometida en un entorno digital hiperconectado puede ser utilizada para manipular sistemas, cometer delitos o distorsionar realidades personales y sociales. Por ello, integrar la educación en ciberseguridad desde edades tempranas no solo promueve una ciudadanía más consciente y resiliente, sino que también fortalece la capacidad colectiva de anticiparse y responder ante escenarios críticos, donde las consecuencias de una identidad comprometida podrían ser irreversibles.

ISSN: 2015-5392

Es en este punto donde debe iniciarse el proceso de comprensión de algunos términos clave, con el fin de establecer el contexto en el que se debe actuar desde una etapa previa. Purpura (2006) define la prevención como "métodos de reducción de las posibilidades de que ocurra una pérdida y también los gastos asociados" (p. 21). A partir de esta definición, puede inferirse que la prevención constituye una estrategia orientada a disminuir los posibles efectos adversos de un evento no deseado.

Asimismo, el mismo autor introduce el concepto de prevención de pérdidas, que describe como "una gama más amplia de métodos para proteger a las personas y la propiedad" (p. 20). Este conjunto de métodos integra elementos esenciales, entre ellos la estrategia, entendida como un procedimiento que puede aplicarse de forma metódica para obtener resultados consistentes, sin importar el contexto en el que se implemente. Su finalidad última es salvaguardar los bienes o las personas que se desean proteger.

Es en esta confluencia conceptual donde se vislumbran los marcos internacionales de seguridad de la información como referentes fundamentales para la estructuración de políticas eficaces de protección:

Posicionamiento teórico
Explicación de conceptos clave: Confidencialidad, integridad, disponibilidad.
Resumen de estándares relevantes (ISO 27001, NIST) ISO 27001 y 27002

Las normas ISO/IEC 27001 e ISO/IEC 27002 constituyen pilares fundamentales en la gestión de la seguridad de la información a nivel organizacional. La ISO/IEC 27001 establece un marco integral para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), siendo una norma certificable que define los requisitos esenciales para administrar eficazmente la seguridad informática en cualquier entidad. Su contraparte, la ISO/IEC 27002, actúa como una guía complementaria detallada, ofreciendo directrices específicas y mejores prácticas para la implementación efectiva de los controles de seguridad.

La relevancia de estas normas se manifiesta en diversos aspectos críticos para las organizaciones. En primer lugar, proporcionan una protección robusta frente a filtraciones de datos y ataques cibernéticos mediante un enfoque sistemático de gestión de riesgos. Asimismo, facilitan el cumplimiento de regulaciones legales como el GDPR, HIPAA y PCI-DSS, lo cual resulta esencial en el entorno normativo actual. Las organizaciones que obtienen la certificación ISO/IEC 27001 no solo demuestran un compromiso serio con la seguridad de la información, sino que también adquieren una ventaja competitiva significativa al generar mayor confianza entre clientes y socios estratégicos.

La estructura de estas normas se organiza de forma meticulosa en cuatro categorías principales de controles. Los controles organizacionales, que comprenden 37 elementos, abordan aspectos clave como el establecimiento de políticas de seguridad, la asignación de roles y responsabilidades, la evaluación sistemática de riesgos y el aseguramiento del cumplimiento normativo. Los controles relacionados con las personas, con 8 elementos, se enfocan en aspectos fundamentales como la concienciación en seguridad, la capacitación del personal y la gestión de accesos basada en funciones claramente definidas.

Los controles físicos, integrados por 14 elementos, se centran en la protección tangible de la infraestructura, incluyendo el control de acceso a las instalaciones, la protección de equipos y activos, y la adecuada gestión de residuos y medios de almacenamiento. Por su parte, los controles tecnológicos, compuestos por 34 elementos, constituyen una capa importante de defensa que abarca la protección contra malware, la seguridad en redes y comunicaciones, el cifrado de datos y la gestión de vulnerabilidades.

La implementación de estas normas sigue un proceso estructurado basado en el ciclo de vida del SGSI, que inicia con la definición clara del alcance y los objetivos. Esta fase implica la identificación precisa de los procesos, activos y sistemas que estarán bajo protección, así como el establecimiento de metas medibles y alcanzables. Posteriormente, se desarrolla una evaluación exhaustiva de riesgos, que incluye la clasificación de activos de información, la valoración de amenazas y vulnerabilidades, y la implementación de controles específicos para mitigar los riesgos identificados.

La fase de implementación requiere el desarrollo de políticas y procedimientos formales, la conformación de un equipo competente de respuesta a incidentes y la aplicación de medidas técnicas de protección como el cifrado avanzado, los sistemas de respaldo y los controles de acceso robustos. Este proceso se complementa con auditorías internas periódicas y un compromiso con la mejora continua, que incluye revisiones constantes de cumplimiento y la ejecución de acciones correctivas cuando sea necesario.

Entre las medidas específicas de seguridad se destacan el control de acceso basado en el principio del menor privilegio, la autenticación multifactor, la implementación de firewalls y sistemas de detección de intrusos, así como el uso del cifrado AES-256 para la protección de datos. Asimismo, se subraya la importancia de programas continuos de formación en seguridad informática dirigidos al personal, junto con la adopción de medidas específicas para entornos en la nube, incluyendo plataformas como AWS, Azure y Google Cloud.

Aplicación de ISO/IEC 27001 e ISO/IEC 27002 en centros educativos y oficinas centrales de una organización educativa

La adopción de las normas ISO/IEC 27001 e ISO/IEC 27002 en centros educativos y oficinas administrativas de una organización educativa establece un marco estructurado de seguridad para la protección de la información académica, administrativa y personal de estudiantes, docentes y personal institucional. Esta implementación responde a la necesidad de garantizar la integridad, confidencialidad y disponibilidad de la información, especialmente en un contexto donde la digitalización educativa y el uso de plataformas en la nube son cada vez más frecuentes.

1. Implementación en centros educativos

En los centros educativos, la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 se enfoca en la protección de los datos de estudiantes y docentes, así como en la seguridad de los sistemas digitales utilizados en el entorno educativo. Las principales medidas a implementar incluyen:

Controles organizacionales:

- Definir políticas de seguridad para el manejo de información sensible, como calificaciones, registros médicos y datos personales de los estudiantes.
- Establecer protocolos para la gestión de incidentes de ciberseguridad, asignando roles y responsabilidades al personal docente y administrativo.
- Implementar un programa de formación en ciberseguridad dirigido a docentes y estudiantes, con el objetivo de fomentar una cultura de protección de datos desde edades tempranas.

Controles de personas:

- Capacitar de forma periódica a docentes y estudiantes en temas como phishing, ingeniería social y buenas prácticas de seguridad digital.
- Gestionar los accesos a plataformas educativas y bases de datos mediante mecanismos de autenticación multifactor (MFA) y privilegios basados en roles.

Controles físicos:

- Garantizar que los dispositivos ubicados en laboratorios de cómputo y aulas virtuales cuenten con medidas de acceso restringido, a fin de evitar usos no autorizados.
- Implementar medidas de seguridad en las redes Wi-Fi institucionales para prevenir accesos indebidos y ataques de intermediario (Man-in-the-Middle, MITM).

Controles tecnológicos:

- Aplicar mecanismos de cifrado a las bases de datos académicas para proteger la información sensible.
- Implementar firewalls y sistemas de detección de intrusos para evitar accesos no autorizados a la red institucional.
- Asegurar que todos los dispositivos conectados a la red educativa cuenten con protección contra malware y se mantengan actualizados frente a vulnerabilidades.

ISSN: 2015-5392

2. Implementación en oficinas centrales de la organización educativa

Las oficinas centrales de una organización educativa tienen un enfoque predominantemente administrativo y estratégico, lo que exige controles más estrictos para la protección de la información institucional. La aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en este entorno incluye:

Controles organizacionales:

- Implementar políticas de seguridad para la gestión de datos en plataformas como ERP, LMS y sistemas de nómina.
- Cumplir con las leyes de protección de datos, como el GDPR o la normativa local, para evitar sanciones legales.
- Establecer un comité de seguridad encargado de supervisar el cumplimiento del SGSI y promover su mejora continua.

Controles relacionados con las personas:

- Aplicar programas de concienciación en ciberseguridad dirigidos al personal administrativo, con énfasis en la prevención de fraudes y filtraciones de información.
- Definir políticas de acceso a documentos administrativos sensibles, asegurando que solo el personal autorizado pueda consultarlos.

Controles físicos:

- Implementar medidas de seguridad en servidores y centros de datos para evitar accesos no autorizados.
- Utilizar sistemas de videovigilancia y control de acceso con credenciales biométricas.

Controles tecnológicos:

- Aplicar cifrado AES-256 en documentos críticos, como contratos, registros financieros y planes estratégicos.
- Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades en la infraestructura digital.

Aplicación del marco NIST en el entorno educativo

El National Institute of Standards and Technology (NIST), organismo del Departamento de Comercio de los Estados Unidos, desarrolla estándares, directrices y buenas prácticas para diversos sectores. En el contexto de la seguridad de la información, se recomienda la aplicación de las guías NIST SP 800-53 (controles de seguridad para sistemas de información) y NIST SP 800-30 (análisis de riesgos).

La aplicación adaptada de la NIST 800-53 requiere un enfoque detallado. Se inicia con la gestión de riesgos, que incluye la adopción del Risk Management Framework (RMF), el cual promueve un enfoque sistemático para evaluar y mitigar amenazas. Dentro de este marco, la evaluación de riesgos (RA) permite identificar activos críticos y analizar las vulnerabilidades asociadas.

La NIST 800-53 propone 20 familias de controles y destaca varios de ellos como fundamentales para una política de seguridad eficaz:

- Control de acceso (AC): Debe implementarse la autenticación multifactor (MFA) en todos los entornos donde se requiera autenticación, siendo de uso obligatorio. Además, se deben controlar los privilegios y accesos mediante una gestión basada en roles, así como realizar supervisión y auditoría del acceso a información crítica, asegurando que únicamente los usuarios autorizados puedan acceder a ella.
- Gestión de identidad y autenticación (IA): Es esencial el uso de contraseñas seguras y autenticación robusta, junto con la implementación de una infraestructura de clave pública (PKI). Asimismo, se debe restringir el acceso a usuarios no autorizados, especialmente en oficinas centrales y regionales.
- Monitoreo, auditoría y rendición de cuentas (AU): Es de suma importancia registrar y auditar los eventos de seguridad críticos, implementar un sistema de gestión de información y eventos de seguridad (SIEM) para una respuesta inmediata ante incidentes, y garantizar la notificación y mitigación oportuna. La estructura institucional requiere segmentación por regiones, con controles auditables y supervisión de eventos. Para ello, deben crearse puestos de vigilancia regional o establecer una red nacional que permita la vigilancia centralizada.
- Protección de la integridad del sistema y la información (SI): Se recomienda el uso de soluciones antimalware, la prevención de ejecución de código malicioso, el monitoreo de la integridad de archivos críticos y la segmentación de redes para reducir el impacto de posibles ataques. En este apartado, se hace evidente la necesidad de una homogenización organizacional mediante una política que estandarice el uso de software institucional, con el fin de coordinar la prevención y erradicación de amenazas.

- Respuesta a incidentes (IR): Es fundamental desarrollar un plan de respuesta a incidentes, realizar simulacros regulares y asegurar una comunicación efectiva, así como una rápida recuperación de los sistemas afectados. Este punto requiere entrenamiento y capacitación del personal a nivel nacional sobre cómo actuar y comunicarse adecuadamente frente a eventos adversos, especialmente porque muchos incidentes deben ser atendidos por el MICITT.
- Seguridad en la cadena de suministro (SR): La evaluación de proveedores y terceros desde una perspectiva de seguridad, la implementación de controles para la protección de datos en la cadena de suministro, y la verificación de software y hardware para evitar ataques de tipo "puerta trasera" son pasos esenciales. En este punto, debe fortalecerse la aplicación de la Ley 8968 para proteger a los clientes internos y externos, evitando la filtración de información. Además, se debe proteger la cadena de suministro, particularmente en el caso del MEP, que contrata múltiples servicios a proveedores. Toda junta administrativa o entidad que maneje fondos públicos debe regirse por la Ley 9986, Ley General de Contratación Pública.
- Protección de datos y privacidad (PT): Se debe aplicar cifrado tanto en datos en reposo como en tránsito, utilizar controles que minimicen la exposición de información personal e implementar medidas de privacidad desde el diseño, con el objetivo de preservar la confidencialidad e integridad de los datos. Es trascendental fortalecer la conciencia institucional sobre la Ley 8968 y el tratamiento de datos personales, especialmente en lo relativo a expedientes del personal, información financiera de becas y comedores escolares, datos médicos, adecuaciones curriculares y casos de alta dotación. Además, se recomienda estandarizar, mediante un acuerdo institucional, que todo dispositivo adquirido cuente con cifrado y funciones biométricas de fábrica.

Implementación de una política de seguridad

Para una política de seguridad eficaz, se deben establecer normas de acceso basadas en roles y niveles de seguridad, desarrollar planes de respuesta a incidentes con procedimientos claros, ofrecer capacitación continua en ciberseguridad para sensibilizar y formar al personal, y mantener un sistema de monitoreo y auditoría constante para revisar registros (logs), controlar el acceso a los datos y detectar posibles anomalías. Asimismo, es esencial que todos los proveedores y contratistas cumplan con los estándares de seguridad establecidos.

Análisis de riesgos: NIST 800-30 y marco normativo costarricense

Otro elemento fundamental es el análisis de riesgos, donde entra en juego la guía NIST 800-30. No obstante, en el contexto costarricense, debe considerarse la Ley Nacional de Emergencias y Prevención del Riesgo Nº 8488, así como normativa complementaria relevante, con el objetivo de unificar criterios que permitan establecer un enfoque coherente en la construcción de un entorno digital seguro.

La seguridad de la información en centros educativos y oficinas administrativas constituye un pilar esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos. El documento NIST 800-30 proporciona un marco sólido para la evaluación de riesgos en sistemas de información, lo que permite la implementación de controles efectivos para prevenir incidentes de ciberseguridad. A su vez, documentos clave como la Política Nacional de Gestión del Riesgo 2016–2030, el Plan Nacional de Gestión del Riesgo 2021–2025 y la Estrategia de Gestión del Riesgo de Desastres en el Sector Educativo 2022–2026 subrayan la necesidad de fortalecer la resiliencia digital en las instituciones educativas y administrativas del país.

Se presentan así los principales elementos aplicables en materia de seguridad de la información y ciberseguridad en entornos educativos, con el fin de garantizar la protección de datos, la continuidad de los servicios institucionales y la consolidación de una cultura de seguridad digital.

1. Gestión de riesgos en la seguridad de la información

La NIST 800-30 enfatiza la importancia de la gestión de riesgos como punto de partida para cualquier estrategia de ciberseguridad. En los ámbitos educativo y administrativo, esto implica:

- Identificación de activos críticos: Sistemas de gestión del aprendizaje (LMS), bases de datos de estudiantes y docentes, plataformas de comunicación interna y externa, servidores de documentos y redes institucionales.

ISSN: 2015-5392

- Análisis de amenazas: Desde ataques de phishing y malware, hasta suplantación de identidad y accesos no autorizados a datos sensibles.
- Evaluación de vulnerabilidades: Infraestructura desactualizada, contraseñas débiles, falta de segmentación de redes y ausencia de autenticación multifactor.
- Determinación del impacto potencial: Un ciberataque puede comprometer registros académicos, exponer datos personales y paralizar sistemas administrativos esenciales.
- Estrategias de mitigación: Implementación de cifrado, realización de copias de seguridad periódicas y monitoreo en tiempo real de amenazas.

2. Protección de infraestructura crítica en entornos educativos

Los centros educativos y oficinas administrativas manejan grandes volúmenes de información sensible, por lo que es esencial contar con una infraestructura tecnológica segura y resiliente. Se recomienda lo siguiente:

- Segmentación de redes: Separar las redes académicas, administrativas y de acceso público para evitar intrusiones no autorizadas.
- Cifrado de datos: Proteger las bases de datos mediante algoritmos de cifrado robustos que resguarden la información confidencial.
- Uso de firewalls y sistemas de prevención/detección de intrusiones (IPS/IDS): Controlar y monitorear el tráfico de red para detectar y bloquear actividades sospechosas.
- Autenticación multifactor (MFA): Reforzar el acceso a plataformas digitales mediante la utilización de credenciales adicionales.
- Actualización y parcheo de sistemas: Mantener el software y el hardware al día para prevenir la explotación de vulnerabilidades.

3. Concienciación y capacitación en ciberseguridad

Uno de los eslabones más débiles en la seguridad de la información es el factor humano. Por ello, es fundamental fomentar una cultura de ciberseguridad en la comunidad educativa y administrativa mediante:

- Capacitaciones regulares: Sensibilizar a docentes, estudiantes y personal administrativo sobre amenazas como phishing, ingeniería social y malware.
- Políticas de uso responsable de dispositivos y redes: Establecer normativas claras para el uso adecuado de dispositivos personales en entornos institucionales.
- Ejercicios de simulación de ataques: Realizar pruebas de phishing y simulacros de respuesta ante incidentes para evaluar la preparación de los usuarios.
- Gestión de accesos y permisos: Aplicar el principio de mínimo privilegio, limitando el acceso a información sensible únicamente a usuarios autorizados.

4. Planes de continuidad y respuesta ante incidentes

Documentos clave de gestión del riesgo en Costa Rica, como el Plan Nacional de Gestión del Riesgo 2021–2025, destacan la importancia de contar con estrategias de respuesta y recuperación ante incidentes de seguridad informática. Para ello, se deben establecer:

- Planes de respuesta ante incidentes: Procedimientos estructurados para identificar, contener, erradicar y recuperar los sistemas afectados por ciberataques.
- Copias de seguridad periódicas: Implementación de backups en servidores físicos y en la nube, con políticas claras de recuperación.
- Centros de operaciones de seguridad (SOC): Monitoreo en tiempo real de eventos de ciberseguridad para detectar y mitigar ataques de manera proactiva.
- Simulacros de ciberataques y desastres tecnológicos: Evaluar la capacidad de respuesta de la institución frente a eventos críticos.

ANÁLISIS: POLÍTICA DE CIBERSEGURIDAD DEL MEP

Este proceso pretende generar debate y concienciar sobre los elementos débiles o ausentes en la política de ciberseguridad y seguridad de la información del MEP. Con el fin de facilitar su comprensión y sistematizar la información, esta se ha condensado de la siguiente manera:

Categoría	Debilidad o Inconsistencia	Impacto Potencial
Inconsistencias Técnicas	Falta de especificidad en la implementación de medidas técnicas	Implementaciones ineficaces que dejan vulnerabilidades abiertas
Inconsistencias Técnicas	Ausencia de un enfoque basado en riesgos	No hay un método claro para evaluar y mitigar amenazas
Inconsistencias Técnicas	No se integra con estándares internacionales como ISO 27001 o NIST	Falta de alineación con estándares globales, lo que reduce la efectividad
Inconsistencias Técnicas	Autenticación multifactor (MFA) opcional en lugar de obligatoria	Mayor riesgo de accesos no autorizados a sistemas críticos
Inconsistencias Técnicas	No se menciona el cifrado de extremo a extremo para comunicaciones y almacenamiento	Mayor exposición a ataques de intercepción y robo de datos
Gestión y Cumplimiento	No se especifican sanciones claras en caso de incumplimiento	Falta de disuasión y cumplimiento deficiente de la política
Gestión y Cumplimiento	Falta de monitoreo continuo y respuesta a incidentes en tiempo real	Las amenazas pueden no detectarse a tiempo, aumentando el daño
Gestión y Cumplimiento	No se detallan mecanismos de auditoría y control de cumplimiento	Falta de supervisión efectiva que permita verificar el cumplimiento
Gestión y Cumplimiento	No hay un plan de continuidad del negocio ni recuperación ante desastres	Institución vulnerable a interrupciones prolongadas por ataques
Gestión y Cumplimiento	Falta de requerimientos estrictos de seguridad en la contratación de terceros	Proveedores pueden representar una puerta de entrada a ataques
Operativos y educativos	Capacitación insuficiente en ciberseguridad para funcionarios	Usuarios mal preparados pueden ser el punto débil en la seguridad
Operativos y educativos	No hay estrategias concretas contra ataques de ingeniería social (phishing)	Mayor exposición a fraudes y engaños dirigidos a funcionarios
Operativos y educativos	No se establecen controles claros para el uso de dispositivos personales (BYOD)	Riesgo de filtración de datos por falta de control sobre dispositivos externos
Operativos y educativos	Definición ambigua de responsabilidades entre distintas direcciones del MEP	Dificultad en la aplicación de la política por falta de claridad en roles
Operativos y educativos	No se establece un proceso de actualización periódica de la política	Riesgo de que la política quede obsoleta frente a nuevas amenazas

Fuente de elaboración propia

ISSN: 2015-5392

1. Ausencia de especificidad técnica

Por lo expresado anteriormente, se puede afirmar que la política presenta vacíos significativos en la implementación técnica de seguridad. Aunque se mencionan herramientas fundamentales como firewalls e IDS/IPS, no se establecen parámetros específicos para su implementación efectiva. La ausencia de estándares mínimos y protocolos de actualización compromete la solidez del sistema de seguridad.

Impacto

Esta falta de especificidad técnica puede derivar en:

- Implementaciones inconsistentes entre departamentos.
- Dificultad para evaluar el cumplimiento de las medidas de seguridad.
- Vulnerabilidades potenciales debido a la inexistencia de estándares claros.

Recomendaciones de mejora

- Es necesario desarrollar un anexo técnico que especifique:
- Estándares mínimos para las configuraciones de seguridad.
- Protocolos detallados de implementación y mantenimiento.
- Integración con marcos de referencia internacionales como ISO/IEC 27001 y NIST.

2. GESTIÓN DE RIESGOS Y CUMPLIMIENTO

La política carece de una metodología estructurada para la gestión de riesgos y no establece mecanismos claros de cumplimiento ni de rendición de cuentas (accountability). La falta de sanciones específicas y de procesos de auditoría debilita su capacidad de aplicación.

Impacto

Estas carencias generan:

- Dificultad para priorizar recursos y esfuerzos en materia de seguridad.
- Ambigüedad en cuanto a las consecuencias por incumplimiento.
- Imposibilidad de medir eficazmente el nivel de seguridad.

Recomendaciones de mejora

Se recomienda incorporar:

- Una metodología detallada de evaluación y gestión de riesgos.
- Un régimen de sanciones específico y gradual.
- Procedimientos de auditoría con plazos y métricas claramente definidos.

3. Respuesta a incidentes y continuidad operativa

La política no contempla de forma adecuada la gestión de incidentes ni la continuidad operativa. Se carece de un framework integral para el manejo de crisis y la recuperación ante desastres.

Impacto

Esta omisión puede traducirse en:

- Respuestas desorganizadas frente a incidentes de seguridad.
- Tiempos de recuperación prolongados.
- Pérdida potencial de datos críticos.

Recomendaciones de mejora

Es imprescindible desarrollar:

- Un plan detallado de respuesta ante incidentes.
- Protocolos de continuidad del negocio con asignación clara de roles.
- Procedimientos de recuperación ante desastres con tiempos objetivos definidos.

4. Factor humano y capacitación

La política subestima el papel del factor humano en la seguridad de la información. La ausencia de programas estructurados de capacitación y concienciación representa un riesgo considerable.

Impacto

Estas deficiencias pueden provocar:

- Mayor exposición a ataques de ingeniería social.
- Comportamientos inseguros por parte del personal.
- Incidentes de seguridad derivados del error humano.

Recomendaciones de mejora

Es esencial implementar:

- Programas obligatorios de capacitación con evaluaciones periódicas.
- Simulacros regulares de ataques de phishing.
- Políticas claras sobre el uso de dispositivos personales.

5. Falta de control sobre los datos personales

En años anteriores, se han presentado incidentes relacionados con el manejo de datos personales en el MEP. Parte de esta situación se ve reflejada en las omisiones y debilidades de la política actual

Problema identificado	Impacto potencial
Falta de aplicación de la Ley 8968 en la política de ciberseguridad	Riesgo legal y posibles sanciones por incumplimiento de la legislación de protección de datos
No se establecen mecanismos claros para la recolección, tratamiento y almacenamiento de datos personales	Vulnerabilidad ante filtraciones y mal uso de información personal
No se garantiza el derecho a la autodeterminación informativa conforme a la Ley 8968	Falta de transparencia y confianza en el manejo de información de estudiantes y funcionarios
No se definen procesos de consentimiento informado para el tratamiento de datos	Riesgo de demandas o denuncias por uso indebido de datos personales
No se especifican medidas de seguridad para la protección de datos personales	Mayor exposición a ataques y fugas de información sensible
No se aborda el derecho de acceso, rectificación y eliminación de datos personales	Usuarios sin herramientas para corregir o eliminar sus datos de sistemas del MEP
No se establecen lineamientos sobre la transferencia de datos a terceros	Riesgo de transferencia inadecuada de datos a empresas o terceros sin control
No se menciona la anonimización de datos como una práctica obligatoria	Exposición innecesaria de información sensible que podría ser usada de manera malintencionada
No se prevén sanciones o medidas disciplinarias por incumplimiento en la protección de datos	Ausencia de consecuencias fomenta el incumplimiento de buenas prácticas en protección de datos
No se especifica un ente responsable de velar por el cumplimiento de la Ley 8968 dentro del MEP	No hay un equipo o departamento específico que garantice la correcta aplicación de la normativa

ISSN: 2015-5392

La política actual presenta graves omisiones en relación con el cumplimiento de la Ley 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales. No se establecen mecanismos fundamentales para garantizar la protección de los datos ni se designan responsables claros para su implementación.

1. Impacto legal

La falta de alineación con la Ley 8968 expone al MEP a:

- Sanciones legales y administrativas.
- Vulnerabilidad ante demandas por el mal manejo de datos.
- Incumplimiento de obligaciones constitucionales en materia de autodeterminación informativa.

Recomendaciones normativas

Es necesario implementar:

- Un marco específico de cumplimiento de la Ley 8968.
- La designación de un oficial de protección de datos.
- Procedimientos claros para el ejercicio de derechos ARCO.

2. Gestión de datos personales

La política carece de procedimientos específicos para:

- La recolección y el tratamiento de datos personales.
- Procesos de consentimiento informado.
- Mecanismos de anonimización de información sensible.

Impacto operativo

Estas carencias resultan en:

- Riesgo de filtración de información personal.
- Falta de transparencia en el manejo de datos.
- Vulnerabilidad ante usos no autorizados de información.

Recomendaciones de mejora

Debe establecerse:

- Protocolos detallados para la recolección y tratamiento de datos.
- Sistemas formales de consentimiento informado.
- Procedimientos obligatorios de anonimización.

3. Derechos de las personas titulares de datos

La política no contempla adecuadamente:

- Mecanismos para ejercer derechos ARCO.
- Procedimientos de rectificación de datos.
- Protocolos de eliminación de información personal.

Impacto en los usuarios

Esta omisión afecta:

- La capacidad de las personas usuarias para controlar su información.
- La transparencia en el tratamiento de los datos.
- La confianza en los sistemas del MEP.

Recomendaciones de implementación

Es necesario desarrollar:

- Plataformas para el acceso y gestión de datos personales.
- Procedimientos claros de rectificación y actualización.
- Sistemas eficaces de eliminación de información.

4. Transferencia y seguridad de los datos

La política no establece:

- Lineamientos para la transferencia de datos a terceros.
- Requisitos de seguridad específicos para la información personal.
- Controles efectivos sobre el acceso a datos sensibles.

Impacto en la seguridad

Estas carencias generan:

- Riesgos en la transferencia indebida de datos.
- Accesos no autorizados a información confidencial.
- Exposición innecesaria de datos sensibles.

Recomendaciones de seguridad

Debe implementarse:

- Protocolos para la transferencia segura de datos.
- Controles de acceso granulares y auditables.
- Sistemas de monitoreo y auditoría continua.

5. Responsabilidad y cumplimiento

La política carece de:

- Asignación clara de responsabilidades.
- Sanciones específicas por incumplimiento.
- Mecanismos de supervisión y control efectivos.

Impacto institucional

Esta situación se traduce en:

- Falta de responsabilidad concreta.
- Dificultad para implementar medidas correctivas.
- Riesgo de incumplimiento sistemático.

Recomendaciones estructurales

Es fundamental establecer:

- Un comité institucional de protección de datos.
- Un régimen sancionatorio específico.
- Un sistema regular de auditoría y supervisión.

CONCLUSIONES

La política de ciberseguridad del MEP se presenta como un documento carente de sentido práctico, cuya estructura refleja una profunda desconexión entre su propósito declarado y la realidad de la gestión de la seguridad de la información. Aunque en su redacción se incluyen principios generales y terminología técnica propia del ámbito, la ausencia de lineamientos concretos, mecanismos de control y estrategias efectivas de implementación la convierten en un instrumento vacío, destinado más a cumplir con un requisito burocrático que a ofrecer una guía real para la protección de la información y de la infraestructura tecnológica de la institución.

Desde una perspectiva crítica, resulta evidente que este documento no solo carece de coherencia interna, sino que también incurre en una omisión grave respecto al cumplimiento de marcos normativos fundamentales, como la Ley 8968. La recolección, tratamiento, almacenamiento y eliminación de datos personales no están regulados de forma adecuada, lo que deja a estudiantes y funcionarios expuestos a un manejo arbitrario y potencialmente riesgoso de su información. La ausencia de medidas concretas de anonimización, transparencia en la gestión de datos y mecanismos de fiscalización eficaces abre la puerta a vulneraciones de derechos fundamentales, sin un protocolo claro de prevención o mitigación.

Una política de ciberseguridad sin ciberseguridad

El documento falla en cumplir con su propósito central: proteger la información y garantizar la resiliencia tecnológica del MEP. No se identifican mecanismos concretos para la detección, respuesta y recuperación ante incidentes de seguridad. No existe un sistema de monitoreo continuo ni una estrategia clara de auditoría, lo que deja a la institución en un estado de vulnerabilidad permanente. Más allá de un enunciado de intenciones, la falta de procedimientos operativos convierte esta política en un texto sin impacto real en la prevención de ciberataques.

Las experiencias recientes de ataques a instituciones gubernamentales en Costa Rica han demostrado la fragilidad de las infraestructuras digitales y la urgente necesidad de contar con estrategias robustas y bien definidas. No obstante, esta política ignora esas lecciones y no establece medidas concretas para evitar que eventos como los sufridos por el Ministerio de Hacienda, la Caja Costarricense de Seguro Social (CCSS) y otras entidades públicas se repitan. La omisión de controles estrictos de acceso, la falta de un plan detallado de continuidad del negocio y la inexistencia de protocolos ante ciberataques refuerzan la percepción de que este documento no representa un esfuerzo serio por fortalecer la seguridad institucional.

El peligro de convertirse en un documento burocrático

Más allá de sus deficiencias técnicas, la mayor amenaza que representa esta política es su destino previsible: convertirse en un documento de referencia que nadie consulta ni aplica; un archivo más en la maraña burocrática, incapaz de generar cambios reales en la cultura organizacional. La ausencia de sanciones por incumplimiento y de mecanismos efectivos de rendición de cuentas fomenta una cultura de indiferencia, donde la ciberseguridad se reduce a un formalismo sin impacto.

Finalmente, el documento omite un componente esencial: la formación y concienciación de las personas usuarias. Sin una estrategia clara y sostenida de educación en ciberseguridad, cualquier esfuerzo técnico resulta insuficiente. La protección de la información no depende únicamente de herramientas digitales, sino del comportamiento de quienes las utilizan. La falta de programas de formación robustos, continuos y obligatorios evidencia una visión limitada, que deja tanto al personal como al estudiantado sin la preparación necesaria para identificar y mitigar amenazas reales.

ISSN: 2015-5392

Hacia una revisión urgente y una transformación real

La falta de sustancia y aplicabilidad de esta política no solo representa un riesgo institucional, sino que también evidencia una preocupante falta de compromiso con la protección de la información y la seguridad digital de la comunidad educativa. Es imperativo replantear este documento desde una perspectiva que priorice la acción, la eficacia y la adaptabilidad a las amenazas emergentes. Para lograrlo, se deben considerar los siguientes aspectos fundamentales:

Aplicación efectiva de la Ley 8968: Se deben establecer mecanismos de cumplimiento claros para la protección de datos personales, garantizando el derecho de autodeterminación informativa de los estudiantes y funcionarios.

Implementación de medidas de seguridad obligatorias: La autenticación multifactor debe ser un requisito en todos los sistemas críticos, y el cifrado de extremo a extremo debe ser un estándar mínimo.

Monitoreo continuo y respuesta a incidentes: Es necesario establecer un centro de operaciones de seguridad (SOC) que permita la detección y mitigación temprana de amenazas.

Sanciones claras por incumplimiento: El documento debe incluir penalizaciones para quienes no sigan las normativas establecidas, evitando así la impunidad y la negligencia en la gestión de la seguridad.

Educación y cultura de ciberseguridad: Sin una estrategia de capacitación real, la política seguirá siendo ineficaz. Es necesario invertir en formación continua para toda la comunidad educativa.

Auditorías y revisiones periódicas: Se deben establecer mecanismos de auditoría interna y externa para garantizar que las medidas de seguridad sean efectivas y actualizadas ante nuevas amenazas.

La seguridad de la información no es un tema opcional ni secundario; es una necesidad urgente en un mundo cada vez más digitalizado y expuesto a riesgos tecnológicos de gran impacto. La inacción en este campo no solo compromete la integridad de los datos institucionales, sino que también pone en peligro la confianza en el sistema educativo y la seguridad de miles de estudiantes y funcionarios. Es momento de que el MEP deje de lado las políticas vacías y adopte un enfoque serio, técnico y aplicable en la gestión de la ciberseguridad.

REFERENCIAS

Ministerio de Educación Pública. (2019). *Acerca del MEP*. https://dgth.mep.go.cr/sobre-el-mep/

Moreno Guerra, C. B. (2019). Seguridad de la información para instituciones educativas a tercer nivel basado en la ISO/IEC 27001. *Revista Caribeña de Ciencias Sociales*. https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html

Purpura, P. (2006). *Manual de capacitación para personal de seguridad*. Thomson Learning.

Sibaja, D. (2024, 26 de febrero). MEP cerró 180 escuelas en los últimos 10 años. *Teletica*. https://www.teletica.com/calle-7/mep-cerro-180-escuelas-en-los-ultimos-10-anos_352595

DIGITAL TWINS AND THEIR APPLICATIONS IN THE INDUSTRY: A SYSTEMATIC LITERATURE REVIEW

(GEMELOS DIGITALES Y SUS APLICACIONES EN LA INDUSTRIA: UNA REVISIÓN SISTEMÁTICA DE LITERATURA)

Dr. Juan Carlos Sandí-Delgado
Informático, Profesor Catedrático, UCR. JUAN.SANDIDELGADO@ucr.ac.cr
Mag. Steven Cruz-Sancho
Informático, Académico Campus Sarapiquí, UNA. STEVEN.CRUZS.ANCHO@una.cr
Bach. Samuel Jones-Chaves
Informático, estudiante Universidad de Costa Rica. SAMUEL.JONES@ucr.ac.cr
Bach. Xavier Gómez-López
Informático, estudiante Universidad de Costa Rica. XAVIER.GOMEZ@ucr.ac.cr

ABSTRACT:

Digital twin technology enables the creation of simulated representations of physical entities through simulations and predictions, which can help reduce costs and improve production in industrial settings. This technology is based on key aspects of Industry 4.0, such as Artificial Intelligence, the Internet of Things, and Big Data. This research aims to analyze the implementation of digital twins, their development, and their level of support within the industry. A systematic literature review was conducted on digital twins and their industrial applications, following a previously established review protocol. The results identified a set of fundamental components and technologies required for the implementation of digital twins in industry, as well as the extent of their use in manufacturing. It was concluded that Artificial Intelligence plays a fundamental role in the functioning of digital twins, and the potential benefits of incorporating this technology into the medical field were also highlighted.

Keywords: Digital twins, Industry 4.0, Artificial Intelligence, Internet of Things, Big Data.

RESUMEN:

La tecnología de los gemelos digitales permite la creación de representaciones simuladas de entidades físicas mediante simulaciones y predicciones, lo que podría contribuir a la reducción de costos y a la mejora de la producción en las industrias. Esta tecnología se basa en aspectos característicos de la Industria 4.0, como la inteligencia artificial, el Internet de las Cosas y el Big Data. El objetivo de esta investigación es analizar las implementaciones de los gemelos digitales, su desarrollo y su grado de adopción en la industria. Se llevó a cabo una revisión sistemática de la literatura relacionada con los gemelos digitales y sus aplicaciones en el ámbito industrial, conforme a un protocolo de revisión previamente establecido.

Los resultados permitieron identificar una serie de componentes y tecnologías fundamentales necesarias para la implementación de los gemelos digitales en la industria, así como la magnitud de su participación en el área de la manufactura. Se determinó que la inteligencia artificial es una parte esencial para el funcionamiento de los gemelos digitales, y se destacó la relevancia de su incorporación en el campo de la medicina.

Palabras clave: Gemelos digitales, Industria 4.0, inteligencia artificial, Internet de las Cosas, Big data.

I. INTRODUCTION

A digital twin (DG) can be understood as a virtual representation of a physical entity that enables simulations and the prediction of events [1]. The concept has been broadly defined by various researchers [2, 1, 3, 7], which has led to variations in its interpretation depending on the researcher and their field of expertise. This variability has also contributed to confusion with related technologies, such as digital models and digital shadows [1].

The main difference between DGs, digital models, and digital shadows lies in the nature of data connection and transmission. Digital models do not require automatic or continuous data processing from the physical model, serving only as static representations of a physical product. In contrast, a digital shadow is based on a physical object whose state must update in response to changes in that object; therefore, it typically involves a continuous one-way flow of data from the physical entity to its virtual counterpart. In summary, a DG differs significantly from these other technologies due to its requirement for two-way data exchange between the physical entity and its digital representation [2, 1].

It is important to examine DG implementation, as it has demonstrated numerous benefits across various fields. Industry, in particular, has gained significantly from DGs due to their potential to maximize economic returns while reducing costs [1]. Consequently, the inclusion of DGs in industrial settings is essential: when implemented correctly, they can profoundly impact efficiency at both national and international levels by improving process effectiveness.

II. THEORETICAL FRAMEWORK

This section will explain some of the essential concepts related to DG. Likewise, the information presented is important for answering RQ1 and RQ2, which are described in detail in the methodology section. Therefore, the definition of the concept of DG, its characteristics, and the implications of implementing this technology are discussed.

2.1 DG (RQ1)

The concept of DG is generally attributed to Professor Grieves at the University of Michigan in 2003, who described it as the virtual representation of a physical object and its associated information. He also stated that DGs are composed of three parts: a physical product, its virtual representation, and a bidirectional connection, this last component enabling constant information exchange between the physical and virtual parts [8].

The development of DG has contributed to the advancement of other Industry 4.0 technologies, such as Big Data, Artificial Intelligence, and the Internet of Things. This has enabled DGs to go beyond simple simulations of “real-world” products and, today, take on functions such as predicting future events and even providing solutions to potential failures. This is made possible by the application of Artificial Intelligence in DGs, which allows for the continuous exchange of data between the physical object or entity and its digital counterpart [9, 11].

Table 1 presents the characteristics or common elements identified in various definitions of DG.

Based on the characterizing aspects found in the different definitions reviewed in the systematic literature review, along with the characteristics summarized in Table 1, we propose the following definition of DG: a DG can be understood as a real-time virtual representation of a physical entity or process which, through technologies such as Artificial Intelligence, Big Data, and the Internet of Things, enables simulations and predictions of that physical entity.

Table 1. Characteristics of DGs according to the referenced authors.

Reference	Integration of technologies related to the Industry 4.0	Prediction function	Simulation function
[12]	×	✓	×
[9]	✓	✓	✓
[2]	×	×	✓
[8]	✓	×	✓
[1]	×	✓	✓
[13]	✓	✓	✓
[3]	✓	×	✓
[4]	✓	✓	✓
[14]	✓	✓	✓
[15]	×	×	✓
[16]	✓	×	✓
[17]	✓	✓	×
[18]	×	✓	✓
[19]	✓	✓	✓
[20]	×	×	✓

2.2 Characteristics of DGs

Various studies [9, 8, 21] have identified and described a number of characteristics associated with DGs, which have been classified into the following categories:

2.2.1 Entities and Environments

The entities and environments that make up DGs are divided into two main groups: those considered virtual and those belonging to the physical world [8]. That is, virtual entities are those that operate within a digital environment or serve as representations of physical objects. In this regard, it is important to clarify that, according to Professor Grieves's conceptualization of DG, a specific DG system or environment may include more than one virtual entity, each with its own functions and data records of the physical world, and these entities can interact with one another [8].

The virtual environment is the digital "space" that simulates a specific physical location in which the object or physical entity represented by the DG exists. In other words, the virtual environment acts as a mirror of the physical environment. In contrast, the physical entity is the object with tangible properties on which the DG is based. This entity does not necessarily have to be a single object; it can also be a more complex system with the necessary characteristics for digital representation, such as entire cities. For example, in the research conducted by [22], a DG was developed for the city of Dublin, Ireland.

Finally, the physical environment is the space in which the physical entity exists and interacts. Only the data necessary for the simulations performed by the DG are collected from this environment.

2.2.3 Status and Parameters

The state of a DG is defined as the condition of both the DG and its physical counterpart at a specific point in time. This state is determined using parameters, which are the types of data exchanged through the existing connection between them [8].

2.3 Implications of the Use of DGs (RQ2)

This section addresses the implications of using DGs, with a focus on identifying the associated benefits and costs of their implementation. Key considerations include the cost and duration of implementation, the development environment, and the execution process of the DG [1, 17].

The DG development and execution environment must have sensors capable of interacting in real-time with an Artificial Intelligence environment (physical–virtual) [17]. This interaction enables automated learning through data analysis, which in turn supports the optimization, monitoring, and forecasting functions of the DG.

It is necessary to mention that, given the vast amount of data generated by DGs, as well as those necessary for their creation and feedback, it is required to use Artificial Intelligence to improve the efficiency of data flow, allowing to identification of faults and quality defects on the digitally generated object.

The cost of implementing a DG is significant, as it requires personnel with specific competencies for developing the working environment and carrying out the implementation [1]. However, although the initial investment can be high, this cost tends to decrease over time. Once the DG is properly implemented, it enables cost savings by reducing the need for physical prototypes, allowing early identification of potential failures and quality defects, and supporting variations in production and functionality to achieve optimal design. These advantages of DGs help reduce both resource use and development time, as the creation of a physical prototype becomes unnecessary [5].

The development of a DG is a process that requires time. It is long and complex, as it must be guided, operated, and optimized in conjunction with various software tools, including those needed for Big Data analysis, as well as reliable sensor technology for data collection, processing, and interpretation. Therefore, ensuring synchronization between the DG and the physical environment is essential [17].

Consequently, although DGs are complex to implement due to the factors mentioned above, they can represent a significant improvement in modern industry, as noted by researchers [15, 17]. Their use can lead to increased productivity, improved efficiency, higher quality, and cost reduction in industries or companies that adopt them. However, it is also recognized that DGs are not always suitable, as they may introduce additional complexity into production and development processes.

III. RELATED WORK

The systematic literature review made it possible to identify research works related to the application of DGs in industry, where the benefits and challenges of including this technology in the area are evidenced. In this sense, primary works that address the topic under study and allow answering RQ3 are examined.

In Spain, a study was conducted involving the development of a DG for a workstation dedicated to assembling parts produced through 3D printing [14]. The project followed several key steps, including the modeling of the station, the creation of an automation project, and the integration of the system into Industry 4.0-related architectures. Ultimately, a physical workstation was built based on the data and insights obtained from the DG developed during the study.

Other researchers in Spain generated a DG that allows to manage processes within an industrial laundry facility [23]. The study involved the creation of a model aimed at supporting decision-making, with linen processing as the primary operational focus. The DG provided relevant information to enhance production efficiency. The system's outputs closely aligned with the decisions typically made by human experts, demonstrating the potential of DGs to support and even automate decision-making processes.

Researchers from Canada and Pakistan implemented a DG to optimize the performance of the 5G network by creating a neural network that could predict the variable behavior of the network. This allows real-time monitoring and data collection, which were then fed into the neural network to facilitate autonomous network management. As a result, the system was able to accurately estimate network dynamics and support effective segmentation, ultimately leading to a near-optimal management policy.

In China, researchers conducted a study on DGs and intelligent manufacturing that has received increased attention due to the rise of Industry 4.0 technologies [15]. The study found that the use of DGs in advanced manufacturing enhances operational efficiency and enables the prediction of production failures, thereby supporting the implementation of preventive measures to reduce their impact.

In summary, it is evident that the implementation of DG has been promoted internationally, particularly in Europe, Asia, and North America. However, the primary studies analyzed do not provide evidence of the specific aspects that should be considered for its application in industry, revealing a gap in the literature that this study seeks to address.

IV. METHODOLOGY

This section describes how the information supporting the research was obtained and processed, from the research approach to the results obtained with the selection processes. Section 4.1 presents the approach used in the research, followed by a description of the study population in section 4.2. Finally, section 4.3 describes the data collection techniques, the inclusion and exclusion criteria for selecting primary sources, and the preliminary and final selection processes.

4.1 Research Approach

This research adopts a qualitative approach based on how the data were obtained and subsequently analyzed. The primary studies were examined through a systematic literature review, using the protocol established by Kitchenham as a reference [25]. This process enabled the identification of relevant information about DGs and their applications in the industry, addressing three research questions: RQ1. How has the term "DG" been defined and characterized? RQ2. What are the implications of implementing a DG? and RQ3. In what ways have DGs been applied in the industry, and what are the antecedents in this regard? These research questions supported the objective of the study, which is to define DGs and demonstrate their applications in the industrial context.

4.2 Study Population

For this research, the primary studies regarding DGs and their applications in industry constitute the study population. These documents include definitions of DGs and descriptions of how this technology has been implemented in industrial contexts.

4.3 Data Collection Technique

To locate the primary studies on DGs and their applications in industry, a search was conducted in indexed databases specializing in scientific and academic publications, such as IEEE Xplore Digital Library, ScienceDirect, and SpringerLink [26]. Keywords in both Spanish and English were used: gemelos digitales (DGs), industria (industry), and manufactura (manufacture), along with search strings combining these keywords across both languages.

4.4 Information Processing

For the processing of the information, inclusion and exclusion criteria were established for the bibliographic sources, including the following:

4.4.1 Inclusion Criteria

They are the set of criteria used to determine whether an article should be included in the literature review. These criteria are:

- Primary documents written in English or Spanish.
- Primary documents whose main topic is related to the term DGs.
- Primary papers that gather experiences or research results concerning the application of DGs in industry.
- Primary papers published between 2018 and 2022.

4.4.2 Exclusion Criteria

These are the set of guidelines that exclude an article from being contemplated in the literature review:

- Studies for which full-text access was not available.
- Studies derived from other studies.
- Papers published in journals or conference proceedings without international peer review.

4.4.3 Preliminary Selection Process

After applying the search criteria described above, a total of 156 primary studies were identified. The preliminary selection process involved analyzing the titles, abstracts, and keywords of these studies, which allowed for the exclusion of documents that were not relevant to the present research. As a result, 40 documents were selected for further review.

4.4.4 Final Selection Process

Once the results of the preliminary selection were obtained, a full reading of the identified primary studies was conducted, followed by the preparation of corresponding technical data sheets. These sheets compiled key information from each document (objectives, methodology, and results) in order to determine which studies aligned with the objective of this research. As a result, 30 documents were selected.

Of the total number of selected documents, 16 were used to address RQ1, which relates to the definition of DG. Four references contributed to answering RQ2, focused on the implications of DG implementation. Finally, 15 studies were used to address RQ3, concerning the application of DG in industry. It is important to note that some documents provided information relevant to more than one research question.

V. RESULTS

Based on the systematic literature review, several ways in which DGs have been applied across different areas of industry were identified. Therefore, this section presents an analysis organized according to the categories and criteria defined for this purpose, which are:

- A. General Aspects – This category includes criteria related to language and country of origin of the studies.
- B. Technological Aspects – This category comprises criteria for the components and technologies used to operate DG applications. The selection of these criteria is based on the contributions of relevant researchers in the area [1], [17], particularly regarding the technologies involved in DG development.
- C. Application Aspects – This category includes criteria related to the size and classification of the industries in which DGs have been implemented.

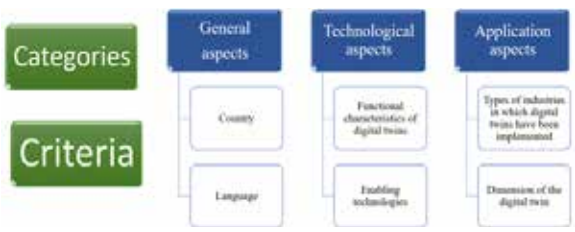


Fig. 1. Categories and criteria for analysis.

The following describes the criteria to provide a clearer understanding of the study categories.

ISSN: 2015-5392

A. General Aspects

This category includes two criteria: the country in which the DG application was developed and the language in which it was documented:

- Country – This criterion identifies the country where the DG application was developed.
- Language – This criterion refers to the language in which the DG research was published.

B. Technological Aspects

This category includes two criteria related to the components involved in DG operation and the enabling technologies used in their development:

- Enabling Technologies – This criterion refers to the technologies used to plan, develop, and implement DGs. These are typically associated with Industry 4.0, and the values considered for this criterion include Big Data, Artificial Intelligence, Internet of Things, Cyber-Physical Systems, and Machine Learning.
- Functional Characteristics of DGs – This criterion identifies the key elements that constitute a DG and are essential for its optimal functioning. Possible values include data analysis, object simulation, and self-learning.

C. Application Aspects

This category includes two criteria related to the type of industry in which DGs were implemented and the dimension or scale of the DGs:

- Types of Industries in Which DGs were Implemented – This Criterion Classifies DG Applications Based on the type of industry in which they were applied. Possible values include the food industry, manufacturing, automotive, among others.
- DG Dimension – This criterion categorizes DG applications according to the size or scope of the system, which can be classified as either a single system or a large-scale system (composite system).

The following section presents a detailed description of the results obtained through the application of each analysis criterion.

5.1 DG Applications Selected for Analysis

Based on the systematic literature review, a set of DG applications was selected for analysis to address RQ2 and RQ3. Table 2 presents the studies related to DG applications, organized by country of origin.

Table 2. Studies related to DG applications by country of origin.

Reference	Country
[12]	Spain
[9]	Spain
[2]	China
[8]	China
[1]	China
[13]	China
[3]	Finland
[4]	United States of America
[14]	Germany
[15]	China
[16]	China
[17]	Korea
[18]	China
[19]	United Kingdom
[20]	China

In the same vein, Table 3 provides a brief description of each DG application experience based on the selected primary case studies, with references to the researchers who conducted them.

Table 3. Description of DG applications according to referenced authors.

Reference	Application description
[12]	Parts assembly station with different tools and a series of established steps; simulation and integration of industrial assets.
[9]	Operations management of industrial laundry, generated from the factory study; this DG is intended to support decision-making within the factory
[2]	B5G network to perform an optimal cutting policy using neural networks and reinforcement learning.
[8]	Asset management of a sustainable smart factory to optimize processes.
[1]	Power plant to generate trend predictions, better water management, increased efficiency, and reduced emissions.
[13]	Monitoring the transformation of sea waves into renewable energy, using technologies such as neural networks to generate a prediction of the data for DG development.
[3]	Automatic generation of DGs for intelligent manufacturing systems to control automated vehicles, enabling their autonomous movement through workspaces.
[4]	Connected and automated vehicles based on the Unity graphics engine, implementing different subsystems to satisfy the different preferences of each driver.
[14]	Manufacturing production, optimization of factory processes.
[15]	Risk assessments on highways are based on the analysis of vehicle trajectories and behaviors, obtained through aerial footage captured by drones and other surveillance equipment at the sites.
[16]	Satellite assembly station, in order to improve efficiency through a real-time control of the manufacturing process assets, which allows to organize them and make predictions based on the data obtained from the physical space.
[17]	A DG based on a vertical farm is implemented to monitor the state of the crops from data obtained from devices in the physical farm.
[18]	Based on reinforcement learning techniques, the DG adopts training functions to automate intelligent production systems.
[19]	Development of a DG for a utility system of a chemical plant, which allows site personnel with data on different parameters related to plant operations. Additionally, it presents prediction functions on future failures and simulation of hypothetical cases for better preparation for these events.
[20]	Using a DG to manage vehicular traffic from network data with Edge Computing functions, which allows analyzing and predicting the state of the networks, and obtaining benefits such as reduced vehicular congestion.

5.2. Analysis of the Results Based on The Evaluation Criteria

This section presents the results of the analysis conducted on the selected DG applications, organized according to each criterion within the defined analysis categories.

A. General Aspects

Regarding the results of the analysis for the criterion related to the country in which the DG was developed, Figure 2 shows that 46.6% (7) of the references correspond to studies conducted in China. Spain accounts for 13.3% (2), while the United States, Canada, Germany, the Republic of Korea, Finland, and the United Kingdom each represent 6.6% (1). This suggests that the implementation of DG has gained greater relevance and

usage in Asia. Additionally, its growing presence can be observed in various European countries. In the Americas, initiatives are evident only in Canada and the United States.

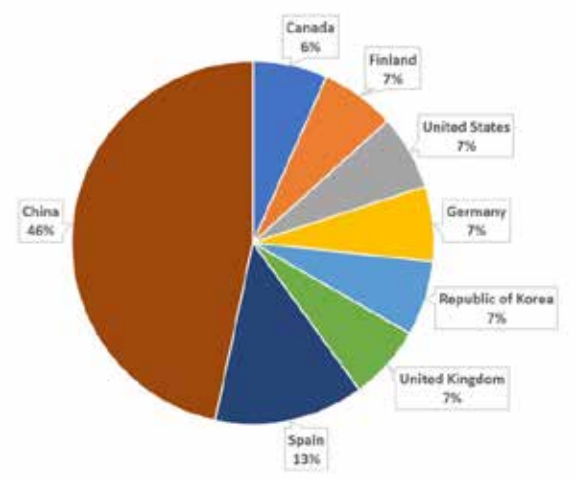


Fig. 2. Country where the DG was developed

Regarding the language criterion, Table 4 shows that 87% (13) of the analyzed applications were documented in English, while 13% (2) were in Spanish. This may be due to the fact that English is a universal language, enabling researchers to reach a broader international audience.

Table 4. Language of primary studies of DG applications

Reference	Language
[12]	Spanish
[9]	Spanish
[2]	English
[8]	English
[1]	English
[13]	English
[3]	English
[4]	English
[14]	English
[15]	English
[16]	English
[17]	English
[18]	English
[19]	English
[20]	English

B. Technological Aspects

With respect to the Enabling Technologies criterion, Table 5 shows that 87% (13) of the analyzed studies highlight the importance of implementing Artificial Intelligence in the development of DGs, followed by the use of the Internet of Things.

Table 5. Enabling technologies for the development of a DG

Reference	Big Data		Artificial intelligence	Machine Learning	Cyber-physical system
[12]	✓	✓	✓	×	✓
[9]	×	×	✓	×	×
[2]	×	×	✓	✓	×
[8]	✓	✓	✓	×	×
[1]	✓	✓	×	✓	×
[13]	✓	×	✓	×	×
[3]	×	×	✓	×	✓
[4]	×	×	✓	✓	×
[14]	×	×	✓	×	×
[15]	×	×	✓	✓	×
[16]	✓	✓	✓	✓	✓
[17]	✓	×	✓	×	×
[18]	✓	✓	✓	✓	✓
[19]	×	×	×	×	×
[20]	✓	×	✓	✓	×

As for the criterion Functional characteristics of DGs, Table 6 shows that data analysis (87%, 13 studies) and object simulation (80%, 12 studies) are considered essential features for DG operation. These characteristics enable interaction within the virtual model without the constraints of the physical system and support decision-making based on the DG's behavior across various scenarios.

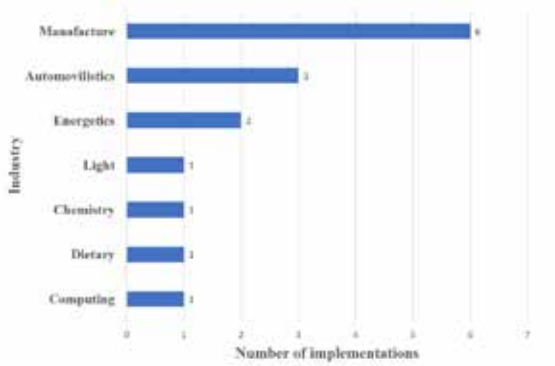
Table 6. Functional characteristics of DGs

Reference	Data analysis	Simulation of the object	Self-study
[12]	✓	✓	×
[9]	✓	✓	×
[2]	✓	✓	✓
[8]	✓	✓	×
[1]	✓	✓	✓
[13]	×	×	×
[3]	✓	×	×
[4]	✓	✓	✓
[14]	✓	✓	×
[15]	✓	✓	✓
[16]	✓	✓	✓
[17]	×	×	×
[18]	✓	✓	✓
[19]	✓	✓	×
[20]	✓	✓	✓

C. Application Aspects

According to the criterion Areas in Which DGs Were Implemented, the analysis revealed that 40% (6) of the applications focused on improving the efficiency of manufacturing processes, as shown in Fig. 3.

Fig. 3. Types of industry in which DGs have been implemented



Note: The numbers in the bars indicate the reference number of the applications according to Table 3.

Regarding the DG Dimension criterion, Table 7 shows that 33% (5) of the applications refer to DGs composed of other DGs or integrated with other IT systems. In contrast, 67% (10) of the analyzed applications involve individual DGs, meaning their functionality does not depend on other systems.

Table 7. Dimension of the DG

Reference	Individual system	Compound system
[12]	✓	×
[9]	✓	×
[2]	✓	×
[8]	×	✓
[1]	✓	×
[13]	✓	×
[3]	×	✓
[4]	✓	×
[14]	×	✓
[15]	✓	×
[16]	×	✓
[17]	✓	×
[18]	✓	×
[19]	✓	×
[20]	×	✓

In summary, from the literature review and the analysis criteria applied, it is evident that DGs have been mostly implemented in China, whose reference data are mostly socialized in English. Then, the use of AI for their development is highlighted, where characterizing aspects, such as data analysis and simulation, stand out for their operation-being implemented to improve the efficiency of manufacturing processes.

VI. CONCLUSION

The technology and concept of DG have evolved significantly from the early 21st century to the present, driven in large part by advancements in Industry 4.0 technologies. Based on the research questions addressed in this study, it was possible to identify key definitions and characteristics of DGs, understand the implications of their development, and examine how they have been applied across various types of industries.

Concerning the definitions, the concept of DG and its associated characteristics were clarified, allowing for a better understanding of the technology. Furthermore, the evolution of the concept was traced back to the initial proposals by Grieves and Vickers [12]. Based on the findings from the literature review, a definition was proposed to reflect the current understanding of DG.

Regarding the implications of DG development, the literature highlights its close relationship with other Industry 4.0 technologies in both its creation and operation [1], [17]. Among these, Artificial Intelligence (AI) emerges as a fundamental component for the effective functioning of a DG.

In terms of DG applications across different industries, the manufacturing sector receives the greatest focus for DG implementation. This finding aligns with previous research that provides evidence of how DGs are being applied within industrial contexts [13], [9].

The results of the systematic literature review may hold significant relevance at both national and international levels for researchers and industries interested in the use and implementation of DGs. This study can serve as a reference point for understanding the current state of DG implementation in the industrial sector.

Finally, it is considered necessary to conduct further studies on DGs in other fields of knowledge, such as medicine, which, based on the findings of this research, could greatly benefit from the application of DG technologies.

ISSN: 2015-5392

ACKNOWLEDGMENT

We extend our gratitude to the courses IF-5000 Networks and Data Communications and IF-6000 Networks in Business of the Business Informatics program at the Guápiles Campus – Atlantic Campus, University of Costa Rica, for providing various forms of support during 2022–2023. These included workshops, training sessions, guidance, and, most importantly, continuous support, all of which contributed to the development of research competencies and skills among the student body.

Competing Interests

The authors declare no competing interests.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Juan Carlos Sandí-Delgado
https://orcid.org/0000-0003-3932-3045

Steven Cruz-Sancho
https://orcid.org/0000-0001-5549-4990

Samuel Jones-Chaves
https://orcid.org/0000-0002-8356-6485

Xavier Gómez-López
https://orcid.org/0000-0003-0202-3276

REFERENCES

[1] A. Fuller, Z. Fan, C. Day, and C. Barlow, *"Digital Twin: Enabling Technologies, Challenges and Open Research," IEEE Access*, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[2] Y. Zheng, S. Yang, and H. Cheng, *"An Application Framework of Digital Twin and Its Case Study," Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1141–1153, 2019, doi: 10.1007/s12652-018-0911-3.

[3] M. Varas Chiquito, J. C. García Plua, M. E. Bustamante Chong, and C. Bustamante Chong, "*Gemelos digitales y su evolución en la Industria," RECIMUNDO*, vol. 4, no. 4, pp. 300–308, 2020, doi: 10.26820/recimundo/4.(4).noviembre.2020.300-308.

[4] J. Wu, Y. Yang, X. Cheng, H. Zuo, and Z. Cheng, *"The Development of Digital Twin Technology Review," in Proc. Chinese Automation Congress (CAC),* Shanghai, China, 2020, pp. 4901–4906, doi: 10.1109/CAC51589.2020.9327756.

[5] F. J. Toala Arias, K. Maldonado Zúñiga, M. M. Toala Zambrano, and J. E. Álava Cruzatty, *"Gemelos Digitales En La Industria," Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, vol. 4, no. 1, pp. 75–83, 2022. [En línea]. Disponible en: https://editorialalema.org/index.php/pentaciencias/article/view/29

[6] M. F. Dávila R, F. Schwark, L. Dawel, and A. Pehlken, *"Sustainability Digital Twin: A Tool for the Manufacturing Industry," Procedia CIRP,* vol. 116, pp. 143–148, 2023, doi: 10.1016/j.procir.2023.02.025.

[7] M. Soori, B. Arezoo, and R. Dastres, *"Digital twin for smart manufacturing, A review," Sustainable Manufacturing and Service Economy,* vol. 2, 100017, 2023, doi: 10.1016/j.smse.2023.100017.

[8] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, *"Characterising the Digital Twin: A Systematic Literature Review," CIRP Journal of Manufacturing Science and Technology,* vol. 29, pp. 36–52, 2020, doi: 10.1016/j.cirpj.2020.02.002.

[9] B. R. Barricelli, E. Casiraghi, and D. Fogli, "*A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications," IEEE Access,* vol. 7, pp. 167653–167671, 2019, doi: 10.1109/ACCESS.2019.2953499.

[10] D. Rico-Bautista et al., "*Smart University: A vision of technology adoption," Revista Colombiana de Computación,* vol. 22, no. 1, pp. 44–55, 2021, doi: 10.29375/25392115.4153.

[11] E. Romero-Riaño, C. Galeano-Barrera, C. D. Guerrero, M. Martinez-Toro, and D. Rico-Bautista, "*IoT applied to irrigation systems in agriculture: A usability analysis," Revista Colombiana de Computación*, vol. 23, no. 1, pp. 44–52, 2022, doi: 10.29375/25392115.4483.

[12] M. Grieves and J. Vickers, "*Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in Transdisciplinary Perspectives on Complex Systems*, J. Kahlen, S. Flumerfelt, and A. Alves, Eds. Cham, Switzerland: Springer, 2017, pp. 85–113, doi: 10.1007/978-3-319-38756-7_4.

[13] I. Errandonea, S. Beltrán, and S. Arrizabalaga, "*Digital Twin for Maintenance: A Literature Review," Computers in Industry,* vol. 123, Art. no. 103316, 2020, doi: 10.1016/j.compind.2020.103316.

[14] D. Orive, A. López, E. Estévez, A. Orive, and M. Marcos, *"Desarrollo de Gemelos Digitales para la Simulación e Integración de Activos de Fabricación en la Industria 4.0," in Proc. XLII Jornadas de Automática:* Libro de Actas, Barcelona, España, Sep. 1–3, 2021, pp. 709–716, doi: 10.17979/spudc.9788497498043.709.

[15] B. He and K. J. Bai, *"Digital Twin-Based Sustainable Intelligent Manufacturing: A Review," Advanced Manufacturing*, vol. 9, pp. 1–21, Mar. 2021, doi: 10.1007/s40436-020-00302-5.

[16] L. T. Reiche, C. S. Gundlach, G. F. Mewes, and A. Fay, *"The Digital Twin of a System: A Structure for Networks of Digital Twins," in Proc. 26th IEEE Int. Conf. Emerging Technologies and Factory Automation* (ETFA), Västerås, Sweden, Sep. 7–10, 2021, pp. 1–8, doi: 10.1109/ETFA45728.2021.9613594.

[17] S. Khan, T. Arslan, and T. Ratnarajah, *"Digital Twin Perspective of Fourth Industrial and Healthcare Revolution," IEEE Access*, vol. 10, pp. 25732–25754, 2022, doi: 10.1109/ACCESS.2022.3156062.

[18] D. Bowman, L. Dwyer, A. Levers, E. A. Patterson, S. Purdie, and K. Vikhorev, *"A Unified Approach to Digital Twin Architecture—Proof-of-Concept Activity in the Nuclear Sector," IEEE Access,* vol. 10, pp. 44691–44709, 2022, doi: 10.1109/ACCESS.2022.3161626.

[19] X. Fang, H. Wang, G. Liu, X. Tian, G. Ding, and H. Zhang, *"Industry Application of Digital Twin: From Concept to Implementation," International Journal of Advanced Manufacturing Technology,* vol. 121, pp. 4289–4312, 2022, doi: 10.1007/s00170-022-09632-z.

[20] N. Gorbatenko, A. Ovsov, V. Vedernikov, and A. Lebedeva, *"The Concept of Creating a Software Digital Twin of an Electronic Device," in Proc. 2nd Int. Conf. Technology Enhanced Learning in Higher Education* (TELE), Lipetsk, Russia, May 26–27, 2022, pp. 115–117, doi: 10.1109/tele55498.2022.9801058.

[21] S. Yoon, *"Building digital twinning: Data, information, and models,"* Journal of Building Engineering, vol. 76, Art. no. 107021, 2023, doi: 10.1016/j.jobe.2023.107021.

[22] G. White, A. Zink, L. Codecá, and S. Clarke, *"A Digital Twin Smart City for Citizen Feedback,"* Cities, vol. 110, Art. no. 103064, 2021, doi: 10.1016/j.cities.2020.103064.

[23] G. G. Rodríguez, J. M. González-Cava, E. Jove, J. L. Calvo-Rolle, and J. A. Méndez Pérez, *"Diseño de un gemelo digital para el gestor de operaciones de una lavandería industrial," in XL Jornadas de Automática*: Libro de Actas, Ferrol, España, Sep. 4–6, 2019, pp. 499–505, Servizo de Publicacións, doi: 10.17979/spudc.9788497497169.499.

[24] F. Naeem, G. Kaddoum, and M. Tariq, *"Digital Twin-Empowered Network Slicing in B5G Networks: Experience-Driven Approach," in Proc. IEEE Globecom Workshops (GC Wkshps),* Madrid, España, Dec. 7–11, 2021, pp. 1–5, doi: 10.1109/GCWkshps52748.2021.9682073.

[25] B. Kitchenham, "*Procedures for Performing Systematic Reviews, Version 1.0," Empirical Software Engineering,* vol. 33, pp. 1–26, 2004. [En línea]. Disponible en: https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

[26] L. J. Martínez, C*ómo buscar y usar información científica: Guía para estudiantes universitarios,* 2016. [En línea]. Disponible en: https://www.researchgate.net/publication/301620258_Como_buscar_y_usar_informacion_cientifica_Guia_para_estudiantes_universitarios.

LA INTELIGENCIA ARTIFICIAL EN AMÉRICA LATINA Y EL CARIBE: HOJA DE RUTA PARA UNA ADOPCIÓN ÉTICA, INCLUSIVA Y ESTRATÉGICA

Mba. José Andrés Fernández Marmolejo
Coordinador, Comisión de Inteligencia Artificial
Colegio de Profesionales en Informática y Computación (CPIC)

RESUMEN

Este artículo analiza el estado actual de la inteligencia artificial (IA) en América Latina y el Caribe, destacando tanto las oportunidades como los riesgos asociados a su adopción en contextos sociales desiguales. Se identifican brechas en infraestructura, formación, gobernanza y legislación, al tiempo que se destacan casos exitosos y sectores estratégicos con alto potencial de transformación. El texto propone principios éticos para una IA centrada en las personas y presenta recomendaciones específicas para gobiernos, academia, gremios, empresas y ciudadanía. Asimismo, subraya el papel fundamental del gremio informático como actor ético y técnico en la construcción de un modelo de IA inclusivo, transparente y soberano. Se concluye con un llamado a la acción para definir una hoja de ruta regional que permita aprovechar la IA con equidad, justicia social y visión de futuro.

ABSTRACT

This article examines the current state of artificial intelligence (AI) in Latin America and the Caribbean, highlighting both opportunities and risks associated with its adoption in unequal social contexts. It identifies gaps in infrastructure, education, governance, and legislation, while showcasing success stories and strategic sectors with high transformative potential. The text proposes ethical principles for human-centered AI and offers specific recommendations for governments, academia, professional associations, businesses, and civil society. It also emphasizes the essential role of IT professionals as ethical and technical agents in shaping an inclusive, transparent, and sovereign AI model. The article concludes with a call to action for defining a regional roadmap to harness AI with equity, social justice, and long-term vision.

I. INTRODUCCIÓN

La inteligencia artificial (IA) está transformando radicalmente la manera en que las sociedades producen, interactúan y resuelven problemas complejos. Su avance vertiginoso no solo plantea oportunidades sin precedentes en campos como la salud, la educación, la agricultura y la administración pública, sino también desafíos significativos en materia ética, regulatoria y de equidad social.

América Latina y el Caribe (ALC), una región caracterizada por su diversidad, talento humano y potencial de crecimiento, enfrenta una doble encrucijada: aprovechar las ventajas de la IA para impulsar el desarrollo sostenible, o quedar rezagada frente a economías más avanzadas tecnológicamente. A pesar de algunos esfuerzos emergentes en países como Brasil, México, Colombia, Chile y Costa Rica, la mayoría de las naciones latinoamericanas carecen de estrategias nacionales sólidas que orienten la adopción responsable y efectiva de estas tecnologías.

En este contexto, surge la necesidad urgente de construir una hoja de ruta regional para la adopción ética y estratégica de la IA, fundamentada en los principios de transparencia, inclusión, soberanía tecnológica y beneficio social. Esto implica no solo considerar los aspectos técnicos de implementación, sino también el diseño de marcos normativos, éticos y educativos que garanticen un despliegue justo y sostenible.

Este artículo tiene como objetivo analizar el estado actual de la IA en ALC, identificar los principales retos y oportunidades que enfrenta la región, así como proponer lineamientos para una adopción que combine innovación, ética y visión a largo plazo. Asimismo, se destacará el rol fundamental que pueden jugar los colegios profesionales, como el Colegio de Profesionales en Informática y Computación (CPIC) de Costa Rica, en la construcción de una gobernanza regional para la IA que sea inclusiva, técnica y humanamente consciente.

II. DIAGNÓSTICO REGIONAL: ESTADO DE LA IA EN ALC

A pesar del creciente protagonismo de la IA en el escenario global, ALC todavía se encuentra en una etapa incipiente en cuanto a su adopción, regulación e integración en sectores clave. Mientras que potencias tecnológicas como Estados Unidos, China y la Unión Europea han avanzado en estrategias robustas de desarrollo, la región latinoamericana enfrenta una combinación de avances dispersos, iniciativas desarticuladas y brechas estructurales.

En términos de políticas públicas, solo un grupo reducido de países ha desarrollado estrategias nacionales de IA. Brasil, por ejemplo, publicó en 2021 su Estrategia Brasileña de Inteligencia Artificial, centrada en fomentar la investigación, el desarrollo ético y la formación de talento. México presentó una estrategia preliminar en 2018 a través de C Minds y la Secretaría de Hacienda, aunque su implementación ha sido limitada. Colombia y Chile han logrado avances significativos, con planes nacionales que integran componentes éticos, regulatorios y educativos. En el caso de Uruguay, se ha promovido el uso de IA en servicios públicos a través de la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC). Costa Rica, por su parte, ha desarrollado iniciativas desde el sector académico y gremial, como la Comisión de Inteligencia Artificial del CPIC, aunque todavía carece de una estrategia nacional consolidada.

Desde el punto de vista educativo, la región presenta avances importantes pero desiguales. Algunas universidades han creado programas especializados en IA, ciencia de datos y aprendizaje automático, aunque la oferta sigue concentrada en centros urbanos y en instituciones con acceso a fondos internacionales. La formación técnica en habilidades digitales aún no ha sido integrada de forma transversal en los sistemas educativos nacionales, lo que limita la generación de talento calificado a gran escala.

En el ámbito empresarial, las grandes empresas multinacionales instaladas en la región lideran los procesos de adopción de IA, mientras que las pequeñas y medianas empresas (pymes), que representan más del 90 % del tejido productivo regional, enfrentan obstáculos como falta de financiamiento, desconocimiento de tecnologías emergentes y ausencia de políticas de incentivos para la transformación digital. Según el reporte Latin America Digital Transformation Report 2023 del Banco Interamericano de Desarrollo (BID) y el Foro Económico Mundial, solo el 17 % de las pymes en América Latina ha explorado soluciones de IA y menos del 10 % ha implementado pilotos funcionales.

Adicionalmente, existe una brecha significativa en infraestructura digital, con países que aún enfrentan dificultades de acceso a internet de calidad, sobre todo en zonas rurales. Esta limitación no solo reduce el alcance de las soluciones basadas en IA, sino que también amplifica las desigualdades sociales al impedir una participación inclusiva en la economía digital.

Finalmente, uno de los aspectos más críticos es la ausencia de marcos regulatorios claros y coordinados en materia de IA. Mientras Europa avanza en leyes como el AI Act y Estados Unidos emite directrices ejecutivas específicas, la mayoría de los países latinoamericanos carece de legislación vinculante sobre el uso, límites, rendición de cuentas o ética de los sistemas de IA.

A partir de lo anterior, puede decirse que la región muestra señales alentadoras en términos de interés, talento emergente y casos de uso puntuales. Sin embargo, el panorama general evidencia una necesidad urgente de coordinación regional, planificación estratégica y alineamiento ético que permita a América Latina no solo ponerse al día, sino convertirse en un actor activo en la definición del futuro de la inteligencia artificial a nivel global.

Tabla 1

País	Año de publicación	Institución responsable	Enfoque destacado
Brasil	2021	Ministerio de Ciencia y Tecnología	Innovación, ética, competitividad
Colombia	2020	MinCiencias y MinTIC	IA para el desarrollo sostenible
Chile	2021	Ministerio de Ciencia y Ministerio de Economía	Datos abiertos, inclusión digital
México	2018 (borrador)	C Minds + Secretaría de Hacienda	Ética, desarrollo económico
Uruguay	2022 (lineamientos)	AGESIC	Gobierno digital, servicios públicos
Argentina	En desarrollo	Ministerio de Ciencia y Tecnología	Participación pública

La Tabla 1 resume el estado actual de las estrategias nacionales de IA en algunos países de ALC y refleja tanto avances como vacíos institucionales que deben ser abordados para consolidar una agenda regional.

ISSN: 2015-5392

III. OPORTUNIDADES CLAVE PARA ALC

Lejos de limitarse a los desafíos, ALC enfrenta una oportunidad histórica para impulsar su desarrollo económico y social a través de la IA, siempre que esta adopción se acompañe de una visión ética, regulada e inclusiva. Si bien la región parte de una base heterogénea, sus características demográficas, culturales, ecológicas y productivas la posicionan estratégicamente para convertirse en un laboratorio natural de innovación tecnológica con impacto social.

A. Transformación del sector público y gobierno digital

La IA tiene el potencial de optimizar la administración pública mediante automatización de procesos, predicción de riesgos sociales, y personalización de servicios ciudadanos. Países como Uruguay y Chile han comenzado a incorporar algoritmos en procesos de atención al ciudadano, fiscalización y planificación urbana. La expansión de estas iniciativas puede conducir a una gestión estatal más eficiente, transparente y orientada a resultados. Para ello, es de suma importancia establecer marcos legales claros sobre el uso de IA en la toma de decisiones públicas, lo cual garantiza transparencia, rendición de cuentas y mecanismos de apelación ante decisiones automatizadas.

B. Educación inclusiva y adaptativa

La IA puede ser utilizada para personalizar el aprendizaje, identificar brechas en tiempo real, automatizar evaluaciones y generar contenidos adecuados a diferentes estilos y ritmos de aprendizaje. En regiones donde las desigualdades educativas son profundas, estas tecnologías representan una oportunidad sin precedentes para democratizar el acceso al conocimiento. Sin embargo, esto requiere reformas regulatorias en los sistemas educativos e integran la ética digital, la alfabetización en IA y el uso seguro de estas herramientas desde la educación primaria.

C. Innovación en salud pública

Desde sistemas de diagnóstico asistido por IA hasta el análisis predictivo de brotes epidemiológicos, las tecnologías basadas en datos pueden salvar vidas y reducir costos. La región tiene la posibilidad de aplicar estas herramientas en salud preventiva, telesalud y gestión de recursos hospitalarios. Para ello, es urgente modificar los marcos legales sobre protección de datos de salud, asegurando que el uso de IA no comprometa la privacidad ni fomente discriminaciones algorítmicas.

D. Agricultura inteligente y sostenibilidad

La agroindustria representa uno de los sectores más importantes en varias economías de la región. La IA puede contribuir con sistemas de predicción climática, riego automatizado, monitoreo por drones y control de plagas. Esto puede aumentar la productividad, reducir desperdicios y hacer frente al cambio climático. No obstante, se requiere actualizar las normativas agrarias y ambientales para regular el uso de datos geoespaciales y garantizar una aplicación ética de la IA en ecosistemas naturales.

E. Formalización del empleo y protección laboral

La automatización de procesos productivos puede generar reemplazo de tareas humanas, pero también nuevas oportunidades laborales si se acompañan de políticas activas de reconversión laboral. La IA puede servir para mapear habilidades emergentes, guiar procesos de formación y optimizar estrategias de inserción laboral. Esto demanda una actualización urgente de las legislaciones laborales para incluir nuevas formas de trabajo asistido por IA, derechos frente a decisiones automatizadas y acceso equitativo a las oportunidades de la economía digital.

En conclusión, las oportunidades de la IA en América Latina solo serán sostenibles si se impulsan en paralelo a una modernización de los marcos legales, éticos e institucionales, que velen por la protección de los derechos humanos, el acceso igualitario a los beneficios tecnológicos y la soberanía digital de los países. La región no solo puede adoptar inteligencia artificial: puede y debe influir en su desarrollo responsable, desde nuestras realidades.

IV. RIESGOS EMERGENTES Y DILEMAS ÉTICOS EN LA ADOPCIÓN DE LA IA

Fig. 1. Bechas clave en la adopción de IA en América Latina

La Figura 1 ilustra de forma comparativa las principales brechas que enfrenta la región en el proceso de adopción de IA, y que requieren atención prioritaria desde una perspectiva ética y estructural.

A medida que América Latina y el Caribe explora el uso de la IA para impulsar su desarrollo, también se expone a una serie de riesgos éticos, sociales y jurídicos que podrían ampliar las desigualdades existentes si no se abordan de forma preventiva y deliberada. La ausencia de marcos regulatorios específicos, combinada con una limitada capacidad institucional para fiscalizar sistemas complejos, plantea interrogantes urgentes sobre la gobernanza de la IA en la región.

A. Discriminación algorítmica y reproducción de sesgos

Los sistemas de IA aprenden a partir de datos históricos, que muchas veces contienen sesgos estructurales derivados de desigualdades sociales, económicas o de género. En países latinoamericanos, donde las estadísticas públicas pueden ser incompletas, fragmentadas o reflejar discriminaciones pasadas, el riesgo de construir modelos que perpetúen exclusiones es alto. Aplicaciones en salud, educación, justicia o contratación podrían discriminar sin intención explícita, pero con consecuencias reales. La región necesita normativas claras sobre auditoría algorítmica, transparencia y mecanismos de reparación para los afectados.

B. Vulneración del derecho a la privacidad y vigilancia masiva

El uso indiscriminado de sistemas de reconocimiento facial, vigilancia predictiva o recopilación masiva de datos personales sin consentimiento informado representa un grave riesgo a los derechos fundamentales. En varios países de la región, estos sistemas se están implementando sin una legislación específica sobre inteligencia artificial ni marcos de protección de datos robustos. Es urgente que los estados latinoamericanos adopten leyes de protección de datos que contemplen específicamente los nuevos desafíos que impone la IA.

C. Concentración de poder tecnológico y dependencia digital

Gran parte de las plataformas de IA más avanzadas son desarrolladas por un pequeño grupo de corporaciones transnacionales, ubicadas fuera de la región. Esto genera una dependencia tecnológica que puede limitar la soberanía digital de los países latinoamericanos, restringiendo su capacidad de auditar, adaptar o controlar el funcionamiento de estos sistemas. La solución no solo pasa por el consumo responsable, sino también por el desarrollo de capacidades locales, marcos de interoperabilidad abiertos y la promoción de tecnologías éticas de código abierto.

D. Impacto en el empleo y la informalidad

Si bien la IA puede generar nuevas oportunidades laborales, también implica la automatización de tareas que tradicionalmente han sido fuente de empleo para millones de personas. En economías donde la informalidad laboral es alta, la automatización sin acompañamiento puede ampliar las brechas sociales. Es trascendental que la adopción de IA en el sector productivo venga acompañada de políticas activas de formación, reconversión laboral y protección de los derechos de los trabajadores en entornos híbridos humano-máquina.

E. Falta de mecanismos éticos y regulatorios adaptados a la realidad regional

La mayoría de países latinoamericanos carecen de organismos especializados que supervisen el uso de IA desde una perspectiva ética y técnica. A diferencia de la Unión Europea, que avanza con el AI Act, o Canadá y Estados Unidos, que discuten marcos de rendición de cuentas algorítmica, en América Latina predominan las lagunas legales. Esto deja a la región vulnerable ante prácticas irresponsables, y refuerza la necesidad de crear marcos regulatorios propios, basados en los valores de la región, pero en diálogo con los estándares internacionales.

El desarrollo de la inteligencia artificial en América Latina no puede limitarse a una carrera por la innovación. Requiere un enfoque proactivo de gobernanza tecnológica, que integre principios de equidad, inclusión, derechos humanos y sostenibilidad. Reconocer estos riesgos es el primer paso para mitigarlos y construir una IA confiable, legítima y al servicio del bien común.

V. PRINCIPIOS PARA UNA IA ÉTICA Y CONFIABLE EN ALC

Frente a los riesgos emergentes y la necesidad de orientar el desarrollo tecnológico hacia el bienestar colectivo, ALC tienen la oportunidad de adoptar una IA que sea ética, inclusiva y socialmente útil. Para lograrlo, no basta con implementar tecnologías avanzadas: es necesario definir los principios rectores que guíen su diseño, implementación, monitoreo y gobernanza. Estos principios deben considerar tanto los estándares internacionales como las realidades culturales, sociales y económicas de la región.

ISSN: 2015-5392

A. Transparencia y explicabilidad

Los sistemas de IA que toman decisiones que afectan a las personas deben ser comprensibles, auditables y capaces de justificar sus resultados. Esto es esencial para garantizar la confianza del público y prevenir abusos. En contextos donde existe una historia de desconfianza institucional, la explicabilidad de los algoritmos se convierte en una herramienta clave para reforzar la legitimidad democrática y la rendición de cuentas.

B. Justicia, equidad e inclusión

La IA debe diseñarse y desplegarse con el objetivo de reducir desigualdades, no de profundizarlas. Esto implica incluir múltiples voces en los procesos de desarrollo tecnológico, asegurar que los sistemas no discriminen por género, raza, condición socioeconómica o discapacidad, y fomentar la participación de grupos históricamente excluidos en el ecosistema digital.

C. Protección de los derechos fundamentales

El respeto a la privacidad, la libertad de expresión, la no discriminación y el debido proceso deben ser pilares de cualquier iniciativa basada en IA. Estos derechos no deben verse comprometidos por la eficiencia técnica o la automatización. En este sentido, se requiere un marco legal robusto y actualizado, que garantice los derechos humanos en entornos digitales y automatizados.

D. Responsabilidad y rendición de cuentas

Debe existir claridad sobre quién es responsable cuando un sistema de IA falla o produce consecuencias negativas. Esta trazabilidad es especialmente importante en aplicaciones críticas como justicia, salud, seguridad o servicios financieros. La región necesita impulsar leyes que establezcan obligaciones claras para desarrolladores, proveedores, usuarios y entidades públicas que integran IA en sus procesos.

E. Seguridad y robustez técnica

Los sistemas de IA deben ser seguros por diseño, resistentes a ataques, fallas o manipulaciones maliciosas. Esto implica aplicar metodologías rigurosas de desarrollo, pruebas extensas, y sistemas de monitoreo constante. En América Latina, donde existen vulnerabilidades cibernéticas y capacidad limitada de fiscalización, la seguridad de los sistemas algorítmicos debe ser una prioridad regulatoria.

F. Sostenibilidad y enfoque ambiental

El impacto ecológico de la IA, incluyendo el consumo energético de los modelos y los centros de datos, debe formar parte del análisis ético. América Latina, como región vulnerable al cambio climático, no puede adoptar tecnologías que amplifiquen los problemas ambientales. Se requiere un enfoque tecnológico sustentable, que mida y mitigue la huella ecológica de la transformación digital.

G. Soberanía tecnológica y cooperación regional

Finalmente, es fundamental garantizar que los países de la región mantengan control sobre sus datos, sus infraestructuras y sus decisiones tecnológicas. Esto implica fomentar el desarrollo local de soluciones, promover el uso de tecnologías abiertas, y fortalecer las alianzas entre países latinoamericanos para diseñar marcos comunes de gobernanza tecnológica.

Estos principios no deben verse como obstáculos al progreso, sino como condiciones mínimas para un desarrollo tecnológico legítimo, sostenible y centrado en las personas. La adopción de la IA en América Latina será verdaderamente transformadora si se basa en valores compartidos, mecanismos de protección efectivos y una visión de futuro que anteponga el bienestar colectivo al interés individual o comercial.

VI. EL COMPROMISO ÉTICO DEL GREMIO INFORMÁTICO ANTE EL AVANCE DE LA IA EN AMÉRICA LATINA

La transformación impulsada por la IA no es solo tecnológica: es profundamente ética, social y humana. En este contexto, los profesionales de la informática y la computación desempeñan un papel central, no solo como arquitectos del cambio, sino como guardianes de los principios que deben guiar ese cambio. Su rol va más allá del diseño de algoritmos o la programación de sistemas; se trata de asumir la responsabilidad social del conocimiento técnico aplicado.

En ALC, donde las brechas de acceso, la fragilidad institucional y las desigualdades históricas pueden amplificarse con el uso irresponsable de tecnologías avanzadas, el compromiso ético de los profesionales informáticos es más necesario que nunca. Estos profesionales no pueden ser actores neutrales ni espectadores pasivos ante la implementación de soluciones algorítmicas que afectan la vida de millones de personas.

A. De la neutralidad técnica al compromiso ético

La tradicional visión del desarrollador como ejecutor técnico debe ser sustituida por una ética profesional activa. El profesional informático debe cuestionar los propósitos de un sistema, su impacto social, su equidad y su transparencia. Esto implica desarrollar una mirada crítica que permita detectar sesgos, rechazar aplicaciones que violen derechos humanos y proponer alternativas justas y sostenibles.

B. Responsabilidad compartida en el ciclo de vida de los sistemas de IA

Desde el diseño hasta el despliegue, todo sistema de IA atraviesa decisiones críticas que afectan a personas reales. El gremio informático debe velar porque esas decisiones se tomen con base en evidencia, consulta interdisciplinaria y principios éticos sólidos. Esto incluye documentar procesos, fomentar la auditabilidad, y resistirse a presiones comerciales que comprometan la integridad profesional.

C. Formación continua con enfoque humanista

En un entorno tecnológico en constante evolución, la actualización técnica ya no es suficiente. Los informáticos del siglo XXI deben incorporar en su formación elementos de filosofía de la tecnología, derechos digitales, justicia algorítmica y sostenibilidad. Las universidades, los centros de capacitación y los colegios profesionales deben promover un modelo formativo que integre competencias técnicas con pensamiento crítico y sensibilidad social.

D. Cultura gremial y defensa de principios colectivos

El fortalecimiento del gremio pasa por construir una cultura profesional que valore la ética tanto como la innovación. Esto implica crear espacios de discusión crítica, establecer códigos de conducta actualizados, y consolidar redes regionales que permitan compartir buenas prácticas, principios comunes y posiciones técnicas frente a proyectos de alto impacto. En este marco, los colegios profesionales como el CPIC de Costa Rica cumplen un rol clave al promover lineamientos, comisiones especializadas y posicionamientos técnicos que orienten al sector desde una perspectiva ética, legal y humanista.

E. Participación en el debate público y la formulación de políticas

El gremio informático no puede permanecer ajeno al debate sobre el futuro tecnológico de la región. Es necesario que sus miembros participen activamente en la creación de marcos regulatorios, aporten desde su conocimiento técnico a la formulación de leyes y políticas, y ayuden a traducir conceptos complejos a un lenguaje accesible para tomadores de decisión, medios y ciudadanía. La responsabilidad cívica del gremio profesional es fundamental para lograr una IA que refleje los valores democráticos y de justicia social de América Latina.

VII. OPORTUNIDADES Y RECOMENDACIONES ESTRATÉGICAS PARA UNA IA ÉTICA Y SOSTENIBLE EN AMÉRICA LATINA

La adopción de la IA en ALC no debe ser solo un objetivo tecnológico, sino una estrategia integral de transformación social, económica y democrática. Para avanzar hacia una IA centrada en las personas, es indispensable articular esfuerzos entre los distintos actores del ecosistema. A continuación, se presentan recomendaciones estratégicas orientadas a fomentar un desarrollo responsable, inclusivo y sostenible de la IA en la región.

A. Para los gobiernos y legisladores

- Diseñar estrategias nacionales de IA con enfoque ético, social y productivo, adaptadas a las realidades y prioridades de cada país.
- Actualizar marcos legales que regulen el uso de IA, especialmente en lo referente a transparencia algorítmica, protección de datos, derechos digitales y responsabilidad ante errores o discriminaciones automatizadas.
- Crear órganos nacionales de supervisión y ética algorítmica, con participación multisectorial, que evalúen el uso de IA en instituciones públicas y privadas.
- Incentivar el desarrollo de soluciones locales mediante fondos públicos, concursos, compras estatales innovadoras y cooperación internacional.

ISSN: 2015-5392

B. Para la academia y centros de investigación

- Incorporar contenidos de IA, ética y derechos digitales en planes de estudio de carreras tecnológicas, humanísticas y jurídicas.
- Fomentar la investigación interdisciplinaria en temas como gobernanza algorítmica, justicia digital, y modelos sostenibles de IA para el desarrollo.
- Promover la formación continua del profesorado en nuevas tecnologías y enfoques pedagógicos basados en IA.
- Establecer observatorios regionales que analicen y publiquen el impacto de la IA en distintas áreas de la sociedad.

C. Para los colegios profesionales y gremios técnicos

- Revisar y actualizar los códigos de ética profesional, incluyendo criterios sobre el diseño, uso y fiscalización de sistemas de IA.
- Crear comisiones permanentes sobre IA y nuevas tecnologías que orienten técnicamente a sus agremiados y a otros sectores del país.
- Impulsar programas de certificación ética y técnica en IA, que garanticen estándares mínimos de calidad, equidad y seguridad en los desarrollos locales.
- Fomentar una cultura gremial de responsabilidad social, transparencia y participación pública en los debates sobre tecnologías disruptivas.

D. Para el sector empresarial

- Adoptar principios de IA responsable en sus procesos productivos y servicios, más allá del cumplimiento legal mínimo.
- Establecer mecanismos de evaluación de impacto algorítmico, especialmente en sectores sensibles como finanzas, recursos humanos, salud y educación.
- Invertir en formación interna para sus equipos técnicos, promoviendo una ética empresarial alineada con la innovación sustentable.
- Establecer alianzas con universidades, startups y gobiernos para crear soluciones de IA con impacto social positivo.

E. Para la sociedad civil y la ciudadanía

- Fomentar el debate informado sobre los beneficios, riesgos y límites de la IA, promoviendo una participación activa en la formulación de políticas.
- Exigir transparencia y rendición de cuentas cuando los servicios públicos o privados usen algoritmos que afecten derechos fundamentales.
- Apoyar proyectos de alfabetización digital y ética tecnológica, especialmente en comunidades vulnerables.
- Organizar redes de vigilancia ciudadana y colaboración en temas como privacidad, sesgo algorítmico y vigilancia estatal o comercial.

F. Para la región en su conjunto

- Crear una agenda latinoamericana de inteligencia artificial ética y cooperativa, promovida por organismos regionales como CEPAL, BID, OEI o Parlamentos regionales.
- Establecer marcos comunes de gobernanza, estándares interoperables y mecanismos de cooperación técnica entre países.
- Desarrollar una infraestructura tecnológica soberana y abierta, que permita a los países compartir datos de forma segura, entrenar modelos regionales y proteger sus intereses estratégicos.
- Impulsar una narrativa latinoamericana de la IA, basada en la justicia social, la equidad, el desarrollo sostenible y la inclusión cultural.

VIII. CONCLUSIONES

La inteligencia artificial (IA) representa uno de los avances tecnológicos más disruptivos de nuestra era, con el potencial de transformar profundamente las estructuras sociales, económicas e institucionales. Para América Latina y el Caribe, esta transformación no es solo una cuestión de innovación, sino una decisión estratégica sobre el modelo de desarrollo que la región desea construir.

El análisis presentado en este artículo ha evidenciado que, si bien existen esfuerzos incipientes en varios países, aún persisten retos significativos en términos de gobernanza, formación de talento, infraestructura y marcos legales. En paralelo, se abren oportunidades sin precedentes para aplicar la IA en sectores clave como salud, educación, agricultura, medio ambiente y gestión pública.

Sin embargo, aprovechar estas oportunidades sin agravar las desigualdades estructurales de la región requiere una IA que no solo sea eficiente, sino también ética, justa, explicable y centrada en las personas. Esto implica construir una hoja de ruta regional donde la tecnología se ponga al servicio del bien común, y donde la soberanía digital, los derechos humanos y la inclusión sean principios rectores.

El rol del gremio profesional de la informática es esencial en este proceso. Más allá de su competencia técnica, los profesionales del sector deben ejercer un liderazgo ético, crítico y colaborativo, participando activamente en la construcción de marcos normativos, en la promoción de buenas prácticas, y en la defensa de una IA que respete la dignidad humana.

Asimismo, es imperativo que los Estados de la región, junto con universidades, empresas, gremios y sociedad civil, actúen de forma coordinada para diseñar políticas públicas robustas, fomentar capacidades locales y promover la cooperación regional en torno a la IA. El desafío es grande, pero también lo es la oportunidad de convertir a América Latina en un referente global de una inteligencia artificial responsable, inclusiva y con identidad propia.

El momento de actuar es ahora. La inteligencia artificial será parte de nuestro futuro; lo que está en juego es quién la diseña, con qué valores y para qué fines. La región tiene talento, tiene visión y tiene vocación de justicia. Lo que falta es decisión colectiva para convertir el potencial en transformación real.

IX. REFERENCIAS

[1] Comisión Económica para América Latina y el Caribe (CEPAL), Inteligencia artificial en América Latina: Panorama, desafíos y oportunidades, Naciones Unidas, 2021. [En línea]. Disponible en: https://www.cepal.org/es/publicaciones/47170-inteligencia-artificial-america-latina-panorama-desafios-oportunidades

[2] UNESCO, Recomendación sobre la ética de la inteligencia artificial, Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2021. [En línea]. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000381137

[3] Interamericano de Desarrollo (BID), Latin America Digital Transformation Report 2023, 2023. [En línea]. Disponible en: https://www.weforum.org/publications/latin-america-digital-transformation-2023/

[4] OCDE, Principios de la OCDE sobre inteligencia artificial, Organización para la Cooperación y el Desarrollo Económicos, 2019. [En línea]. Disponible en: https://www.oecd.org/going-digital/ai/principles/

[5] Ministerio de Ciencia, Tecnología e Innovación (Colombia), Estrategia Nacional de Inteligencia Artificial Colombia 2020–2024, 2021. [En línea]. Disponible en: https://minciencias.gov.co/

[6] Gobierno de Brasil, Estratégia Brasileira de Inteligência Artificial, Ministério da Ciência, Tecnologia e Inovações, 2021. [En línea]. Disponible en: https://www.gov.br/mcti/pt-br/assuntos/inteligencia-artificial

[7] Comisión Europea, AI Act: Proposal for a Regulation laying down harmonised rules on artificial intelligence, 2024. [En línea]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[8] C Minds, Hacia una estrategia de inteligencia artificial para México: Recomendaciones de política pública, 2018. [En línea]. Disponible en: https://cminds.co/

[9] CPIC – Colegio de Profesionales en Informática y Computación, Comisión de Inteligencia Artificial, 2024. [En línea]. Disponible en: https://cpic.or.cr

[10] B. R. Bioni, “Protección de datos personales e inteligencia artificial en América Latina: una revisión comparada,” Revista Latinoamericana de Derecho y Tecnología, vol. 3, no. 2, pp. 25–42, 2022.

[11] L. Floridi, “Establishing the rules for building trustworthy AI,” Nature Machine Intelligence, vol. 1, no. 6, pp. 261–262, 2019. [En línea]. Disponible en: https://doi.org/10.1038/s42256-019-0055-y

[12] A. Jobin, M. Ienca y E. Vayena, “The global landscape of AI ethics guidelines,” Nature Machine Intelligence, vol. 1, no. 9, pp. 389–399, 2019. [En línea]. Disponible en: https://doi.org/10.1038/s42256-019-0088-2

LA INTELIGENCIA ARTIFICIAL YA ESTÁ EN LAS AULAS: ¿CÓMO RESPONDE COSTA RICA?

J. Alonso Solano Segura
Autor. Docente Universitario, San José, Costa Rica,
asolanos@uned.ac.cr

RESUMEN

Este artículo presenta una revisión crítica de literatura reciente sobre el impacto de la inteligencia artificial (IA) y la tecnología en la educación superior en Costa Rica. A través del análisis de cinco ejes: docencia, evaluación, ética, transformación institucional y competencias digitales se evidencian tanto avances significativos como desafíos urgentes. Las universidades han incorporado herramientas de IA en procesos académicos y administrativos, promoviendo innovación pedagógica y automatización. Sin embargo, persisten brechas tecnológicas, desigualdades regionales y ausencia de marcos normativos claros. Además, la cultura institucional aún enfrenta resistencia al cambio y carece de formación sólida en competencias digitales y éticas. Se concluye que, aunque Costa Rica ya convive con la IA en sus aulas universitarias, aún no está plenamente preparada para una integración estratégica, inclusiva y crítica. La transformación digital debe ser también cultural y humana, para garantizar un uso responsable y equitativo de la IA en el sistema educativo nacional.

I. INTRODUCCIÓN

En este artículo se realiza una revisión crítica de la literatura con el objetivo de establecer un estado actual sobre el impacto de la inteligencia artificial en la educación superior y como diferentes instituciones en Costa Rica, responden a ello. Para esto, se consideran únicamente fuentes con menos de tres años de antigüedad, dado que en un entorno tan dinámico y en constante evolución como lo es la inteligencia artificial, resulta fundamental contar con información actualizada y pertinente. Asimismo, se privilegia el uso de literatura nacional, con el fin de contextualizar adecuadamente el fenómeno desde la realidad costarricense y ofrecer una lectura cercana, comprensible y significativa para quienes vivimos y trabajamos en este país.

La transformación digital de las últimas décadas ha alcanzado de lleno a la educación superior. Tecnologías emergentes, en especial la inteligencia artificial (IA), están transformando la manera en que se enseña y aprende a nivel universitario en todo el mundo. La IA ofrece el potencial de personalizar la educación, optimizar la labor docente y hacer más eficientes los procesos académicos [1]. Herramientas basadas en IA permiten adaptar contenidos a las necesidades individuales de cada estudiante y automatizar tareas administrativas, como la calificación de exámenes, liberando así tiempo para una enseñanza más interactiva. Organismos internacionales como la UNESCO subrayan que, si bien la IA generativa promete mejorar la educación, su implementación debe ser segura, ética y con docentes capacitados para guiar su uso [2].

En Costa Rica, el impacto de la IA y la tecnología en la educación superior se aborda de forma cada vez más estratégica. El país ha reconocido la importancia de fortalecer las capacidades digitales de su población para el futuro, lo que se refleja en la Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027 publicada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones [3]. Esta hoja de ruta nacional plantea integrar la IA en todos los niveles educativos, incluida la educación universitaria, e impulsar la formación continua en competencias digitales y de IA para estudiantes, docentes y ciudadanos [1]. Asimismo, la experiencia de la pandemia de COVID-19 aceleró la transformación digital en las universidades costarricenses, evidenciando tanto el potencial de las plataformas virtuales como la urgencia de atender brechas en infraestructura y capacitación docente [4]. En este contexto, resulta clave analizar cómo la IA y la tecnología están incidiendo en diferentes ámbitos de la educación superior costarricense. A continuación, se abordan cinco ejes temáticos fundamentales: docencia universitaria, evaluación del aprendizaje, ética y uso responsable, transformación digital institucional, y desarrollo de competencias digitales en docentes y estudiantes.

II. EJES TEMÁTICOS

A. Docencia universitaria

La incorporación de la IA y las plataformas digitales está transformando la praxis docente en las universidades. Tras la experiencia de la educación remota por pandemia, las instituciones costarricenses han adoptado modelos mixtos y virtuales en mayor proporción. Por ejemplo, la Universidad de Costa Rica reportó que en el primer semestre de 2022 un 18,9% de los cursos se impartieron totalmente en línea y otro 30% en modalidad bimodal o con alta virtualidad, superando la meta institucional del 20% [5]. Esto refleja una flexibilización metodológica donde se combinan clases presenciales con entornos virtuales de aprendizaje robustos (p. ej., la plataforma Mediación Virtual de la UCR) para enriquecer la enseñanza con recursos digitales.

Al mismo tiempo, emergen nuevas formas de apoyo a la docencia mediante IA. Un caso pionero es el de la Escuela de Lenguas Modernas de la UCR, que integra algoritmos de aprendizaje automático en cursos iniciales de idiomas para ajustar los ejercicios según las fortalezas y debilidades de cada estudiante [6]. Este tipo de tutor inteligente personaliza el ritmo y nivel de los contenidos, brindando práctica adicional en los temas donde el estudiante muestra rezagos y avanzando más rápido en los dominios ya comprendidos. Así, la IA facilita una atención más individualizada dentro del aula universitaria, algo antes difícil de lograr en grupos numerosos.

Los beneficios reportados de incorporar IA en la docencia son notables. Un estudio local con 50 docentes encontró que las clases apoyadas con herramientas de IA mostraron mejoras significativas en las calificaciones del estudiantado, a la vez que redujeron la carga rutinaria del profesorado [7]. La automatización de tareas como la calificación de cuestionarios o la gestión de contenidos alivia el desgaste docente y permite dedicar más tiempo a la interacción pedagógica. De hecho, se observó una disminución del estrés y mayor satisfacción laboral entre los profesores que adoptaron IA, mejorando la sustentabilidad de su práctica. En palabras de los investigadores, la IA puede ser una aliada poderosa para combatir el agotamiento profesional y crear un entorno de enseñanza más positivo [7].

Ahora bien, la integración efectiva de estas tecnologías requiere desarrollo profesional y orientación. La UNED, en su recién publicada guía sobre uso de IA, incentiva a los docentes a innovar sus metodologías con apoyo de estas herramientas de forma crítica. Por ejemplo, su equipo institucional sugiere experimentar elaborando exámenes y materiales con IA, para que el profesorado comprenda de primera mano sus alcances y limitaciones. Además, se promueve que los académicos discutan con los estudiantes el uso ético de herramientas como ChatGPT en las asignaturas, de manera que la IA complemente la enseñanza sin sustituir la interacción humana ni el desarrollo del pensamiento crítico [8]. En conjunto, estos avances se traducen en una docencia universitaria más flexible, personalizada y apoyada por tecnología, siempre que se apliquen de forma reflexiva y centrada en el aprendizaje del estudiante.

B. Evaluación del aprendizaje

La evaluación académica es otro ámbito impactado por la IA, con oportunidades y desafíos notorios. Por un lado, las herramientas inteligentes permiten desarrollar nuevas formas de medir el rendimiento de manera más personalizada. Un ejemplo es el Programa de Evaluación en Lenguas Extranjeras (PELEx) de la UCR, que aplica pruebas adaptativas impulsadas por IA para diagnosticar el dominio de idiomas [5]. Este sistema ajusta la dificultad de las preguntas según las respuestas del estudiante, mejorando la precisión y la experiencia de aprendizaje durante el examen. También se explora la evaluación automatizada de tareas: ciertas plataformas pueden corregir ejercicios de selección múltiple o evaluar actividades de práctica de manera inmediata, retroalimentando al estudiante al instante y liberando tiempo para que el docente se concentre en aspectos más cualitativos [1]. Estas innovaciones sugieren un futuro donde la medición del aprendizaje sea más continua, individualizada y eficiente.

Por otro lado, la IA generativa presenta retos importantes para la integridad académica y los métodos evaluativos tradicionales. Herramientas como ChatGPT pueden generar respuestas a preguntas académicas al instante, lo que pone en jaque exámenes convencionales. De hecho, la UNED advierte que una IA puede resolver evaluaciones de tipo test o tareas rutinarias si están mal diseñadas, evidenciando la necesidad de reformular las estrategias evaluativas [8]. Muchos docentes han expresado preocupación por la dependencia de los estudiantes en estas herramientas para obtener respuestas sin realmente comprender el contenido, lo que deriva en aprendizajes superficiales y copia de información sin análisis crítico [7]. Además, actualmente no existen detectores de contenido generado por IA que sean confiables los disponibles suelen arrojar altos porcentajes de falsos positivos y negativos, lo que dificulta comprobar si un trabajo fue realizado por el estudiante o por una máquina [8]. Ante esta realidad, las universidades se enfrentan al doble desafío de desalentar el plagio asistido por IA y, a la vez, aprovechar estas tecnologías para enriquecer la evaluación.

ISSN: 2015-5392

Para responder a estos retos, se están implementando varias estrategias en el contexto costarricense. Una de ellas es rediseñar las pruebas para fomentar habilidades de orden superior: se sugiere privilegiar las preguntas abiertas, proyectos aplicados, debates orales y tareas que requieran análisis crítico, las cuales son más difíciles de resolver por simple automatismo. Por ejemplo, la UNED propone que el profesorado incluso utilice la IA como aliada en este proceso: generando respuestas con IA para que el estudiante deba evaluarlas, comentarlas o sintetizarlas, obligándolo así a demostrar comprensión y pensamiento crítico sobre la materia [8]. También se está promoviendo la cultura de la honestidad académica en torno a la IA, con medidas como solicitar a los alumnos declaraciones de originalidad y del uso de herramientas de IA en sus entregas. Estas iniciativas buscan asegurar que la evaluación del aprendizaje siga siendo válida y formativa en la era de la inteligencia artificial, combinando la innovación tecnológica con la preservación de la integridad y calidad educativas.

C. Ética y uso responsable

La adopción de IA en la educación superior debe ir acompañada de fuertes consideraciones éticas. Un aspecto central es la privacidad y seguridad de los datos de los estudiantes. Cualquier sistema inteligente que recopile información (por ejemplo, plataformas adaptativas o tutores virtuales) debe garantizar la confidencialidad de los expedientes académicos y respetar la legislación de protección de datos. Así lo enfatiza la Estrategia Nacional de IA, al proponer marcos para gestionar riesgos y asegurar la transparencia en las decisiones automatizadas [3]. En pocas palabras, la implementación de sistemas de IA debe hacerse cuidando siempre la privacidad de alumnos y docentes, y explicando cómo dichas herramientas toman sus decisiones. Por ejemplo, si se utiliza un algoritmo para recomendar recursos o calificar actividades, se debe vigilar que no introduzca sesgos que perjudiquen a algún grupo de estudiantes ni que opere como una "caja negra" inexplicable [1]. Solo abordando estas consideraciones se podrá generar confianza en la comunidad educativa hacia el uso de IA.

Otro principio fundamental es garantizar la equidad y ausencia de sesgos en las aplicaciones de IA. Los algoritmos pueden amplificar discriminaciones si se entrenan con datos parciales o no representativos. En el contexto costarricense, esto implica asegurarse de que las soluciones de IA educativas funcionen bien para distintos grupos socioeconómicos, regiones y estilos de aprendizaje, sin excluir a quienes tengan menor acceso tecnológico. También se requiere que las decisiones automatizadas (por ejemplo, un software que identifique dificultades de aprendizaje) sean explicables y justificadas en términos pedagógicos, de modo que los docentes puedan validarlas o corregirlas cuando sea necesario [1].

Las universidades de Costa Rica han empezado a responder a estos desafíos éticos con diversas iniciativas. La UNED marcó un hito en 2024 al aprobar la primera guía institucional sobre uso responsable de la IA en la educación superior [8]. Este documento pionero establece orientaciones para un uso ético, seguro y transparente de la IA en actividades académicas, advirtiendo tanto sobre sus beneficios como sobre malas prácticas [8]. De igual forma, expertos de la UCR subrayan la urgencia de contar con políticas claras que regulen la IA dentro de la universidad. Según el Dr. Allen Quesada, "la integración de IA debe venir acompañada de directrices claras que garanticen su uso ético, protejan la privacidad de los datos y aseguren el acceso equitativo" [5]. Este llamado destaca la necesidad de reglas internas que orienten a docentes y estudiantes sobre qué está permitido (por ejemplo, el uso de asistentes automáticos en ciertas tareas) y qué está prohibido, evitando lagunas que puedan derivar en abusos o desigualdades.

Por último, la comunidad académica costarricense enfatiza el uso responsable y crítico de la IA, lo cual implica reconocer sus límites. Como se ha insistido en foros universitarios, no se debe "humanizar" a la IA: una máquina no tiene conciencia ni juicio ético, sino que simplemente genera información a partir de patrones [6]. Por ello, nunca se pueden delegar decisiones valorativas o disciplinarias exclusivamente en un algoritmo. Más bien, la IA debe verse como una herramienta de apoyo al criterio humano, no como un reemplazo de éste. Adicionalmente, se aboga por un equilibrio entre regulación y libertad creativa: las normativas sobre IA no deberían basarse solo en prohibiciones, sino en guías positivas que promuevan el uso innovador y ético de la tecnología sin frenar la experimentación responsable [6]. En resumen, Costa Rica busca forjar un modelo propio de gobernanza de IA en la educación superior, donde se conjuguen la innovación tecnológica con los valores humanísticos y derechos fundamentales.

D. Transformación digital institucional

La incorporación de la IA y la tecnología en la educación superior no solo implica cambios en el aula, sino también transformaciones a nivel institucional. Las universidades deben ajustar sus políticas, invertir en infraestructura y desarrollar capacidades organizacionales para integrarse plenamente a la era digital. En Costa Rica, esta transformación digital ha pasado a ser parte de la planificación estratégica del sistema universitario. La ENIA 2024-2027, por ejemplo, plantea estrategias de colaboración entre academia, gobierno y sector productivo para impulsar la adopción de IA: universidades y empresas tecnológicas podrían co-crear cursos y plataformas de formación en IA, y el Ministerio de Educación Pública coordinar con startups iniciativas de innovación educativa [1]. Esta visión intersectorial reconoce que la transformación digital es un esfuerzo país, donde la educación superior actúa como eje catalizador.

A lo interno de las instituciones, se han establecido nuevos programas y unidades para liderar el cambio. La UCR, desde hace más de una década, cuenta con METICS (Mediación Tecnológica), un equipo interdisciplinario dedicado a apoyar la docencia virtual y la innovación educativa. A la fecha, METICS ha capacitado a más de 5.700 personas en la UCR (docentes, administrativos y estudiantes) en temas como educación híbrida, uso didáctico de tecnologías digitales y producción de recursos multimedia [5]. Gracias a estos esfuerzos, la universidad contaba ya con un marco de referencia para la docencia en entornos virtuales desde 2016, el cual fue reforzado en pandemia con lineamientos académicos para virtualizar cursos. En la UNED, por su parte, recientemente se creó un Equipo Institucional de IA y se ejecutan proyectos piloto para integrar la IA en distintas cátedras, al tiempo que se brinda alfabetización digital en IA a todo el personal docente y estudiantil [8]. Estas iniciativas demuestran el compromiso de las universidades públicas por adaptarse rápidamente a los cambios tecnológicos.

Un factor crítico en la transformación institucional es la inversión en recursos tecnológicos y la sostenibilidad financiera. Voceros académicos han hecho un llamado a destinar fondos suficientes para modernizar la educación superior: cumplir con la inversión educativa constitucional y priorizar infraestructura tecnológica, conectividad y capacitación son condiciones indispensables [4]. En efecto, persisten brechas de acceso entre sedes y regiones; se necesita equipamiento, plataformas robustas y anchos de banda adecuados para asegurar que todos los estudiantes se beneficien por igual de la digitalización [4]. Las autoridades universitarias también se han propuesto sensibilizar sobre la importancia de estas inversiones: superar la resistencia al cambio y la percepción de que la tecnología es secundaria exige demostrar con resultados concretos el valor añadido de la transformación digital [1].

Por último, la gestión del cambio cultural dentro de las instituciones es clave. Las universidades están promoviendo una cultura de innovación donde la experimentación con nuevas tecnologías sea parte del quehacer académico. Eventos interuniversitarios, como el foro nacional “Inteligencia Artificial e implicaciones en la Educación Superior” realizado en 2024, evidencian el trabajo conjunto de las cinco universidades públicas para definir políticas y buenas prácticas comunes [9]. Además, instituciones como la UCR se plantean metas ambiciosas, buscando consolidarse como referentes regionales en innovación educativa con IA [5]. Lograr esto requerirá un liderazgo compartido, donde rectorías, facultades y organismos como el CONARE alineen esfuerzos en pro de una transformación digital inclusiva y sustentable en la educación superior costarricense.

E. DESARROLLO DE COMPETENCIAS DIGITALES EN DOCENTES Y ESTUDIANTES

El éxito de la transformación educativa basada en IA depende en gran medida de las competencias digitales de sus protagonistas: el personal docente y el estudiantado. Al inicio de esta década quedó en evidencia que existían importantes brechas en este ámbito. En Costa Rica, el Informe Estado de la Educación 2021 reveló que un 46% de los docentes tenían niveles bajos de competencias digitales al comenzar la pandemia, lo que exponía una preparación limitada para la educación virtual [4]. Además, más del 50% del personal carecía de formación específica en herramientas tecnológicas, y estas carencias se vieron agravadas por desigualdades de acceso especialmente en zonas periféricas con infraestructura insuficiente. Este diagnóstico puso de manifiesto la urgencia de desarrollar competencias digitales de forma masiva y equitativa entre los educadores y alumnos del país.

En respuesta, se han multiplicado las iniciativas de capacitación y formación tanto a nivel nacional como institucional. La ENIA 2024-2027 destaca la formación de talento humano como pilar para aprovechar la IA, subrayando la necesidad de preparar a estudiantes, profesionales y ciudadanos en general en habilidades digitales y de IA. Esto implica actualizar los currículos para incorporar nociones de programación, aprendizaje automático y ética de datos desde la educación básica hasta la universitaria [1], así como ofrecer oportunidades de capacitación

continua para quienes ya ejercen. En línea con ello, las universidades han fortalecido sus programas de desarrollo profesional docente en TIC. Por ejemplo, el Centro de Investigación y Docencia en Educación (CIDE) de la UNA impulsa proyectos como “UNA Esperanza Joven en conexión digital” (para dotar de tecnologías a escuelas vulnerables) y experiencias con realidad virtual inmersiva para mejorar habilidades de resolución de problemas en niñez, integrando a las familias en el proceso [4]. Además, se promueven propuestas pedagógicas innovadoras que integran tecnologías emergentes en diversos entornos de aprendizaje, de modo que los futuros docentes egresen familiarizados con su uso. Como enfatiza la vicedecana del CIDE, “no basta con desarrollar competencias técnicas en el personal docente; es indispensable dotarlos de herramientas pedagógicas y éticas” para integrar la IA de forma crítica, priorizando valores humanos como la creatividad y la empatía por encima de la mera tecnología [4].

Paralelamente, la alfabetización digital del estudiantado universitario también recibe atención. La UNED, por ejemplo, incluyó en su plan de acción la alfabetización en IA para todos sus alumnos, reconociendo que deben ser formados no solo como consumidores sino como usuarios críticos de estas herramientas [8]. En el sector privado, algunas universidades han comenzado a incorporar módulos de tecnología educativa y uso de IA en sus mallas curriculares. Tal es el caso de U Fidélitas, que integró la enseñanza del uso de IA en las carreras de formación docente (Inglés, Educación Primaria, Educación Preescolar), con el objetivo de que sus egresados dominen estas herramientas y las apliquen en su práctica profesional [7]. Todo este impulso en la formación digital está generando una nueva generación de educadores y profesionales más competentes en tecnología. Según la visión del MICITT, invertir en estas competencias permitirá que Costa Rica cuente con el talento necesario para liderar proyectos de IA e innovación en el ámbito global [1], cerrando la brecha entre la educación superior y las demandas de la economía digital del siglo XXI.

III. ¿ESTÁ COSTA RICA LISTA PARA LA IA EN LA DOCENCIA?

Costa Rica se encuentra en un punto de inflexión frente al avance de la inteligencia artificial en el ámbito educativo. Por un lado, se señala que el uso de IA ya es una realidad cotidiana entre estudiantes universitarios, lo que obliga a las instituciones a tomar decisiones sobre su incorporación pedagógica y su regulación ética [10]. Se reconoce un creciente interés institucional, pero también una falta de políticas prácticas claras en algunas instituciones para guiar esta transición.

Por otro lado, se advierte sobre obstáculos estructurales y culturales más amplios: desde la resistencia al cambio en los modelos laborales hasta las brechas tecnológicas en zonas rurales, lo que limita la adopción plena de tecnologías emergentes como la IA. Aunque se plantean recomendaciones para fomentar una transformación digital inclusiva, el estudio concluye que el país aún enfrenta desafíos importantes en infraestructura, capacitación y visión estratégica [11].

En conjunto, los estudios revelan que Costa Rica tiene potencial, pero aún no está plenamente lista. El camino hacia una docencia universitaria apoyada por IA requiere superar rezagos institucionales y socioeconómicos, consolidar marcos normativos y fomentar una cultura de innovación educativa que sea ética, crítica e inclusiva.

IV. CONCLUSIONES

La incorporación de la inteligencia artificial en la educación superior costarricense marca un punto de inflexión en la manera en que concebimos la enseñanza, el aprendizaje y la gestión académica. En un corto periodo de tiempo, estas tecnologías han pasado de ser una posibilidad remota para convertirse en parte activa del quehacer diario universitario, impulsadas tanto por la aceleración digital de la pandemia como por la evolución natural del entorno tecnológico global. Este proceso ha revelado un sistema que, si bien ha demostrado voluntad de adaptarse, aún enfrenta importantes desafíos estructurales, éticos y culturales.

El impacto de la IA se manifiesta de manera transversal: transforma los métodos de enseñanza, exige nuevas formas de evaluación, redefine el rol docente y obliga a replantear políticas institucionales. Las universidades costarricenses han respondido con creatividad y compromiso, desarrollando estrategias innovadoras, guías éticas y programas de formación, pero al mismo tiempo persisten brechas importantes, especialmente en lo que respecta al acceso tecnológico en regiones periféricas y al uso inadecuado de estas herramientas por parte de quienes priorizan la aprobación por encima del aprendizaje.

La construcción de un ecosistema educativo equilibrado y éticamente sólido requiere más que infraestructura o normativas: exige un cambio cultural profundo. Un cambio que reconozca que la transformación digital no es solo técnica, sino esencialmente humana. Formar profesionales para un mundo atravesado por la IA implica educar también en valores, en pensamiento crítico y en responsabilidad social. No se trata de resistir la tecnología, sino de humanizarla, de integrarla de forma consciente en los procesos que nos definen como sociedad.

Podemos determinar dos grandes conclusiones con esta investigación:

A. La inteligencia artificial ya es parte activa de la educación universitaria en Costa Rica, pero aún falta una estrategia clara y equitativa para su implementación.

Uno de los hallazgos más visibles y relevantes es que la IA no es una posibilidad futura, sino una realidad actual en las aulas universitarias del país. Estudiantes ya la utilizan en actividades académicas cotidianas y las instituciones han comenzado a responder con guías, políticas y adaptaciones metodológicas. Sin embargo, este avance no ha sido homogéneo ni estructurado, lo que genera incertidumbre tanto en docentes como en autoridades sobre cómo regular su uso, asegurar la integridad académica y garantizar un acceso equitativo. El público general, especialmente estudiantes, docentes y padres de familia, debe comprender que el uso responsable de la IA requiere acompañamiento, formación ética y marcos institucionales sólidos, no solo herramientas tecnológicas.

B. La brecha digital y el cambio cultural son las principales barreras para una transformación educativa inclusiva y sostenible.

Aunque se registran esfuerzos importantes en capacitación y digitalización, la investigación evidencia que persisten fuertes desigualdades entre zonas urbanas y rurales, así como una cultura institucional que en algunos casos se resiste al cambio tecnológico. Esta situación pone en riesgo la equidad del sistema educativo, limitando el potencial transformador de la IA. El aporte aquí es una llamada de atención pública: si no se invierte con visión país en infraestructura, formación docente y cultura digital, Costa Rica corre el riesgo de quedarse atrás en el desarrollo educativo y profesional de su población.

Costa Rica cuenta con las capacidades, la visión y el talento para liderar este proceso de forma ejemplar, ya muchas instituciones como hemos visto a lo largo de este artículo tiene iniciativas fuertes y planificadas. La tarea ahora es colectiva: docentes, estudiantes, autoridades y comunidad académica debemos asumir el reto de transformar la educación sin perder la esencia que la hace valiosa. Porque al final, por más digital que sea el futuro, la educación seguirá siendo, sobre todo, un acto profundamente humano.

REFERENCIAS

[1] Universidad Americana (UAM), Informe 15: Inteligencia artificial y educación en Costa Rica: análisis de la estrategia nacional 2024-2027. Observatorio de la Educación, 2024. [En línea]. Disponible en: https://uam.ac.cr/observatorio-de-educacion/informes/15

[2] UNESCO, “Los gobiernos deben regular rápidamente la inteligencia artificial generativa en las escuelas”, 7 de septiembre de 2023. [En línea]. Disponible en: https://www.unesco.org/es/articles/unesco-los-gobiernos-deben-regular-rapidamente-la-inteligencia-artificial-generativa-en-las-escuelas

[3] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027. [En línea]. Disponible en: https://www.micitt.go.cr/gobierno_digital/inteligencia_artificial

[4] Salas Gómez, N., “Educación e inteligencia artificial: preservando la humanidad en la era de la automatización”, UNA Comunica, Universidad Nacional, Costa Rica, 23 de enero de 2025. [En línea]. Disponible en: https://www.unacomunica.una.ac.cr/index.php/enero-2025/5848-educacion-e-inteligencia-artificial-preservando-la-humanidad-en-la-era-de-la-automatizacion

[5] B. Ocampo Hernández, “La UCR a la vanguardia en virtualidad y uso pedagógico de las tecnologías”, 27 de septiembre de 2022. [En línea]. Disponible en: https://www.ucr.ac.cr/noticias/2022/9/27/la-ucr-a-la-vanguardia-en-virtualidad-y-uso-pedagogico-de-las-tecnologias.html

[6] A. Sánchez Agüero, “Expertos alertan sobre urgencia de crear políticas sobre inteligencia artificial”, Portal de la Investigación, 18 de febrero de 2025. [En línea]. Disponible en: https://vinv.ucr.ac.cr/es/noticias/expertos-alertan-sobre-urgencia-de-crear-politicas-sobre-inteligencia-artificial

[7] R. Zúñiga Sibaja, “Estudio liderado por director de Educación de U Fidélitas revela el impacto positivo de la inteligencia artificial en la educación costarricense”, Blog Universidad Fidélitas, 5 de agosto de 2024. [En línea]. Disponible en: https://ufidelitas.ac.cr/blog/educacion/impacto-de-la-inteligencia-artificial-en-la-educacion/

[8] K. Ramírez Chinchilla, “UNED lidera el camino hacia una IA responsable en la educación superior estatal de Costa Rica”, Acontecer UNED, Universidad Estatal a Distancia, 19 de julio de 2024. [En línea]. Disponible en: https://acontecer.uned.ac.cr/uned-lidera-el-camino-hacia-una-ia-responsable-en-la-educacion-superior-estatal-de-costa-rica/

[9] Instituto Tecnológico de Costa Rica (TEC), Foro: Inteligencia Artificial, implicaciones en la educación superior, 2024. [En línea]. Disponible en: https://www.tec.ac.cr/foro-inteligencia-artificial-implicaciones-educacion-superior

[10] A. Solano Segura, “¿Cómo está transformando la inteligencia artificial la educación universitaria en Costa Rica?”, Dos Tecnología y Negocios, 15 de mayo de 2025. [En línea]. Disponible en: https://www.dostecnologiaynegocios.com/2025/05/como-esta-transformando-la-inteligencia.html

[11] R. Rosales Robles, “Costa Rica y la próxima ola tecnológica: ¿Estamos preparados para el futuro del trabajo?”, Ciencia Latina, vol. 9, no. 2, pp. 1115–1129, 2024. [En línea]. Disponible en: https://doi.org/10.37811/cl_rcm.v9i2.16935

METODOLOGÍAS ÁGILES PARA EL DESARROLLO DE SISTEMAS

Licdo. Joseph Rodríguez Marín
MAP., Autor

RESUMEN

Cada día se escucha con más fuerza a nivel global el tema de la emergente utilización de metodologías ágiles para el desarrollo de software: versiones más recientes de libros de autores reconocidos en la ingeniería de software ya tocan este tema; además de los innumerables simposios que se realizan al respecto. Sin embargo: ¿Qué son las metodologías ágiles?, ¿qué nuevas implicaciones traen al desarrollo de software y en el cambio cultural de las organizaciones?, ¿qué tanto se conoce y que se está haciendo en Costa Rica al respecto? En el presente artículo, se pretende dar respuesta a estas interrogantes.

I. ¿QUÉ SON LAS METODOLOGÍAS ÁGILES?

El desarrollo ágil comprende un conjunto de metodologías para la creación de software, todas fundamentadas en principios comunes que giran en torno al denominado Manifiesto para el desarrollo ágil de software [1]. Este manifiesto establece que debe priorizarse la conformación del equipo por encima del entorno, las herramientas o los métodos. En consecuencia, el entorno del proyecto debe adaptarse al equipo responsable de su ejecución; se debe evitar la elaboración de documentación innecesaria, enfocándose en lo esencial; propiciar una colaboración constante entre el equipo y el cliente; y privilegiar la capacidad de adaptación frente a una adhesión estricta al plan inicial, el cual debe ser flexible y abierto, no rígido.

Asimismo, el Manifiesto se articula en torno a una serie de principios fundamentales, entre los cuales destacan: otorgar máxima prioridad a la entrega rápida de productos funcionales al cliente; acoger los cambios en los requisitos en cualquier fase del desarrollo, entendidos como una ventaja competitiva; entregar versiones operativas del software en intervalos breves; fomentar una colaboración estrecha entre desarrolladores y clientes; procurar que el software funcione desde la primera entrega; mantener un compromiso permanente con la excelencia técnica y el diseño de calidad, lo cual favorece la agilidad; y practicar la simplicidad, entendida como la capacidad de maximizar la cantidad de trabajo no realizado.

Dentro de este enfoque, las metodologías ágiles presentan diversas variantes o “sabores”, cada una con una perspectiva particular sobre cómo abordar el desarrollo de software. Entre ellas se encuentran:

- XP, “la programación extrema”, formulada por Kent Beck [2], pone más énfasis en la adaptabilidad que en la previsibilidad. Es decir, los cambios en los requisitos son inevitables y deben considerarse parte natural del proceso de desarrollo. Resulta irrealista intentar formular todos los requisitos desde el inicio, siendo lo fundamental fomentar una colaboración estrecha entre el desarrollador y el cliente. XP se basa en principios como los siguientes: el uso de historias de usuario, en las que el cliente describe brevemente, mediante tarjetas físicas, las características que el sistema debe poseer; la definición de los roles del equipo; y un proceso de desarrollo orientado a iteraciones breves, con el objetivo de entregar software funcional con rapidez. Los principios fundamentales de la programación extrema son: simplicidad, comunicación, retroalimentación y “mucho coraje”.
- Scrum, finalmente formalizado por Ken Schwaber [2], describe, mediante un enfoque ágil, la gestión y el control de desarrollos complejos de software y productos, utilizando prácticas iterativas e incrementales. SCRUM promueve el desarrollo en iteraciones breves (sprints) de no más de un mes, durante las cuales se crea un incremento de software operativo. Las características priorizadas para desarrollar (backlog) durante el sprint son definidas por el dueño del producto (Product Owner), quien las comunica al equipo. Al finalizar el sprint, el equipo presenta el incremento funcional del software.

Scrum propone la organización de equipos auto-dirigidos que realizan reuniones breves, pero altamente efectivas conocidas como scrums diarios, en las que se revisa el avance del proyecto. Durante el sprint, el cliente se integra al equipo; se elaboran planes para la identificación y mitigación de riesgos a lo largo del proceso, y se fomenta la transparencia respecto a las responsabilidades de cada miembro ("todos saben qué tiene a cargo cada uno"). Las reuniones de avance son frecuentes y deben existir mecanismos tempranos de advertencia: los problemas "no se barren bajo la alfombra". Al concluir el sprint, se realiza una sesión de retroalimentación conocida como retrospectiva.

Fig. 1. Flujo de SCRUM [2].

- Otros métodos ágiles incluyen el Desarrollo de Sistemas Dinámico (Dynamic Systems Development Method, DSDM), Crystal Clear, Agile Unified Process (AUP), así como prácticas ágiles específicas como Test-Driven Development (TDD) y Pair Programming.

II. ¿CUÁLES NUEVAS IMPLICACIONES TRAE LA UTILIZACIÓN LAS METODOLOGÍAS ÁGILES AL DESARROLLO DE SOFTWARE Y A LAS ORGANIZACIONES?

El desarrollo ágil parte del principio de generar únicamente la documentación mínima necesaria. Las organizaciones actuales tienen arraigada la costumbre de producir documentación para todo, muchas veces de forma excesiva. El formato y volumen de esta documentación han sido, en muchos casos, definidos por requerimientos de auditoría. No sorprende, entonces, que el desarrollo ágil proponga, en primera instancia, que el entorno debe adaptarse al equipo, especialmente cuando el cliente forma parte activa de dicho equipo.

- Las metodologías: El paradigma tradicional, usualmente conocido como modelo en cascada -aún el más utilizado - da paso a iteraciones mucho más breves, en las que el cliente recibe versiones funcionales del producto en lapsos máximos de un mes, según lo establece Scrum. Esta dinámica favorece una mayor calidad del producto, al menos desde la perspectiva de aceptación, ya que el cliente puede visualizar el producto de forma anticipada y, en consecuencia, aprobarlo o solicitar adaptaciones sin que esto implique un impacto severo en el software ya construido [3]. Las metodologías ágiles, además, resultan más comprensibles que otras más voluminosas y complejas en sus principios y procedimientos.
- Los estimados: Es difícil generar estimaciones realistas del proyecto si no se dispone de una visión completa de los requisitos desde el inicio -*"es difícil ver el bosque cuando solo se ve un árbol"-*. Este es un aspecto que debe mitigarse si se pretende utilizar metodologías ágiles, las cuales proponen iniciar el desarrollo sin conocer en detalle todos los requerimientos del sistema.
- El control de cambios: En el enfoque ágil, el cambio es considerado parte natural del proceso y, por tanto, inevitable. Esto convierte la gestión del cambio en un reto constante para los desarrolladores.
- El cliente como parte del desarrollo: En metodologías como Scrum, la participación continua del cliente en múltiples iteraciones (sprints) puede volver el proceso costoso para este, además de requerir una mayor presencia y compromiso por parte del usuario.
- Diseño del software: Los métodos ágiles promueven el uso exclusivo de la documentación esencial, lo cual, llevado al extremo, podría derivar en un diseño insuficiente. "Un problema no técnico de la metodología es cuando los clientes del sistema utilizan una organización externa para el desarrollo" [4]. Esta situación se complica si no existe documentación suficiente, lo cual dificulta, por ejemplo, la redacción de contratos entre el cliente y el proveedor en ausencia de un documento de requerimientos formal.
- Cambio cultural: Este es un aspecto que la organización debe abordar previamente si desea implementar con éxito una metodología ágil.
- Requiere valentía: Se necesita determinación para sustituir código ya desarrollado en función de cambios en los requisitos surgidos durante el proceso.

ISSN: 2015-5392

III.¿QUÉ TANTO SE CONOCE Y QUE SE ESTÁ HACIENDO EN COSTA RICA AL RESPECTO?

De acuerdo con el Manifiesto para el desarrollo ágil de software:

> *En entrevista al señor Tomás Araya, encargado del Departamento de TI – Innovaplant de Costa Rica, él comenta: Estamos muy convencidos con la programación extrema ya que los tiempos de respuesta a una solicitud en cuanto un proyecto son más cortos y esto nos ahorra tener que contratar más ingenieros, y lograr desarrollar más proyectos en corto tiempo, actualmente nosotros utilizamos este método para el 100% de los proyectos y no hemos tenido problema alguno, hemos visto que los riesgos o errores son más fáciles de corregir, si presentamos primero un ejemplo al usuario final y que este decida si así está bien o desea una modificación, el método nos permite programar rápido, dejando un poco de lado la documentación [5].*

Para los fines de este artículo, se llevó a cabo una breve investigación sobre el uso de metodologías ágiles entre estudiantes de la Universidad Latina, campus Heredia, en el nivel de licenciatura de la carrera de Ingeniería en Sistemas, así como en un par de otras universidades [6]. Los resultados fueron los siguientes:

Fig. 2. Metodología ágil que más utilizan es Scrum [6].

Fig. 3. Lugar en el que se aprende de la metodología ágil [6].

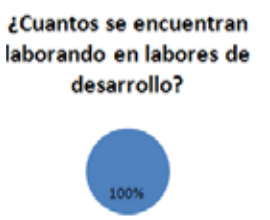


Fig. 4. Cantidad de personas que se encuentra laborando en desarrollo [6].

Fig. 5. Manera en la que definen metodología ágil [6].

En efecto, en la actualidad, las empresas e instituciones utilizan con mayor frecuencia Scrum, al tratarse de una metodología ágil para el desarrollo tanto del proyecto como del producto.

IV. CONCLUSIONES

- Cambio cultural de las organizaciones: Este es un factor fundamental para implementar con éxito las metodologías ágiles. La organización debe ser capaz de seleccionar, entre las distintas opciones disponibles, aquella metodología que mejor se ajuste a las características de su proyecto. Debe alcanzarse el principio de que el entorno se define en función del equipo, y no a la inversa.

- Documentación: El uso de metodologías ágiles no implica necesariamente la ausencia total de documentación, sino la producción de la documentación estrictamente necesaria. Lo que se debe procurar es un enfoque práctico. Desde la perspectiva de este autor, en aras de garantizar la calidad, es indispensable documentar adecuadamente los modelos requeridos.

- ¿Cero calidad?: Las metodologías ágiles, al promover principios como el trabajo en equipo, la comunicación, la simplicidad, la planificación, la mitigación de riesgos, la entrega temprana al cliente en iteraciones cortas y la clara definición de roles y responsabilidades, contienen elementos que apoyan el logro de la calidad. “XP es un enfoque para el desarrollo de software que utiliza buenas prácticas de desarrollo y las lleva a los extremos. Se basa en valores, principios y prácticas esenciales” [7].

- Conocimiento experto: Dado que la documentación es mínima y que se trabaja con una entrega ágil de productos en función de un orden priorizado de requerimientos, se vuelve fundamental el conocimiento previo del equipo, por ejemplo, en cuanto a reglas de negocio. Una estrategia para mitigar riesgos consiste en integrar expertos directamente en el proceso. No está de más reiterar que un factor crítico para lograr agilidad es el conocimiento especializado del propio equipo de desarrollo.

- Como en las demás metodologías, siempre se seguirá Recurso humano: Al igual que en otras metodologías, el éxito sigue dependiendo de las actitudes y aptitudes del recurso humano.

La dependencia del usuario, más crítica en el enfoque ágil, debe medirse y equilibrarse antes de iniciar el desarrollo; por ejemplo, designando usuarios expertos con capacidad de decisión. “La programación extrema es un método ágil conocido que integra una variedad de buenas prácticas de programación, como las pruebas sistemáticas, la continua mejora del software y la participación del cliente en el equipo de desarrollo” [4].

- Entrega y desarrollo rápido: En muchos casos, la entrega oportuna de sistemas nuevos puede ser más valiosa para las empresas que contar con una funcionalidad completamente detallada desde el inicio.

- Enfoque iterativo y producción: Por sus principios, las metodologías ágiles permiten al equipo enfocarse en la producción de software funcional. Sommerville [4] recomienda que, “al crecer la presión por una entrega rápida del software, se utiliza cada vez más un enfoque iterativo para el desarrollo del software como una técnica de desarrollo estándar para sistemas pequeños y de tamaño medio, especialmente en el dominio de los negocios” [4].

REFERENCIAS

[1] K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, S. Mellor, K. Schwaber, J. Sutherland y D. Thomas, Manifiesto por el Desarrollo Ágil de Software, 2001. [En línea]. Disponible en: https://agilemanifesto.org/iso/es/manifesto.html

[2] Laboratorio Nacional de Calidad del Software, Metodologías de desarrollo de software. En Ingeniería del software: Metodologías y ciclos de vida, pp. 39–43, INTECO, España, 2009.

[3] S. R. Pressman, Ingeniería de software: un enfoque práctico, McGraw-Hill, 2006.

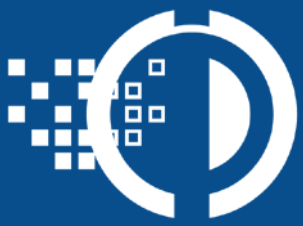
[4] I. Sommerville, Ingeniería de software, 7.ª ed., Addison Wesley, 2005.

[5] A. Céspedes, entrevista, Innovaplant de Costa Rica, 16 de julio de 2013.

[6] J. Rodríguez, Resultados encuesta: Utilización de metodologías ágiles, 2013, inédito.

[7] K. E. Kendall y J. E. Kendall, Análisis y diseño de sistemas, 6.ª ed., Pearson Educación, 2005.

ISSN: 2015-5392



CPIC

COLEGIO DE PROFESIONALES EN
INFORMÁTICA Y COMPUTACIÓN