RIIF

INGENIERÍA E INNOVACIÓN DEL FUTURO

VOL.2 NÚM.1
2023
ENERO - JUNIO

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023

CONTENIDO

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023

PÁGINA LEGAL

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023

PERIODICIDAD DE PUBLICACIÓN Semestral – publicación continua

enero-junio

ENTIDAD EDITORA Editorial Scientific Future

info@editorialscientificfuture.com

(593) 98 289 5312

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

Explorando la Intersección Tecnológica: Lenguajes de Programación, Inteligencia Artificial y Teleoperación Robótica

Exploring the Technological Intersection: Programming Languages, Artificial Intelligence and Robotic Teleoperation

Fecha de recepción: 2023-01-10 • Fecha de aceptación: 2023-03-23 • Fecha de publicación: 2023-04-05

Anthon Gallo[1], Cristopher Trujillo[1], Jesael Maila[1]
[1] Universidad Israel, Quito, Ecuador
e1726439563@uisrael.edu.ec, e1751492545@uisrael.edu.ec, e1754563946@uisrael.edu.ec

Resumen,,

Este análisis investiga las cruciales intersecciones tecnológicas en la contemporaneidad, explorando temáticas entrelazadas que abarcan la evolución de los lenguajes informáticos, el comportamiento del consumidor frente a la inteligencia artificial (IA), y el desarrollo de vehículos robóticos teleoperados que complementan las anteriores áreas tecnológicas. Desde la diversidad de lenguajes de programación hasta su aplicación en el desarrollo de la IA y el progreso tangible en vehículos robóticos, se examinan cuestiones clave. La investigación exploratoria sobre el aprendizaje de programación identifica patrones en distintos grupos etarios, enriqueciendo el conocimiento social y resaltando los beneficios y aplicaciones en el ámbito tecnológico. Se analiza el impacto de la IA, desde su percepción inicial hasta su integración en la sociedad, destacando tanto sus beneficios como los desafíos éticos asociados. La presentación de un prototipo de carro robot teleoperado con tecnología ESP 32 subraya la aplicabilidad práctica de la tecnología en ámbitos críticos. El ensayo cierra con reflexiones sobre el futuro y la necesidad de estándares avanzados, proporcionando una visión integral de las intersecciones tecnológicas y su repercusión en la sociedad.

Palabras clave

Evolución, lenguajes informáticos, inteligencia artificial, comportamiento del consumidor, vehículos robóticos teleoperados, tecnología

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

Abstract

This analysis investigates the crucial technological intersections of today, exploring intertwined themes that encompass the evolution of computer languages, consumer behavior in the face of artificial intelligence (AI), and the development of teleoperated robotic vehicles that complement the previous technological areas. From the diversity of programming languages to their application in AI development and tangible progress in robotic vehicles, key questions are examined. Exploratory research on programming learning identifies patterns in different age groups, enriching social knowledge and highlighting the benefits and applications in the technological field. The impact of AI is analyzed, from its initial perception to its integration into society, highlighting both its benefits and the associated ethical challenges. The presentation of a prototype of a teleoperated robot car with ESP 32 technology highlights the practical applicability of the technology in critical areas. The essay closes with reflections on the future and the need for advanced standards, providing a comprehensive vision of technological intersections and their impact on society.

Keywords

Evolution, computer languages, artificial intelligence, consumer behavior, teleoperated robotic vehicles, technology

Introducción

La tecnología desde la prehistoria hasta nuestro tiempo actual ha sido considerada una de las mayores y mejoradas herramientas que pudo haber creado la humanidad, desde la construcción de herramientas de piedra, uso del fuego, invención de la rueda hasta computadoras, internet, dispositivos electrónicos, etc., todas estas creaciones han sido para satisfacer cada una de las necesidades humanas y también es la solución a cualquier problema [1].

El conjunto de términos diseñados específicamente para facilitar la comunicación a través de computadoras en el ámbito de la informática ha experimentado un crecimiento exponencial a lo largo de los años, convirtiéndose en la piedra angular de la tecnología contemporánea.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

Este lenguaje especializado ha evolucionado para abordar las complejidades y demandas de la informática, dando origen a un vasto y dinámico vocabulario que sustenta la interacción digital [2].

El estudio de mercado para determinar el comportamiento del consumidor relacionado al uso de la Inteligencia Artificial (IA) forma parte de un tema importante dentro del seguimiento del mercado. A lo largo de las décadas la IA ha experimentado una evolución significativa, desde su primera aparición en 1920 hasta lo que en 2023 consideramos una IA General. Este análisis tiene como objetivo explorar la trayectoria evolutiva de la IA y su impacto en los consumidores, examinando su vinculación con la sociedad y tanto los beneficiarios directos como también indirectos, asimismo se abordarán los diferentes tipos de inteligencia artificial, desde la IA estrecha hasta la perspectiva de la Super IAc[3].

Esta tecnología sigue revolucionando distintos sectores personales y profesionales a lo cual su amplia posibilidad de aplicación, organización y creación que engloba datos y modelos a gran escala para el uso de actividades cotidianas, la inteligencia artificial tiene capacidad para "generalizar un modo indicado, basado en datos escasos".

Existen vehículos robóticos teleoperados que combinan la movilidad de un vehículo a control remoto y un robot, tiene ciertas características como exploración de desastres, seguridad, inspección de infraestructura y asistencia médica. Se implementa un proceso de prototipo de carro robot teleoperado con tecnología ESP 32 especializado en la investigación del canal WIFI teniendo en cuenta la cobertura, pérdida de paquetes y latencia. Determina el objetivo del trabajo. Se incluye sobre qué se basó el trabajo, en este caso, el nombre de la ponencia seleccionada e incluir una idea innovadora[4]**.**

Cuerpo

La diversidad lingüística global se refleja de manera única en la variada existencia de lenguajes de programación. Estos lenguajes sirven como herramientas fundamentales, abriendo un abanico de posibilidades que impulsa la innovación constante en el desarrollo de software. Desde simples scripts hasta complejas aplicaciones, los programadores utilizan estos lenguajes para materializar ideas y abordar problemas de manera eficiente.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

La intersección entre la evolución del lenguaje informático y la proliferación de lenguajes de programación crea un entorno dinámico y colaborativo. El constante surgimiento de nuevas tecnologías y paradigmas de programación refleja la adaptabilidad y expansión continua de la informática, contribuyendo significativamente al progreso tecnológico en diversos sectores de la sociedad.

Datos compartidos por Madridiario y Stack Overflow revelan patrones y tendencias en el interés y participación en el aprendizaje de lenguajes de programación en diferentes rangos de edad. Este análisis exploratorio busca arrojar luz sobre la relación entre la edad y el proceso de aprendizaje de programación, proporcionando valiosos insights para la comunidad educativa y los profesionales del sector tecnológico [5].

Esta iniciativa busca arrojar luz sobre la relación entre la edad y el proceso de aprendizaje de programación, proporcionando insights valiosos que pueden beneficiar a la comunidad educativa, a los profesionales del sector tecnológico y a cualquier persona interesada en comprender mejor las dinámicas asociadas al desarrollo de habilidades en programación.

La divulgación de estos datos no solo contribuye al conocimiento general sobre la educación en programación, sino que también fomenta la reflexión y el análisis crítico en torno a la influencia de factores como la edad en la adopción de habilidades tecnológicas. Este enfoque exploratorio representa un paso fundamental hacia la comprensión más profunda de las dinámicas educativas en la programación, promoviendo un diálogo informado y enriquecedor en la comunidad [6].

El comportamiento del consumidor frente a la IA ha sufrido una enorme transformación significativa. En algunos casos, la sociedad ha aceptado la presencia de la IA y se ha vuelto tendencia en el contexto académico y comercial. Desde la desconfianza inicial hasta su aceptación, son los consumidores quienes más la apoyan y valoran los beneficios que ofrece, adaptando sus necesidades que empiezan por tareas simples, como resolver un deber, hasta contribuir en la oferta de bienes y servicios.

Sin embargo, existen detractores que se oponen a su uso, como es el caso de profesores y analistas internacionales, que argumentan que la IA genera dependencia, evita el desarrollo

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

de capacidades personales y, en un futuro podría terminar con el empleo de 300 mil trabajadores.

En el ámbito de la inteligencia artificial (IA), el comportamiento del consumidor ha experimentado una transformación significativa. Desde la desconfianza inicial hasta su aceptación generalizada, la sociedad ha adoptado la IA en contextos académicos y comerciales. Los consumidores valoran los beneficios que ofrece, desde resolver tareas simples hasta contribuir en la oferta de bienes y servicios. Sin embargo, existen detractores, como profesores y analistas internacionales, que argumentan que la IA genera dependencia y podría poner en riesgo empleos.

La integración de la IA en la sociedad ha alterado las preferencias de consumo, desde la creación de asistentes virtuales hasta su uso autónomo en procesos industriales, generando beneficios considerables, pero también planteando desafíos éticos y sociales. A su vez la evolución de las IA abarca las etapas de desarrollo que se han presentado y los hitos por los que se ha visto marcada, desde las primeras máquinas de cálculo hasta los algoritmos de aprendizaje sin embargo el impacto más importante se presenta en 1920, cuando por primera vez aparecía el concepto de máquina inteligente capaz de imitar el comportamiento humano, conocida como “máquina enigma” [7]

Entre 1950 y 1960 se desarrollaron los primeros programas de IA, como el “Test de Turing” en 1950, el programa “Logic Theorist” 1956, el “General Problem Solver” en 1958 y “SAIL Lenguaje AI” en 1960; sin embargo, las limitaciones tecnológicas y falta de datos restringían su progreso. Más allá de ser la novedad en aquel entonces, fue en décadas siguientes que, con mejores recursos y mayor cantidad de información se vio su mayor etapa de evolución.

A partir del siglo XXI aparecen programas como “Deep Learning”, “Siri”, “IBM Watson” (IA con capacidad de responder preguntas complejas), “FAIR”, “Robot Sophia”, “Alpha Go”, Waymo” y “Chat GPT”. En 2023, la IA se utiliza ampliamente en la oferta de productos y servicios, se distinguen tipos de IA, desde la estrecha hasta la superinteligencia, que plantea la posibilidad de una "Cuarta Revolución Industrial" [8]

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

La metodología experimental se utiliza en el desarrollo de prototipos, abordando aspectos mecánicos, sensores, controladores y la fuente de energía. La integración de elementos, como la ejecutabilidad para pruebas de usabilidad y el análisis de parámetros del canal Wifi, se considera para el sistema de teleoperaciones. Las consideraciones incluyen la electrónica del prototipo, configuraciones de red Wifi, y el desarrollo de aplicaciones Android e interfaces web para video. El análisis de resultados se centra en pruebas de interfaz y funcionamiento, desde la dirección IP de ESP 32 hasta controles de velocidad, giros y transmisión de video en tiempo real a través de ESP 32 CAM [9]

Este amplio panorama abarca desde la diversidad lingüística en la programación hasta las complejidades éticas y prácticas de la inteligencia artificial, demostrando la interconexión de estos temas en la vanguardia tecnológica actual.

Conclusiones

En resumen, la diversidad de lenguajes de programación impulsa la innovación, dotando a los programadores de herramientas eficientes. La colaboración entre Madridiario y Stack Overflow en la investigación de rangos de edad en el aprendizaje de programación enriquece el conocimiento universal y promueve un diálogo informado en la comunidad tecnológica. La exploración del impacto de la inteligencia artificial en el comportamiento del consumidor plantea la pregunta intrigante sobre el futuro con una superinteligencia artificial impulsando una cuarta revolución industrial.

Dirigiéndose al desarrollo de vehículos robóticos teleoperados, destaca la importancia de estándares como el 802.11n para la confiabilidad en la transmisión de vídeo en tiempo real. Se propone la implementación de tecnologías como Wifi 6 y la exploración de protocolos como el 5G NR, planteando cómo aprovechar estas innovaciones para comprender mejor el ecosistema de desarrollo e innovación. En conjunto, estas conclusiones refuerzan la noción de que las intersecciones tecnológicas catalizan avances de gran impacto en la sociedad, destacando la diversidad, la colaboración y la anticipación de futuras tecnologías como elementos clave en la era tecnológica actual.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

Lo que nos lleva a la siguiente pregunta ¿Afectaría al humano un posible futuro donde podamos llegar a presenciar el nacimiento de una cuarta revolución industrial impulsada por la Super IA y la tecnología?

Referencias

[1] C. M. G. Paredes, C. Machuca, and Y. M. S. Claudio, "ChatGPT API: Brief overview and integration in Software Development," *International Journal of Engineering Insights*, vol. 1, no. 1, pp. 25–29, 2023.

[2] H. Alvarez and R. Toasa, "Usability and sophistication of websites: A path to satisfaction in online retail," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, vol. 2020, no. E34, 2020.

[3] E. Iglesias Rodríguez, A. García Zaballos, P. Puig Gabarró, and I. Benzaquén, "Inteligencia artificial: Gran oportunidad del siglo XXI: Documento de reflexión y propuesta de actuación," *Inteligencia artificial: Gran oportunidad del siglo XXI: Documento de reflexión y propuesta de actuación*, Dec. 2020, doi: 10.18235/0003037.

[4] H. Güvenç, "Wireless ECG Device with Arduino," *TIPTEKNO 2020 - Tip Teknolojileri Kongresi - 2020 Medical Technologies Congress, TIPTEKNO 2020*, Nov. 2020, doi: 10.1109/TIPTEKNO50054.2020.9299248.

[5] G. R. T. White and A. Samuel, "Programmatic Advertising: Forewarning and avoiding hype-cycle failure," *Technol Forecast Soc Change*, vol. 144, pp. 157–168, Jul. 2019, doi: 10.1016/J.TECHFORE.2019.03.020.

[6] L. R. Abbade, M. A. A. da Cruz, J. J. P. C. Rodrigues, P. Lorenz, R. A. L. Rabelo, and J. Al-Muhtadi, "Performance comparison of programming languages for Internet of Things middleware," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3891, Dec. 2020, doi: 10.1002/ETT.3891.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

[7] P. Cinthya, Z. Cisneros, R. Carlos Jiménez Martínez, M. Ricardo Velázquez, D. Rafael, and A. Santamaría, "Inteligencia artificial: desafíos para el marco normativo laboral ecuatoriano," *Universidad y Sociedad*, vol. 13, no. S3, pp. 340–345, Dec. 2021, Accessed: Oct. 05, 2022. [Online]. Available: https://rus.ucf.edu.cu/index.php/rus/article/view/2487

[8] I. Rizwan I Haque and J. Neubert, "Deep learning approaches to biomedical image segmentation," *Inform Med Unlocked*, vol. 18, p. 100297, Jan. 2020, doi: 10.1016/J.IMU.2020.100297.

[9] A. L. de Oliveira, W. A. Gonçalves, and R. M. Hoed, "Arduino: uma proposta para o ensino Introdutório de programação C/C++," *Latin American Journal of Development*, vol. 3, no. 4, pp. 2288–2296, Jul. 2021, doi: 10.46814/LAJDV3N4-038.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.6

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

La inteligencia artificial de la mano de la realidad aumentada dentro del consumidor

Artificial intelligence hand in hand with augmented reality within the consumer.

Fecha de recepción: 2023-02-03 • Fecha de aceptación: 2023-04-05 • Fecha de publicación: 2023-04-14

Steven David Freire Cadena[1] and Julio Cesar Rodríguez Torres[2]
[1] Universidad Tecnológica Israel, Quito, Ecuador
e1718076217@uisrael.edu.ec, e1718076217@uisrael.edu.ec

Resumen

Teniendo una visión global de lo que está viviendo la humanidad, hoy en día enfocando su contextualización del asunto, en el foro económico mundial, el señor Klaus Schwab presidente y fundador del foro económico mundial en el año 2015, escribió el libro que se llama la cuarta revolución industrial. Él plantea que vamos a un mundo inteligente donde todo va a estar programado, planificado, donde las máquinas se van a fusionar y nos van a controlar nuestra actividad para irnos guiando, en pocas palabras, aunque tengamos una libertad, nosotros reaccionamos a cómo nos están guiando los dispositivos y los elementos inteligentes. Básicamente, estamos guiados por un mundo inteligente en el cual nos insertan a nosotros y nosotros vivimos en este mundo, de ahí va el tema del libro de la cuarta revolución industrial con las ciudades inteligentes. La realidad aumentada va a ir evolucionando cada año y actualmente ya existen gafas que pueden tener una doble pantalla y cuando detectan algo en realidad nos va a aparecer en las gafas. Dentro de este contexto, se introduce la inteligencia artificial como un medio para evaluar el comportamiento del cliente. A través del empleo adecuado de diversas herramientas adquiridas por esta tecnología, las empresas de manufactura de la industria de la menor demanda pueden brindar a sus clientes una experiencia de compra satisfactoria, tanto en tienda como en la plataforma web.

Palabras clave

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

Inteligencia artificial, realidad aumentada, innovación, interacción, convergencia, simulación, predicción y experiencia.

Abstract

Having a global vision of what humanity is living, today focusing on its contextualization of the matter, in the World Economic Forum, Mr. Klaus Schwab, president and founder of the World Economic Forum in 2015, wrote a book called the fourth industrial revolution. He states that we are going to an intelligent world where everything will be programmed, planned, where machines will merge and will control our activity to guide us, in short, although we have a freedom, we react to how the devices and intelligent elements are guiding us. Basically, we are guided by an intelligent world in which we are inserted and we live in this world, hence the theme of the book of the fourth industrial revolution with smart cities. Augmented reality is going to evolve every year and currently there are already glasses that can have a double screen and when they detect something it will actually appear on the glasses. Within this context, artificial intelligence is introduced as a means to evaluate customer behavior. Through the proper use of various tools acquired by this technology, manufacturing companies in the off-premise industry can provide their customers with a satisfactory shopping experience, both in-store and on the web platform.

Keywords

Artificial intelligence, augmented reality, innovation, interaction, convergence, simulation, prediction, and experience.

Introducción

Analizar el comportamiento del consumidor frente a la utilización de la inteligencia artificial y la realidad aumentada en los servicios, es un tema de mucha importancia para las organizaciones públicas y privadas del mundo.

Se define a la inteligencia artificial como un conjunto de tecnologías, soluciones o sistemas que se han concebido con el objetivo de imitar las aptitudes cognitivas del ser humano y su forma de abordar las resoluciones de problemas[1].

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

Se estructura en algoritmos que se establecen con el propósito de que un ordenador aprenda de forma automática mediante datos y experiencia, de la misma manera que una persona podría hacerlo. Estas técnicas de aprendizaje posibilitan que los ordenadores aprendan de forma gradual y cada vez de forma más independiente, apoyándose en ejemplos, y a desarrollar su propia lógica y resultados sin necesidad de ser supervisados [2].

Los programadores y desarrolladores de software están incorporando estas tecnologías en sus aplicaciones, siendo las móviles las que han tenido un ascenso emergente muy rápido en los últimos años[3]. La mayoría de las habilidades de informática de la inteligencia artificial se encuentran relacionadas con su capacidad para utilizar información que ya disponemos y con ella generar información que antes no teníamos.

Por otro lado, la realidad virtual y aumentada tiene un auge significante y últimamente están siendo utilizadas en distintas tareas de marketing y comercio electrónico [4].

Se ubicaba en el mundo científico desde el comienzo de los años 90, cuando la tecnología se enfocaba en los ordenadores de procesamiento rápido, la ejecución de gráficos en tiempo real y los sistemas de seguimiento de precisión portables, lo cual posibilita la implementación y combinación de imágenes generadas por computadoras sobre la perspectiva del mundo real [5].

Los proyectos etiquetados como realidad aumentada no han terminado de incrementarse en los últimos años. Existen diversas definiciones de la realidad aumentada y todas ellas presentan un aspecto interesante en la caracterización de este tipo de tecnología.

La inteligencia artificial y la realidad aumentada disminuyen significativamente el esfuerzo y el tiempo necesario para buscar productos, debido a que permiten el acceso al inventario en línea. Sin embargo, esto requiere que las organizaciones mantengan actualizaciones constantes y precisas de su lista en tiempo real, una tarea que puede ser costosa y que requiere una logística eficiente.

El hecho de poder acceder a las críticas y comparaciones de los productos a través de la realidad aumentada puede brindar a los consumidores una mayor seguridad en su elección, en comparación con las tiendas que no ofrezcan esta experiencia. No obstante, la precisión y

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

la autenticidad de tales críticas pueden ser cuestionadas y, por lo tanto, deben ser administradas de manera responsable por los minoristas.

Aunque es cierto que muchos clientes utilizan la tecnología en su existencia diaria, también existe una parte significativa de la población que pueden ser agilizada a adoptar tales progresos. En consecuencia, las organizaciones que implementen esta tecnología deben estar dispuestas a invertir en educación del consumidor y asistencia técnica para simplificar la transición [6].

Los clientes pueden fomentar la promoción de las tiendas que ofrecen experiencias de aprendizaje de tecnologías de aprendizaje y aprendizaje, lo que puede otorgar una ventaja competitiva a las empresas que adopten estas tecnologías. No obstante, las organizaciones de larga duración que no pueden utilizar estas tecnologías debido a costos o barreras técnicas pueden tener un peligro de desventaja.

Cuerpo

Se pretende diseñar una aplicación de Realidad Aumentada (R.A.) basado en la aplicación de inteligencia artificial, que brinde una experiencia de compra personalizada para los clientes de manera más eficaz y atractiva. Los clientes podrían dirigir la cámara de su teléfono hacia los productos en la tienda o incluso hacia los elementos que se encuentran dentro de su hogar. La aplicación buscará los productos y proporcionará información importante como reseñas, comparación de precios, recomendaciones personalizadas basadas en las preferencias del consumidor y sugerencias de productos.

Además, la aplicación podría incluir un asistente de compra con habilidades de inteligencia estudiadas. Este especialista respondería a las cuestiones de los clientes, brindará recomendaciones acerca de sus adquisiciones anteriores y directrices de máquinas de aprendizaje, y facilitaría el proceso de pago una vez que el cliente esté dispuesto a hacer una compra.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

La aplicación de esta aplicación no solo mejoraría la experiencia de compra para los clientes, sino que también brindará a los clientes una amplia gama de datos reveladores acerca del comportamiento del consumidor en la tienda, lo cual podría ser utilizado para optimizar el diseño de la tienda y las estrategias de marketing futuras.

Esta iniciativa innovadora aún evidencia la conexión del comercio electrónico con la gratificación instantánea de las compras físicas, lo cual podría modificar la experiencia de compra de menor tamaño en el futuro.

Se requiere que los sistemas de inteligencia artificial brinden una comprensión precisa a los creadores, los titulares de derechos y los usuarios. Es importante que los diseñadores y ejecutadores de sistemas de inteligencia artificial lleven a cabo una exhaustiva investigación detallada de las publicaciones editoriales y metadatos asociados, así como la base legal a la que se ha obtenido a ella. Asimismo, es imperativo que los editores proporcionen la información necesaria a los editores en el menor plazo posible con el fin de asegurarse de que su contenido sea incluido en los datos de capacitación [7].

Conclusiones

En conclusión, la inteligencia artificial se ha convertido en un factor clave que impacta en el comportamiento del consumidor y en cómo las empresas interactúan con sus clientes. Permite personalizar la experiencia del consumidor como nunca antes. Se emplean algoritmos de aprendizaje automático, mediante los cuales las marcas pueden proporcionar recomendaciones de productos, contenido y servicios personalizados para los usuarios, lo que incrementa la satisfacción del cliente y mejora la retención.

Las organizaciones pueden brindar una experiencia a la cliente enriquecida, con chatbots automatizados capaces de brindar asistencia en tiempo real, redes de aprendizaje profundo que permiten el reconocimiento de voz para la búsqueda por voz y asistentes virtuales.

Con el uso de esta tecnología, las organizaciones pueden anticipar con mayor precisión el comportamiento futuro del consumidor, lo cual les posibilita aprovechar estas perspectivas para diseñar estrategias de marketing y ventas más eficaces.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

Se puede optimizar el proceso de compra para los clientes, desde la investigación de productos hasta el pago, lo cual puede generar una experiencia del usuario más eficaz y sencilla de utilizar. A medida que los consumidores se familiarizan con la eficiencia y personalización que esta tecnología puede ofrecer, sus expectativas con respecto a las experiencias de servicio y compra están evolucionando.

Referencias

[1] Y. Xu *et al.*, "Artificial intelligence: A powerful paradigm for scientific research," *The Innovation*, vol. 2, no. 4, Nov. 2021, doi: 10.1016/J.XINN.2021.100179.

[2] J. F. Pabon, M. Aizaga, H. Recalde, and R. M. Toasa, "Revisión de literatura sobre impacto de la inteligencia artificial y su aplicación en el Ecuador," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E55, pp. 100–113, 2023.

[3] D. Corral, R. M. Toasa, Y. Semblantes, and L. F. Aguas, "Propuesta de App Móvil para la gestión de incidentes de tránsito," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E55, pp. 67–76, 2023.

[4] O. R. Toasa, Y. Semblantes, D. Martínez, P. Baldeón, and R. M. Toasa, "Virtual Reality in E-commerce: Brief Review of Current State," *Smart Innovation, Systems and Technologies*, vol. 344, pp. 647–655, 2024, doi: 10.1007/978-981-99-0333-7_47/COVER.

[5] R. Yung and C. Khoo-Lattimore, "New realities: a systematic literature review on virtual reality and augmented reality in tourism research," *https://doi.org/10.1080/13683500.2017.1417359*, vol. 22, no. 17, pp. 2056–2081, 2017, doi: 10.1080/13683500.2017.1417359.

[6] A. Moreno, D. Martinez, E. Fabián Rivera, and G. Renato Mauricio Toasa, "Starting an E-commerce in Pandemic Times to Ecuador: A Review of the Current State of Affairs," *Smart Innovation, Systems and Technologies*, vol. 280, pp. 635–644, 2022, doi: 10.1007/978-981-16-9272-7_52/COVER.

[7] E. F. Rivera, E. E. Morales, C. C. Florez, and R. M. Toasa, "Development of an Augmented Reality System to Support the Teaching-Learning Process in Automotive

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

Mechatronics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12980 LNCS, pp. 451–461, 2021, doi: 10.1007/978-3-030-87595-4_33/TABLES/1.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.7

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Procesos y Algoritmos que Netflix utiliza para la recolección de información

Processes and Algorithms Netflix uses for data collection.

Fecha de recepción: 2023-03-15 • Fecha de aceptación: 2023-05-03 • Fecha de publicación: 2023-05-26

Victoria Flores[1]
[1] Universidad Tecnológica Israel, Quito, Ecuador
e1752248375@uisrael.edu.ec
ORCID N/A

Resumen

El ensayo propuesto en este documento se centra en la sofisticada estrategia que la plataforma emplea para recopilar datos. Explora cómo Netflix adquiere información sobre el comportamiento de visualización de los usuarios, sus interacciones, preferencias demográficas y retroalimentación. Además, detalla la compleja red de algoritmos que procesan estos datos para generar recomendaciones personalizadas, mejorar el catálogo de contenido y optimizar la experiencia del usuario. El ensayo analiza el impacto de estos procesos en la calidad del servicio, la ética en la manipulación de datos y la importancia de la privacidad del usuario en un entorno digital. Siendo un punto de inicio para nuevas investigaciones en el área.

Palabras clave

Netflix, comportamiento, algoritmos, datos

Abstract

The proposed essay in this paper focuses on the sophisticated strategy the platform employs to collect data. It explores how Netflix acquires information about users' viewing behavior, interactions, demographic preferences, and feedback. It also details the complex web of algorithms that process this data to generate personalized recommendations, improve the content catalog, and optimize the user experience. The essay analyzes the impact of these

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

processes on the quality of service, the ethics of data manipulation and the importance of user privacy in a digital environment. It is a starting point for further research in the area.

Keywords *(*

Netflix, behavior, algorithms, data

Introducción

Netflix ha transformado profundamente la industria del cine y la televisión en el mundo. Desde su incursión como industria del entretenimiento en 1997 en EEUU, ha impactado las lógicas de producción y consumo en el sector audiovisual [1].

Al alcanzar un alto estatus en el ámbito del entretenimiento en línea y atraer a una audiencia global de millones de espectadores, gran parte de su éxito se debe a su amplia oferta de contenido. Sin embargo, es fundamental destacar que uno de los elementos cruciales para este crecimiento exponencial es la personalización. Esta plataforma tiene la capacidad de monitorear lo que se está viendo, el dispositivo utilizado, cuándo se decide retroceder y cuál será la próxima elección. Por esta razón, este ensayo se adentrará en los procesos y algoritmos que hacen factible esta asombrosa capacidad de comprender y adaptarse de manera precisa a las preferencias de cada uno de los usuarios.

En la década de los 80-90 se ponía de moda el alquiler de películas en formato VHS, DVD, etc. Ya que a esa época al no existir o estar en pañales el internet comercial y por ende la ciberpiratería era imposible obtenerlas “gratis”, en estos lugares por unos pocos dólares la rentabas desde días hasta semanas ya que comprar una copia original era muy costosa, el exponente más reconocido fue Blockbuster empresa muy popular en esa época que gracias al auge de Netflix y su nuevo formato de películas en streaming y a su nula innovación y adaptación al mercado quedaría en bancarrota desde inicios de los 2000 y cerrando su última sucursal en 2013[2]

Netflix inició en 1997 con un modelo de negocio similar a Blockbuster, ofreciendo alquiler de DVD en línea. Sin embargo, su transformación llegó en 2007 con el lanzamiento del servicio de streaming, revolucionando la forma en que accedemos al contenido al permitir suscripciones para disfrutar de una amplia gama de títulos sin necesidad de los DVDs físicos.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Con el tiempo, no se conformaron con adquirir contenido existente, sino que incursionaron en la producción de series originales como "Squid Craft Game" y "Stranger Things". Además, implementaron un algoritmo de recomendaciones personalizadas basado en preferencias de género y títulos, ofreciendo sugerencias adaptadas a cada usuario.

Cuerpo

El conocimiento del usuario y la generación de contenidos personalizados son elementos transversales dentro de la estrategia de negocio y de marca de Netflix ([3]). El big data, en consecuencia, es hoy considerado un eje estratégico en el negocio de la distribución y consumo de contenido audiovisual bajo demanda [4]

Por lo que en base a ello a continuación profundizaremos con respecto a los procesos y algoritmos que utiliza Netflix para poder obtener toda la información con la que crea tal contenido personalizado.

2.1. Procesos

Recolección de Datos: todo el tema relacionado con la personalización empieza con la recolección de una abundante cantidad de datos de los usuarios que tienen interacción con la plataforma [5].

Según el portal oficial de Netflix se nos señala que para calcular la probabilidad de que te interesaría ver un determinado título del catálogo que disponen, toman en cuenta varios factores, entre ellos:

- Interacciones que el usuario tiene con el servicio (como el historial de visualización y las calificaciones asignadas a otros títulos)
- Actividad de otros miembros con gustos y preferencias similares a los de usuarios en específico.
- Información sobre los títulos, como género, categorías, actores, año de lanzamiento, etc.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

- Además de saber qué viste en Netflix, también se usan los siguientes datos para personalizar las recomendaciones:
- Hora del día en que se vio el contenido
- Dispositivos que el individuo utiliza para ver Netflix
- Durante cuánto tiempo la persona ve el contenido

Perfil de Usuario: La plataforma utiliza datos de navegación anteriores para construir un perfil de preferencias por cada usuario. Esto incluye géneros, actores, directores y otros factores que influyen en tu elección de contenido[6].

En esta etapa, es importante considerar que los perfiles pueden ser cotejados con los de otros usuarios que compartan gustos similares, con el propósito de identificar el contenido que podría resultar más atractivo para la persona.

Predicción de Preferencias: Netflix hace uso de algoritmos de aprendizaje automático los cúales permiten identificar con mayor facilidad tendencias con respecto al tipo de contenido con el que el usuario podría tener un mayor nivel de afinidad.

Recomendaciones Personalizadas: una vez recolectada toda la información necesaria, Netflix es capaz de brindar al usuario recomendaciones de contenido en función de sus intereses.

Estas recomendaciones aparecen en la página de inicio y en la sección de "Siguientes pasos" cuando terminas de ver una película o serie.

2.1. Algoritmos

En necesario tomar en cuenta que el sistema de recomendación de Netflix se encuentra compuesto por una gran variedad de algoritmos que, en conjunto, sirven en tiempo real para crear lo que se ha denominado la experiencia completa de Netflix [7]. Estos algoritmos, por un lado, generan categorías de contenido personalizadas para el usuario y, por otro, seleccionan estratégicamente las imágenes de presentación, con el fin de hacer atractivo el contenido para sus audiencias

Dentro de estos algoritmos Gomez-Uribe & Hunt en [7], definen:

Personalized Video Ranking: el algoritmo PVR es el que opera en la homepage y muestra el catálogo de títulos disponible según el país en el que se encuentre, así como también categorías de shows según un género específico y personalizado.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Top N-Video Ranker: indica que este algoritmo recopila los títulos más elegidos de cada categoría, y los combina con las preferencias del usuario y sus tendencias de consumo de contenidos históricos.

Trending now: con respecto a este algoritmo, señalan que es el encargado de mostrar tendencias por temporadas como San Valentín, Navidad o intereses de acuerdo al contexto socio cultural que se vive, como huracanes,etc.

Continue watching: que al identificar qué contenido reproduce el suscriptor y a la vez qué contenido abandona o deja de reproducir, le sugiere de manera personalizada que retome la siguiente temporada, capítulo o minuto de reproducción donde se quedó o pausó la última vez

Video Video Similarity (Sims): el algoritmo Sims es usado para generar la fila de títulos "Porque viste...", que muestra recomendaciones de títulos similares a un show ya visto. Este algoritmo analiza cada uno de los shows del catálogo de Netflix para encontrar similitudes con uno visto recientemente, los ordena por ranking de popularidad y despliega de esta manera en la fila, estimando también las probabilidades de que el usuario quiera reproducir cada título

Conclusiones

A partir de la información revisada con respecto a los procesos de recopilación y análisis de datos, se puede concluir que estas prácticas tienen el potencial de generar beneficios significativos. Un ejemplo destacado de este enfoque es el caso de Netflix, que ha demostrado con éxito el valor de la minería de datos y la inteligencia artificial en la prestación de un servicio de alta calidad a sus usuarios. Este enfoque ha resultado en niveles satisfactorios de fidelidad en la industria del entretenimiento en línea.

Netflix ha revolucionado cómo consumimos contenido visual al proporcionar una experiencia adaptada al usuario. Sus algoritmos de recomendación, ajuste de calidad de transmisión y análisis de datos son cruciales para su éxito. La plataforma emplea machine learning y procesamiento de lenguaje natural para entender constantemente las preferencias y necesidades del usuario.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Gracias a un enfoque centrado en el usuario respaldado por algoritmos innovadores, Netflix puede rastrear lo que vemos, cuándo y desde qué dispositivo. Se espera que la personalización y la experiencia del usuario mejoren continuamente a medida que la plataforma avanza.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Referencias

[1] V. HEREDIA RUIZ, "Revolución Netflix: desafíos para la industria audiovisual," *Chasqui. Revista Latinoamericana de Comunicación*, 2016, Accessed: Oct. 05, 2023. [Online]. Available: https://www.redalyc.org/articulo.oa?id=16057381018

[2] S. Chopra and M. Veeraiyan, "Movie Rental Business: Blockbuster, Netflix, and Redbox," *Kellogg School of Management Cases*, pp. 1–21, Jan. 2017, doi: 10.1108/CASE.KELLOGG.2016.000220.

[3] E.-P. Fernández-Manzano, E. Neira, J. Clares-Gavilán, U. Rey, and J. Carlos, "Gestión de datos en el negocio audiovisual: Netflix como estudio de caso," *Profesional de la información*, vol. 25, no. 4, pp. 568–577, Jul. 2016, doi: 10.3145/epi.2016.jul.06.

[4] V. Heredia-Ruiz, A. C. Quirós-Ramírez, B. E. Quiceno-Castañeda, V. Heredia-Ruiz, A. C. Quirós-Ramírez, and B. E. Quiceno-Castañeda, "Netflix: catálogo de contenido y flujo televisivo en tiempos de big data," *Revista de Comunicación*, vol. 20, no. 1, pp. 117–136, Mar. 2021, doi: 10.26441/RC20.1-2021-A7.

[5] R. Walker *et al.*, "Netflix Leading with Data: The Emergence of Data-Driven Video," *Kellogg School of Management Cases*, pp. 1–19, Jan. 2017, doi: 10.1108/CASE.KELLOGG.2016.000232.

[6] S. C. Madanapalli, H. H. Gharakhieli, and V. Sivaraman, "Inferring netflix user experience from broadband network measurement," *TMA 2019 - Proceedings of the 3rd Network Traffic Measurement and Analysis Conference*, pp. 41–48, Jun. 2019, doi: 10.23919/TMA.2019.8784609.

[7] C. A. Gomez-Uribe and N. Hunt, "The Netflix Recommender System," *ACM Transactions on Management Information Systems (TMIS)*, vol. 6, no. 4, Dec. 2015, doi: 10.1145/2843948.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.8

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Propuesta de seguridad informática en los aspectos organizativos de un sistema informático, aplicando ISO 27002 y CSF

Proposal for IT security in the organizational aspects of an IT system, applying ISO 27002 and CSF.

Fecha de recepción 2023-03-22 • Fecha de aceptación: 2023-05-10 • Fecha de publicación: 2023-05-30

Esteban Silva[1],
[1] Universidad Tecnológica Israel, Quito, Ecuador
esilva@uisrael.edu.ec

Resumen

El artículo propone un enfoque integral para abordar la seguridad informática en los aspectos organizativos de un sistema informático. Para lograr esto, se utiliza un marco combinado de ISO 27002 (Norma Internacional de Seguridad de la Información) y el CSF (Framework de Ciberseguridad). La ISO 27002 establece estándares y directrices para la gestión de la seguridad de la información en una organización. Su implementación implica la identificación de activos de información, la evaluación de riesgos, la aplicación de controles de seguridad y la continua mejora del sistema de gestión de la seguridad de la información. Por otro lado, el CSF proporciona un marco específico para la ciberseguridad, abordando la prevención, la detección y la respuesta a amenazas cibernéticas. Este marco puede adaptarse a las necesidades específicas de la organización, permitiendo una mayor flexibilidad en la implementación de medidas de seguridad. La propuesta de seguridad informática se centra en la integración de estos dos marcos para abordar tanto los aspectos generales de la seguridad de la información como las amenazas cibernéticas específicas. Se destaca la importancia de la colaboración interdepartamental y la sensibilización del personal para garantizar una implementación efectiva.

Palabras clave

Modelo, ISO, seguridad, información, CSF

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Abstract

The article proposes a comprehensive approach to address computer security in the organizational aspects of a computer system. To achieve this, a combined framework of ISO 27002 (International Information Security Standard) and the CSF (Cybersecurity Framework) is used. ISO 27002 establishes standards and guidelines for managing information security in an organization. Its implementation involves the identification of information assets, risk assessment, application of security controls and continuous improvement of the information security management system. On the other hand, the CSF provides a specific framework for cybersecurity, addressing the prevention, detection and response to cyber threats. This framework can be tailored to the specific needs of the organization, allowing for greater flexibility in the implementation of security measures. The cyber security approach focuses on integrating these two frameworks to address both general aspects of information security and specific cyber threats. It highlights the importance of interdepartmental collaboration and staff awareness to ensure effective implementation.

Keywords

Model, ISO, security, information, CSF

Introducción

La seguridad de la información se ha vuelto esencial para las organizaciones debido al constante avance tecnológico, permitiéndoles gestionar y controlar eficientemente la información que manejan. En un mundo cada vez más globalizado, los ataques cibernéticos son más frecuentes y agresivos, buscando obtener información sensible que pueda afectar tanto a organizaciones como a individuos.

Los sistemas de gestión estratégica son especialmente susceptibles a estos ciberataques, ya que pueden comprometer la seguridad de la información que manejan [1]. Por esta razón, las organizaciones reconocen la necesidad de innovar y aplicar guías y normativas internacionales para la seguridad de la información. Adoptan políticas, métodos y directrices

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

para resguardar la información, con el objetivo de minimizar riesgos y anticipar posibles ataques [2].

En la actualidad, la informática y la información son componentes fundamentales tanto para instituciones públicas como privadas y empresas. Sin embargo, enfrentan diversas amenazas y desafíos que impactan directamente en su correcto funcionamiento. El uso diario de dispositivos electrónicos para el manejo de información enlazada a Internet, no siempre se realiza con un sistema de seguridad adecuado. Según [3] se destaca que un sistema informático puede ser protegido mediante enfoques lógicos, como el desarrollo de software, o físicos, como el mantenimiento eléctrico, ya que las amenazas pueden surgir tanto de programas maliciosos como de accesos remotos no autorizados.

En [4], se afirma que la seguridad informática se encarga de estudiar cómo preservar la confidencialidad, integridad y disponibilidad de datos y programas en sistemas de cómputo. Actualmente existen riesgos con respecto, a la seguridad informática, que se maneja en las distintas áreas y sistemas de información, dado que podrían atentar o vulnerar la seguridad de la información que se almacena en sus sistemas entre estos; datos personales, estados de cuenta, servicios. Lo cual podría representar un alto riesgo de inseguridad, que si no se trata adecuadamente pueden ocasionar fallos económicos, prestigio y fuga de información[5].

Los sistemas de gestión de la información deberían contar con un esquema apropiado, de políticas y normas internacionales para la seguridad de la información, puesto que en caso contrario se podría originar una amenaza con alto riesgo en los activos de información que se maneja originando una probabilidad de pérdidas económicas [6].

En la actualidad y con el crecimiento desmesurado de la información los ataques cibernéticos son cada vez más comunes en donde los atacantes buscan brechas o posibles vulnerabilidades para poder obtener información sensible para la organización, es por ello que la ciberseguridad se ha convertido en uno de los aspectos principales.

Materiales y Métodos

Para la presente investigación se ha recabado información por medio de documentos, publicaciones y estudios similares a la investigación realizada con el fin de que estos principios sustenten la justificación del mismo.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Se utiliza la metodología cualitativa que se basa en la recopilación y análisis de datos, explorando las interpretaciones que las personas realizan sobre la realidad social a través de significados e intenciones humanas. Comprende enfoques de investigación como la etnografía, fenomenología e interaccionismo simbólico [7].

En la investigación, se examinarán tanto los aportes teóricos como prácticos relacionados con la seguridad de la información en instituciones de educación superior y en organizaciones que implementen la ISO 27002 en sus aspectos organizativos. Este enfoque permitirá la formulación de un modelo fundamentado en normativas de calidad, definiendo los elementos clave para garantizar la ciberseguridad de un sistema.

En [8], se contextualiza una investigación al aplicar la versión 2005 de las normas ISO y sus 11 categorías de control. Este enfoque les facilita evaluar el nivel de madurez de los dominios de seguridad de la información.

Por otro lado, en [9], se afirma que, la utilización del estándar ofrecido por el NIST facilita la identificación de activos, amenazas y vulnerabilidades de la información. El Instituto Nacional de Estándares y Tecnología (NIST) dispone de controles específicos para la infraestructura crítica, los cuales se ocupan de abordar la identificación, evaluación y gestión del riesgo cibernético mediante acciones flexibles, priorizadas y repetibles. Estas acciones se basan en criterios de desempeño y rentabilidad, e incluyen la identificación y el establecimiento de un marco para la gestión del riesgo de seguridad cibernética.

Comparación entre ISO 27001 y CSF de NITS

Para determinar los aspectos organizativos de una entidad, es esencial establecer una estructura eficaz que fomente la comunicación entre la parte administrativa del sistema, permitiendo la aprobación de políticas de seguridad de la información, la asignación de responsabilidades y la coordinación de niveles de implementación de seguridad.

ISO 27002 propone un esquema organizativo jerárquico que enfatiza la necesidad de una comunicación y colaboración efectivas entre gerentes, clientes, administradores, diseñadores y personal, asignando responsabilidades específicas relacionadas con la seguridad de la información [10].

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

En contraste, la CSF de NITS aboga por la utilización de catálogos de control para satisfacer de manera óptima las necesidades organizativas. Esta normativa se fundamenta en las normas de control de seguridad de la información, adoptando las mejores prácticas para su aplicación. El CSF de NIST introduce el concepto de perfiles, que se asemeja al enfoque jerárquico propuesto por la ISO 27001, gestionando las responsabilidades de manera similar. En la siguiente tabla se detallan estos aspectos.

Tabla 1. Comparativa

	ISO 27002	CSF de NITS	Políticas Sistematización
Identificación de estándares de seguridad y guías	X	X	O
Comité de gestión de la seguridad de la información	X	O	O
Asegurar metas de seguridad de la información	X	O	X
Formulación, revisión y aprobación de la política de seguridad	X	O	O
Directrices claras	X	X	X
Asignación de roles / perfiles	X	X	X
Establecer criterios para la definición de métricas	O	X	O
Identificación de áreas de mejora	X	X	O
Definir el objetivo de la seguridad de la información	X	X	O
Generar comunicación entre las áreas de la institución	X	X	X
Controlar los objetivos alcanzados		X	O
Definición de no cumplimientos	X	O	O
Identificación de cambios significativos de amenazas y exposición de la información	X	O	O
Asignación de responsabilidades	X	X	X
Promoción de la educación, entrenamiento y concienciación	X	O	O

Resultados

Los Evaluadores de Calidad (QA) en el departamento de Sistematización desempeñan la función de llevar a cabo las pruebas correspondientes de funcionamiento, estrés y control del sistema SIGE, asegurando su adecuado rendimiento y calidad. Sin embargo, no tienen políticas establecidas para aprobar cuestiones de seguridad ni cuentan con métricas que definan un criterio de control.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Una vez analizadas las premisas de las normativas, se plantea como objetivo prioritario la gestión de la seguridad de la información en los aspectos organizativos, considerándola como una parte esencial de los objetivos y actividades de la institución. Esto incluye la identificación, control y mejora de las áreas que presentan mayor vulnerabilidad en cuanto a la exposición de la seguridad de la información.

Por consiguiente, se proponen los siguientes puntos como un posible modelo de políticas, basándose en los aspectos organizativos destacados en la comparativa entre la ISO 27002 y el CSF, se detalla en la siguiente tabla:

Tabla 2. Políticas propuestas

Nro.	Actividad	Descripción
1	**Definir un comité de gestión de la seguridad de la información:**	Este comité es encargado de poder establecer las políticas de seguridad de la información que se van a manejar dentro del área de sistematización institucional basados en las principales normativas de regulación de la seguridad de la información mundial. Identificar las personas responsables de cada una de las áreas y las métricas con las cuales se debe asegurar la seguridad de la información. Establecer objetivos y metas claras medibles para el control del manejo de información.
2	**Definir un lenguaje común para la gestión de riesgos de la seguridad de la información:**	Se establece un sistema común y maneja la misma información dentro de las áreas responsables de la seguridad de la información.
3	**Definir las metas y objetivos de seguridad de la información para el área de sistematización institucional:**	Se debe establecer un punto de llegada con el fin de poder dirigir los esfuerzos realizados por cada una de las áreas para poder llegar. Se establecerán objetivos medibles para verificar que se están cumpliendo las políticas establecidas de la seguridad de la información.
4	**Asignar las áreas responsables:**	Se debe establecer áreas que sean responsables de cada una de las metas asignadas para asegurar la seguridad de la información.
5	**Asignación de responsables a cada una de las áreas propuestas:**	Se deben asignar personas encargadas de establecer y dirigir las metas asignas dentro del área de la cual sean responsables para poder asegurar la seguridad de la información.
6	**Asegurar que las actividades se cumplan según las metas definidas:**	Se deben realizar un control de que las acciones y políticas establecidas se estén cumpliendo con respecto a la seguridad de la información. Crear un cronograma de controles para poder establecer métricas de seguridad.
7	**Identificar amenazas y la exposición de información:**	Cada una de las áreas previstas deberá presentar las amenazas o los riesgos de exposición de la información a los cuales se encuentran expuestos.
8	**Capacitación sobre los riesgos del manejo de la información en la propia institución:**	Se deben crear planes de concientización y aprendizaje del riesgo de la seguridad de la información.
9	**Crear una comunicación constante entre las áreas internas de la institución sobre el riesgo de ciberseguridad:**	Se debe tener reuniones periódicas para establecer una comunicación constante entre las áreas implicadas y poder anticiparse a posibles fallos o vulnerabilidades en el manejo de la seguridad de la información.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

El análisis comparativo entre la ISO 27002 y el marco regulatorio de la CSF, que sirven como fundamentos para las mejores políticas en seguridad de la información, concluye que es esencial aplicar un esquema adaptado a las necesidades específicas de dicho ámbito. Esto se debe a que la información manejada posee un nivel de interés para ciberdelincuentes que buscan aprovechar brechas o vulnerabilidades para acceder y apropiarse de la información.

El esquema propuesto se presenta como un conjunto de políticas que deben implementarse en base a principios fundamentales y requisitos mínimos para salvaguardar la seguridad de la información. En este marco, se deben considerar riesgos no asociados, como acciones no autorizadas, fallos técnicos, falta de compromiso de los involucrados, daños físicos a la infraestructura, falta de control, entre otros, que pueden no ser definidos en el momento.

Por ende, es crucial establecer una estructura que sirva como guía para la implementación de políticas de ciberseguridad de la información, basada en un análisis comparativo que aplique las principales prácticas y estándares de organizaciones y normativas a nivel mundial. No obstante, esta estructura puede no ser completamente aceptada por la organización, por lo que se presenta como un esquema susceptible a cambios o ajustes según las necesidades de la institución.

Los puntos delineados en este esquema indican que la implementación es viable para cualquier organización, independientemente de su tamaño, nivel de riesgo o complejidad en ciberseguridad. Este enfoque ofrece diversas aplicaciones que, al vincularse, benefician la seguridad de la información, evitando la pérdida de datos y protegiendo las prioridades cruciales. Además, establece políticas que definen un marco regulador para la gestión de la seguridad de la información, reduciendo el riesgo de robo, pérdida de integridad o información sensible, y generando confianza en las personas que manejan o tienen acceso a dicha información, así como en los servicios ofrecidos. En última instancia, este enfoque fortalece la seguridad a través de una gestión integral y evita depender de sistemas de terceros.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Conclusiones

Se identifica la necesidad de crear un modelo fundamentado en los aspectos organizativos de la seguridad de la información, utilizando las principales políticas y prácticas como base para su aplicación. Se reconoce que la aceptación completa de este modelo por parte de la institución puede no ser garantizada, por lo que se presenta como un modelo sujeto a cambios o adaptable según las necesidades de la institución.

La implementación de este modelo es viable para cualquier organización, sin importar su tamaño, nivel de riesgo o complejidad en ciberseguridad. Este enfoque ofrece diversas aplicaciones que, al combinarse, contribuyen al beneficio de la seguridad de la información, evitando la pérdida de datos y protegiendo las prioridades fundamentales. Además, se busca establecer políticas que definan un marco regulatorio para la gestión de la seguridad de la información, reduciendo el riesgo de robo, pérdida de integridad o divulgación de información sensible o confidencial para la institución.

El objetivo principal de este modelo es generar confianza en las personas que gestionan o tienen acceso a la información, así como en los servicios ofrecidos. De esta manera, se fortalece la seguridad a través de una gestión integral y se evita depender de sistemas de terceros.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Referencias

[1] F. Morales, S. Toapanta, and R. M. Toasa, "Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información," *Revista Ibérica de Sistemas e Tecnologias de Informação*, vol. E, no. 27, pp. 553–565, 2020.

[2] P. F. Baldeon Egas, M. A. Gaibor Saltos, and R. Toasa, "Integrated Strategic Management System," *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, Jun. 2019, doi: 10.23919/CISTI.2019.8760801.

[3] C. A. T. Almeida and L. R. Herrera, "La ciberseguridad en el ecuador, una propuesta de organización," *Revista de Ciencias de Seguridad y Defensa*, vol. IV, no. 7, pp. 156–169, 2019.

[4] M. Cristiá, U. Nacional, and R. Rosario -Argentina, "Apunte de clase Seguridad Informática".

[5] R. Vargas Borbúa, R. P. Reyes Chicango, and L. Recalde Herrera, "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance," *URVIO - Revista Latinoamericana de Estudios de Seguridad*, no. 20, p. 31, Jun. 2017, doi: 10.17141/urvio.20.2017.2571.

[6] J. A. Senn, E. G. U. Medal, and O. A. P. Velasco, *Análisis y diseño de sistemas de información*, vol. 2. McGraw-Hill, 1992.

[7] R. Barrantes Echavarría, *Investigación: un camino al conocimiento Un enfoque cualitativo, cuantitativo y mixto*, 2nd ed. Costa Rica: UNED, 2013. Accessed: Mar. 01, 2021. [Online]. Available: https://editorial.uned.ac.cr/book/U08167

[8] M. Baldeón and J. Guanopatin, "Políticas de seguridad de la información para la Universidad Central del Ecuador bajo los estándares ISO/TEC 27000 y Cobit 5," 2015, Accessed: Dec. 02, 2023. [Online]. Available: http://repositorio.espe.edu.ec/jspui/handle/21000/12551

[9] A. Molina Oviedo, "Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: caso de estudio Universidad Popular del Cesar," 2020, Accessed: Dec. 02, 2023. [Online]. Available: https://manglar.uninorte.edu.co/handle/10584/10394

[10] "¿Qué es ISO 27000 - Seguridad de la Información? | GSS." Accessed: Dec. 02, 2023. [Online]. Available: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.9

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

Propuesta de modelo en seguridad informática en el control de un sistema informático aplicando ISO 27002 y CSF de NIST

IT security model proposal in the control of an IT system applying ISO 27002 and NIST CSF.

Fecha de recepción 2023-04-04 • Fecha de aceptación: 2023-05-29 • Fecha de publicación: 2023-06-05

Jorge Vinicio Gavidia Córdova [1],
[1] Universidad Tecnológica Israel, Quito, Ecuador
jgavidia@uisrael.edu.ec

Resumen

El paper presenta una propuesta de modelo integral de seguridad informática para el control efectivo de un sistema informático, basado en la aplicación combinada de la norma ISO 27002 y el Marco de Ciberseguridad (CSF) de NIST. Se enfatiza la importancia de adoptar estándares reconocidos para fortalecer la seguridad y gestionar eficazmente los riesgos cibernéticos. El modelo propuesto abarca diversos aspectos, incluyendo controles de acceso, gestión de usuarios, monitoreo constante y medidas de respuesta ante posibles amenazas. Se destaca la relevancia de la norma ISO 27002 en proporcionar directrices específicas para la seguridad de la información, mientras que el CSF de NIST complementa y refuerza el enfoque al brindar un marco adaptativo y flexible. La propuesta busca garantizar la confidencialidad, integridad y disponibilidad de la información, al tiempo que se adapta a las particularidades y desafíos específicos del entorno del sistema informático en consideración. Se espera que esta combinación de normas brinde una base sólida para la implementación de medidas de seguridad efectivas y la mitigación de riesgos en el ámbito de la ciberseguridad.

Palabras clave

Modelo, seguridad, ISO, amenazas, sistema informático

Abstract

The paper presents a proposal for a comprehensive IT security model for the effective control of an IT system, based on the combined application of ISO 27002 and the NIST

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

Cybersecurity Framework (CSF). It emphasizes the importance of adopting recognized standards to strengthen security and effectively manage cyber risks. The proposed model covers various aspects, including access controls, user management, constant monitoring and response measures to potential threats. It highlights the relevance of ISO 27002 in providing specific guidelines for information security, while the NIST CSF complements and reinforces the approach by providing an adaptive and flexible framework. The proposal seeks to ensure the confidentiality, integrity and availability of information, while adapting to the specifics and challenges of the IT system environment under consideration. This combination of standards is expected to provide a solid foundation for the implementation of effective security measures and risk mitigation in the field of cybersecurity.

Keywords

Model, Security, ISO, Risk, Computer system

Introducción

Hoy en día, la tecnología ha experimentado un desarrollo considerable, y la automatización de procesos se ha vuelto esencial para la mayoría de las instituciones que ofrecen servicios, especialmente en el ámbito educativo. En este contexto, la gestión de la información se vuelve crucial para las actividades diarias tanto de docentes como de estudiantes en una institución académica.

En el entorno académico, resulta fundamental contar con procesos automatizados que faciliten tareas como la introducción de calificaciones, la administración de exámenes, la generación de registros de asistencia y la realización de evaluaciones periódicas tanto para docentes como para estudiantes. Dada la naturaleza confidencial e importante de la información, como los registros de calificaciones y los expedientes académicos, es imperativo implementar estrategias, métodos y técnicas de control de acceso para proteger la integridad de los datos manejados [1].

En la actualidad, la información se ha convertido en uno de los activos más valiosos de una institución. Ante el notable aumento de ataques informáticos en los últimos años, resulta indispensable establecer controles adecuados para contrarrestar y minimizar el riesgo de

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

accesos no autorizados a los sistemas informáticos. De esta manera, se busca prevenir la pérdida o sustracción de información sensible [2].

Es importante resaltar que no solo las instituciones financieras, gubernamentales o de salud están expuestas al riesgo de sufrir ataques; las instituciones educativas también pueden convertirse en blanco de ciberdelincuentes. Los recientes eventos relacionados con la pandemia han llevado a un intercambio descontrolado de información, con accesos masivos a sistemas, sin la implementación de controles adecuados ni la debida capacitación. Esta falta de medidas adecuadas hace que la información manejada dentro de una institución educativa sea vulnerable, subrayando la importancia de establecer controles eficientes, como marcos de trabajo o estándares internacionales [3].

Existen varios estándares de seguridad de la información entre los cuales se mencionan los siguientes:

- Los estándares proporcionados por la serie ISO 27000 constituyen un conjunto de normas de seguridad de la información. Estas normas ofrecen pautas para la creación de un sistema de gestión de la información. En la tabla 2 se detallan las normas que forman parte de esta familia, y a continuación se describen cada una de ellas [4].
- Estándares de la familia NIST: Este estándar proporciona a las empresas una herramienta para gestionar los riesgos y salvaguardar sus datos mediante el uso de un lenguaje común relacionado con las prácticas de seguridad de la información[5] .
- Controles de Servicio y Organización 2 (SOC 2): Se refiere a la elaboración de informes que detallan los controles necesarios que una organización debe implementar para proteger la información [6].
- SANS: Esta entidad con fines de lucro reúne a profesionales de seguridad informática y se centra principalmente en la identificación de vulnerabilidades en el desarrollo de software [7].

En [8], se destaca la necesidad de que una institución educativa de nivel superior fomente la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura mediante el aprovechamiento de diversas herramientas tecnológicas disponibles. En el contexto ecuatoriano, aún no se ha implementado una estrategia integral de ciberseguridad

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

que incluya directrices esenciales para salvaguardar la información, la infraestructura y, especialmente, a los usuarios frente a posibles ataques.

Por otro lado, en [9] señala la relevancia de las normas ISO 27001-27002 en la gestión de la seguridad de la información en instituciones de educación superior. Destaca la importancia de preservar la confidencialidad, integridad y disponibilidad de la información en estos entornos. El uso normativo basado en las normas ISO se presenta como fundamental para fortalecer la seguridad de las bases de datos, asegurando así la confidencialidad, integridad y disponibilidad de la información en cada uno de los procesos.

Materiales y Métodos

Este trabajo tiene un enfoque de investigación bibliográfica, que puede ser conceptualizada como un examen exhaustivo de todo el material existente y disponible vinculado al tema de investigación. Este proceso facilita la identificación y selección de información pertinente en función de las fuentes empleadas, las cuales pueden incluir libros, revistas, videos, entre otros. Este paso se reconoce como esencial, ya que involucra la observación, investigación, interpretación, reflexión y análisis, con el propósito de obtener los fundamentos necesarios para el avance de la investigación [10].

La metodología de investigación empleada en este trabajo es de naturaleza bibliográfica exploratoria. Se llevó a cabo una revisión exhaustiva de diversas fuentes, como libros, artículos y revistas, con el objetivo de obtener una comprensión general del problema asociado al control de accesos. Esta aproximación se caracteriza por su enfoque cualitativo, ya que implica la formulación de propuestas para controles de seguridad dentro de una institución.

Este proceso investigativo busca profundizar en el tema y proporcionar información significativa sobre un área específica mediante el análisis del comportamiento, las emociones y otros aspectos de la psicología humana que son susceptibles a la interpretación[11] .

Métodos e instrumentos de investigación.

En la realización de este estudio, se emplea la técnica de entrevista, la cual se utilizará para recopilar información esencial que complemente la investigación.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

Entrevista: Se define como un diálogo establecido entre un investigador y la persona seleccionada como sujeto de estudio, con el propósito de obtener respuestas que aborden el problema planteado y contribuyan a resolver las preguntas formuladas en relación con el tema de investigación.

Población y muestra

Siguiendo la metodología de investigación de este trabajo, la población objeto de estudio corresponde a la Unidad de Sistematización Institucional (SI), y la muestra está conformada por dos profesionales encargados del desarrollo e implementación. Se trata de una muestra intencionada, seleccionada debido a las responsabilidades específicas que ostentan los profesionales de la SI.

Para determinar la vulnerabilidad existente se realiza una comparativa entre la ISO 27002:2013 y CSF de NIST versus lo aplicado en el Sistema informático de análisis.

A través de la comparación efectuada, es posible identificar el porcentaje de controles que están actualmente implementados y determinar cuáles son necesarios para su incorporación. Tras realizar la comparación entre los dos estándares internacionales, se pueden identificar las vulnerabilidades existentes actualmente. Para este propósito, se lleva a cabo una entrevista con el director del área de Sistematización y el jefe de programadores, cuya experiencia proporciona información valiosa para evaluar el estado actual del sistema.

En el proceso de esta investigación, se logró recopilar información sustancial que respalda el objeto de estudio. Las fuentes de origen de la información recabada son confiables y aseguran una sólida base para abordar el tema planteado.

Resultados

En este estudio, se han empleado el estándar ISO 27002:2013 y el Marco de Ciberseguridad (CSF) de NIST. Esto se debe a que el primero proporciona directrices esenciales para mantener, implementar o mejorar la seguridad de la información. Por otro lado, el CSF de NIST se presenta como un conjunto ampliado de la norma ISO 27002:2013, como se ilustra en la Figura 1. En otras palabras, el CSF de NIST desempeña un papel crucial al reforzar la

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

seguridad en situaciones en las que la norma ISO 27002:2013 podría no abarcar completamente todas las áreas necesarias.

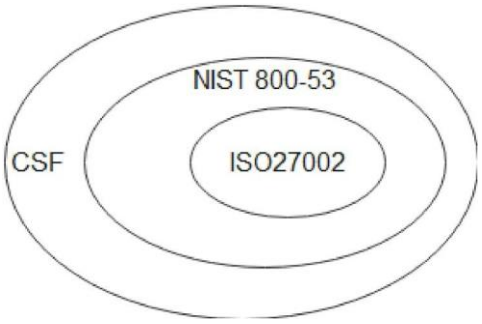

Fig. 1. Estructura de controles dentro de CSF

El Marco de Seguridad Cibernética (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) es una estructura diseñada para elevar los niveles de seguridad de la información. Fue creado en los Estados Unidos en el año 2013 y, en la actualidad, se encuentra en su versión 1.1, la cual fue publicada en 2018, ver la Fig 2.

Fig. 2. Funciones CSF

El propósito fundamental de la norma ISO 27002 consiste en establecer un control en el acceso mediante el empleo de un conjunto de normas, restricciones y procedimientos que

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

aseguren la asignación adecuada de derechos de acceso en cada uno de los sistemas de información [12].

Se opta por la versión ISO 27002:2013 debido a su historial de implementación; es decir, ha sido más ampliamente probada en comparación con la ISO 27002:2022 [13]. Aunque la versión 2022 aborda aspectos más contemporáneos, como la ciberseguridad y asuntos relacionados con la protección de datos y privacidad, es un marco más recientemente publicado, lo que implica que ha sido probado en menor medida.

Este estudio se fundamenta en el ámbito de control de accesos, donde se busca gestionar cualquier acceso no autorizado y reducir al mínimo la probabilidad de que ocurra. Es esencial identificar de manera apropiada el rol asignado a cada usuario para establecer un control efectivo sobre el acceso a la información. A continuación, se describen los controles específicos referentes a este dominio, según lo establecido en la norma ISO 27002:2013:

- Requisitos de negocio para el control de accesos: Este control se centra en gestionar el acceso solo para personal autorizado y se subdivide en los siguientes aspectos:
    - Política de control de acceso: Implica un conjunto de reglas que regulan el acceso a la información, siendo los propietarios quienes determinan las normas aplicables.
    - Control de acceso a las redes y servicios asociados: Se refiere a la autorización de usuarios para acceder a redes y servicios de red.

La administración del acceso de usuario implica la implementación de procesos que regulen la asignación de usuarios y sus respectivos permisos, desde el momento en que se registran en el sistema hasta su eventual desactivación, de manera que se abarque todo el ciclo de vida de acceso de acuerdo con las directrices de la norma ISO 27002. Asegurar el acceso exclusivamente a usuarios autorizados mediante procesos establecidos es crucial para evitar el ingreso de usuarios no autorizados. Dentro de la gestión de acceso de usuarios, se destacan los siguientes controles:

- Gestión de altas y bajas en el registro de usuarios: El departamento de seguridad se encargará de asignar y dar de baja a los usuarios para acceder al sistema, considerando aspectos clave como nombres de usuario únicos y la asignación de roles pertinentes a la respectiva área de actividad.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

- Gestión de los derechos de acceso asignados a usuarios: Estas herramientas posibilitan la asignación y restricción de permisos en los sistemas de información.
- Gestión de los derechos de acceso con privilegios especiales: Implica la identificación por escrito de usuarios que requieren permisos especiales para el acceso.
- Gestión de información confidencial de autenticación de usuarios: Consiste en asignar contraseñas a los usuarios previa autorización del jefe del departamento.
- Revisión de los derechos de acceso de los usuarios: Se refiere a llevar a cabo monitoreos o revisiones periódicas de los permisos asignados a los usuarios.
- Obligaciones del usuario.
- El propósito de este mecanismo es identificar las obligaciones específicas de cada usuario, quienes deben asumir la responsabilidad correspondiente al rol asignado y mantener una conciencia adecuada sobre la información que gestionan.
- Utilización de información confidencial para la autenticación.
- Es esencial que el usuario tenga conocimiento de buenas prácticas, tales como el uso de contraseñas sólidas y la no divulgación de sus credenciales a terceros.
- Gestión del acceso a sistemas y aplicaciones: Es fundamental establecer políticas de acceso que salvaguarden la información, ya sea en forma de documentos u otros medios informáticos, con el fin de prevenir accesos no autorizados.
- Limitación del acceso a la información: Se deben establecer políticas de control que definan restricciones para acceder a los sistemas de información.
- Procedimientos seguros de inicio de sesión: Se trata de controles para asegurar inicios de sesión seguros, capaces de verificar la identidad del usuario.
- Administración de contraseñas de usuario: Se refiere a sistemas que generan contraseñas seguras, lo que incluye la renovación regular de estas contraseñas en intervalos determinados.
- Utilización de herramientas de administración de sistemas: Cualquier sistema con privilegios de acceso debe emplear una autenticación independiente para evitar interferencias en el sistema principal.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

- Control de acceso al código fuente de los programas: Es crucial aplicar restricciones al código fuente de la aplicación mediante el uso de bibliotecas, y el código debe gestionarse en un entorno separado de la red principal.

Conclusiones

La norma ISO 27002:2013, aunque efectivamente hace referencia o propone ciento catorce controles, se ve complementada por aspectos presentes en el Marco de Ciberseguridad (CSF) de NIST, como se pudo constatar durante la revisión de la base teórica.

Después de llevar a cabo el mapeo entre ISO 27002:2013 y CSF de NIST, se identificaron 23 controles relacionados con el control de accesos. Una vez validado el Sistema Integrado de Gestión Estratégica, cumple con un 40.5% según ISO 27002:2013 y un 32.53% según NIST.

Dentro del marco propuesto y basado en los estándares seleccionados, se establece un conjunto de controles que deben aplicarse según principios fundamentales y como requisitos mínimos para salvaguardar la seguridad de la información.

En este esquema, se debe tener en cuenta la existencia de riesgos no asociados que suelen manifestarse como acciones no autorizadas, fallos técnicos, falta de compromiso de los involucrados (usuarios del sistema), daños físicos (infraestructura) y falta de control, entre otros.

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

Referencias

[1] F. Morales, Y. Simbaña, R. Coral, and R. M. Toasa, *Technique for Information Security Based on Controls Established by the SysAdmin Audit, Networking and Security Institute*, vol. 1273 AISC. 2021. doi: 10.1007/978-3-030-59194-6_34.

[2] M. Malik and T. Patel, "DATABASE SECURITY-ATTACKS AND CONTROL METHODS," *International Journal of Information Sciences and Techniques (IJIST)*, vol. 6, no. 1, 2016, doi: 10.5121/ijist.2016.6218.

[3] A. Rasin, J. Wagner, K. Heart, and J. Grier, "Establishing Independent Audit Mechanisms for Database Management Systems," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE, Oct. 2018, pp. 1–7. doi: 10.1109/THS.2018.8574150.

[4] D. N. L. Armendáriz, "Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000," *Revista Tecnológica ESPOL*, vol. 30, no. 1, 2017, Accessed: Jul. 03, 2021. [Online]. Available: http://200.10.150.204/index.php/tecnologica/article/view/581

[5] S. Almuhammadi and M. Alsaleh, "INFORMATION SECURITY MATURITY MODEL FOR NIST CYBER SECURITY FRAMEWORK," pp. 51–62, 2017, doi: 10.5121/csit.2017.70305.

[6] "¿Qué es la auditoría SOC 2?" Accessed: Dec. 03, 2023. [Online]. Available: https://www.auditool.org/blog/auditoria-externa/que-es-la-auditoria-soc-2

[7] D. Harp and B. Gregory-Brown, "A SANS Survey SANS 2016 State of ICS Security Survey," 2016.

[8] P. I. Morales-Paredes and R. P. Medina Chicaiza, "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador," *3 c TIC: cuadernos de desarrollo aplicados a las TIC, ISSN-e 2254-6529, Vol. 10, Nº. 2, 2021, págs. 49-75*, vol. 10, no. 2, pp. 49–75, 2021, doi: 10.17993/3ctic.2021.102.49-75.

[9] N. Camacho, J. Mesias, R. Lucas, and J. Jose, "Auditoría informática dirigida al Centro de Cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con base en las Normas ISO 27001 y 27002." Universidad

ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10

de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales., 2020. Accessed: Dec. 03, 2023. [Online]. Available: http://repositorio.ug.edu.ec/handle/redug/48923

[10] J. Daniel, C. Flores, and B. Leticia González Becerra, "Objetos de aprendizaje: Una Investigación Bibliográfica y Compilación," *Revista de Educación a Distancia (RED)*, no. 34, 2012, Accessed: Dec. 03, 2023. [Online]. Available: https://revistas.um.es/red/article/view/233351

[11] I. Gallego-Galán and others, "La investigación cualitativa," *Investigación de Mercados I*, 2020.

[12] L. M. C. M. da Fonseca and L. M. C. M. da Fonseca, "ISO 14001:2015: An improved tool for sustainability," *Journal of Industrial Engineering and Management*, vol. 8, no. 1, pp. 37–50, Feb. 2015, doi: 10.3926/jiem.1298.

[13] M. Baldeón and J. Guanopatin, "Políticas de seguridad de la información para la Universidad Central del Ecuador bajo los estándares ISO/TEC 27000 y Cobit 5," 2015, Accessed: Dec. 02, 2023. [Online]. Available: http://repositorio.espe.edu.ec/jspui/handle/21000/12551

Período enero-junio 2023
Vol. 2 No. 1 riif@editorialscientificfuture.com
ISSN-L: 3028-869X **DOI:** https://doi.org/10.62465/riif.v2n1.2023.10