Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Revolución de la ciberseguridad en la cuarta revolución industrial

Cybersecurity revolution in the fourth industrial revolution

Fecha de recepción: 2023-05-25 • Fecha de aceptación: 2023-07-04 • Fecha de publicación: 2023-07-21

Javier Guaña-Moya[1]
[1] Instituto Superior Tecnológico Japón, Quito, Ecuador
eguana@itsjapon.edu.ec
ORCID: 0000-0003-4296-0299

Resumen

La cuarta revolución industrial (Industria 4.0) ha generado cambios significativos en la forma en que las empresas producen y distribuyen bienes y servicios a nivel global. Sin embargo, también ha creado nuevas vulnerabilidades en materia de ciberseguridad, que deben abordarse mediante una colaboración público-privada. Para ello, se ha desarrollado el concepto de ciberseguridad 4.0, que busca proteger la integridad, confidencialidad y disponibilidad de los sistemas cibernéticos en un contexto de Industria 4.0. Los profesionales de la ciberseguridad deben estar actualizados en las competencias técnicas necesarias para gestionar incidentes de ciberseguridad en el entorno digital y garantizar la continuidad del negocio. Además, es necesario desarrollar técnicas de encriptación y detección de anomalías en la comunicación entre dispositivos, como los PLC, y la nube en la industria 4.0. La ciberseguridad es un asunto que concierne a todos los sectores de la sociedad, incluyendo la administración pública y los ciudadanos. En el marco de la cuarta revolución industrial, la ciberseguridad es una asignatura pendiente y un reto para abordar para garantizar la sostenibilidad y el crecimiento económico en el futuro. Por lo tanto, se requiere una mayor investigación y formación en este ámbito, así como una regulación más rigurosa en materia de ciberseguridad.

Palabras claves: industria 4.0, ciberseguridad 4.0, entorno digital, competencias técnicas.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Abstract

The fourth industrial revolution (Industry 4.0) has generated significant changes in the way companies produce and distribute goods and services globally. However, it has also created new cybersecurity vulnerabilities, which must be addressed through public-private collaboration. To this end, the concept of cybersecurity 4.0 has been developed, which seeks to protect the integrity, confidentiality, and availability of cyber systems in an Industry 4.0 context. Cybersecurity professionals must be updated in the technical skills needed to manage cybersecurity incidents in the digital environment and ensure business continuity. In addition, it is necessary to develop encryption and anomaly detection techniques for communication between devices, such as PLCs, and the cloud in Industry 4.0. Cybersecurity is an issue that concerns all sectors of society, including public administration and citizens. In the framework of the fourth industrial revolution, cybersecurity is an unfinished business and a challenge to be addressed to ensure sustainability and economic growth in the future. Therefore, more research and training are required in this area, as well as more rigorous regulation in the field of cybersecurity.

Keywords: industry 4.0, cybersecurity 4.0, digital environment, technical skills.

Introducción

La cuarta revolución industrial ha generado un gran impacto en la forma en que las empresas operan y los consumidores interactúan con ellas. El avance de la tecnología, la automatización y la conectividad han creado un mundo interconectado en el que la información es la nueva moneda. Sin embargo, con esta revolución también ha surgido una nueva amenaza: la ciberseguridad, como menciona [1], “el potencial de una brecha en la ciberseguridad podría ser catastrófico para la economía global”. Es por eso que la colaboración público-privada es crucial en este contexto, ya que la ciberseguridad es un desafío que no puede ser enfrentado por una sola entidad.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Con referencia a lo anterior, en esta era de la Industria 4.0, la ciberseguridad se ha convertido en un pilar fundamental para el éxito de las empresas y organizaciones. En efecto, [2] afirma que "la administración de la ciberseguridad debe ser una prioridad para las empresas que quieren garantizar la protección de su información y la de sus clientes". En este sentido, es necesario que las empresas y organizaciones estén preparadas para enfrentar los nuevos desafíos que se presentan en la era digital.

A los efectos de este, la educación en ingeniería también ha sido impactada por la cuarta revolución industrial. De acuerdo con [3], "las tecnologías de la información y las comunicaciones son fundamentales en la educación en ingeniería en la era de la Industria 4.0". Sin embargo, esto también ha creado nuevos desafíos en cuanto a la seguridad de la información y la privacidad de los estudiantes y profesores.

Ante la situación planteada, la colaboración entre el sector público y privado es fundamental para garantizar la ciberseguridad en la cuarta revolución industrial. Como indica [4], "la cooperación entre empresas, gobiernos y otros actores es necesaria para enfrentar los nuevos desafíos en el mundo digital". Al mismo tiempo, la formación de expertos en ciberseguridad es crucial para garantizar la protección de la información en este nuevo contexto.

Hechas las consideraciones anteriores, en la era de la cuarta revolución industrial, es necesario estar preparados para enfrentar los nuevos desafíos que se presentan en cuanto a la seguridad de la información. Así pues, [5] infiere, "la seguridad cibernética es una prioridad en las universidades para garantizar la protección de la información de los estudiantes y profesores". La ciberseguridad es un desafío global que requiere de una colaboración público-privada y de la formación de expertos para enfrentar los nuevos desafíos que se presentan en este nuevo contexto tecnológico.

Revisión de literatura

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

La cuarta revolución industrial ha traído consigo la integración de tecnologías digitales avanzadas en los procesos productivos, lo que ha generado grandes oportunidades, pero también importantes riesgos. En relación con este último, [6] manifiestan que, esta revolución ha generado una transformación profunda en el mundo empresarial, en la que la ciberseguridad juega un papel fundamental para garantizar la seguridad de los datos y la continuidad del negocio. Por su parte, [7] señala que la ciberseguridad sigue siendo una asignatura pendiente en esta revolución, y que es necesario abordarla de manera urgente para garantizar la estabilidad y la confianza en el nuevo entorno digital.

Tal como se observa, [8] resalta que, junto con la revolución digital, también ha surgido un importante riesgo en el ámbito de la responsabilidad civil, en el que es necesario establecer medidas claras para garantizar la protección de los datos de los usuarios y la responsabilidad de las empresas en caso de incidentes de ciberseguridad. También, la pandemia del COVID-19 ha intensificado la necesidad de ciberseguridad en todos los ámbitos, como señala [9], quien subraya la importancia de la ciberinmunidad para hacer frente a las amenazas cibernéticas.

Por otra parte, la revolución digital ha llevado a una transformación en el ámbito contractual, como señala [10], quien acentúa la necesidad de revisar los principios de la libertad contractual para adaptarlos a la era digital y garantizar la protección de los datos y la privacidad de los usuarios. Dadas las condiciones que anteceden, el informe de [11] enfatiza que la ciberseguridad es una cuestión que nos incumbe a todos, y que es necesario establecer medidas claras para garantizar la seguridad en el ámbito digital.

En cuanto a la industria 4.0, [12] destaca que la ciberseguridad es un medio fundamental para garantizar la continuidad del negocio en un entorno altamente digitalizado. Cabe agregar que, para [13], la ciberseguridad es una preocupación creciente en la industria 4.0, y que es necesario abordarla de manera integral para garantizar la seguridad de los procesos productivos. Significa entonces, según [14] que es importante establecer normas claras y

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

estándares de certificación en materia de seguridad cibernética para aplicarlos en la industria 4.0 y en el Internet de las cosas.

Por último, [15] enfatizan la importancia del desarrollo de técnicas de ciberseguridad específicas para la industria 4.0, como la encriptación de datos y la detección de anomalías en la comunicación entre PLC y la nube, para garantizar la seguridad de los procesos productivos. En definitiva, la ciberseguridad es una cuestión fundamental en la cuarta revolución industrial, y es necesario abordarla de manera integral para garantizar la seguridad de los datos y la continuidad del negocio.

Metodología

Para llevar a cabo la investigación sobre la revolución de la ciberseguridad en la cuarta revolución industrial, se utilizará una metodología cualitativa que permita comprender las experiencias, percepciones y opiniones de los actores involucrados. Se recopilarán datos a través del análisis bibliográfico-documental de artículos científicos, libros, entre otros, de diversas bases de datos, y se analizarán por medio de un enfoque interpretativo. Como señalan [16], la metodología cualitativa permitirá explorar y comprender fenómenos complejos, especialmente aquellos que no son fácilmente cuantificables, y se enfatizará en la interpretación de los datos en lugar de la medición.

En este propósito, la investigación cualitativa es descriptiva y explicativa, como indica [17], ya que se enfoca en describir y comprender los fenómenos sociales y culturales, y en explicar cómo los individuos experimentan y perciben esos fenómenos. Por último, [18] subrayan que la investigación cualitativa es un enfoque flexible y reflexivo que permite a los investigadores adaptar su enfoque a medida que surgen nuevos conocimientos a lo largo del proceso de investigación. En síntesis, la metodología cualitativa permitirá una exploración en profundidad y una comprensión rica y detallada de la revolución de la ciberseguridad en la cuarta revolución industrial, desde la perspectiva de los actores involucrados.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Resultados

De los anteriores planteamientos se deduce que la mayoría de los autores coinciden en que la cuarta revolución industrial (Industria 4.0) está transformando los procesos productivos a través de la digitalización y la automatización, lo que ha generado nuevos desafíos en términos de ciberseguridad. En este mismo orden y dirección, [1] señala que la colaboración público-privada es clave para abordar estos desafíos, especialmente en lo que se refiere a la protección de infraestructuras críticas.

Hoy día, [2] destaca la importancia de la administración de la ciberseguridad en el contexto de la Industria 4.0, señalando que esta debe ser una responsabilidad compartida entre las organizaciones y los individuos. También, [3] recalca la necesidad de que los profesionales de la ingeniería adquieran habilidades en ciberseguridad para hacer frente a los nuevos desafíos que plantea la digitalización.

Por lo tanto, [4] acentúa la importancia de la colaboración público-privada en la implementación de estrategias de ciberseguridad eficaces, mientras que [5] resalta la importancia de los pilares tecnológicos universitarios en la formación de los profesionales del futuro.

Consecutivamente, [19] contextualizan la cuarta revolución industrial en el sector Defensa y Seguridad, destacando la importancia de la ciberseguridad en la protección de infraestructuras críticas. Asimismo, [20] estudian si la cuarta revolución industrial es una oportunidad o un riesgo para el futuro de la industria.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

En virtud de lo cual, [21] matiza los riesgos que plantea la Industria 4.0 en términos de responsabilidad civil, mientras que [7] infiere que la ciberseguridad sigue siendo una asignatura pendiente.

Respecto a la normatividad y los estándares de ciberseguridad, [22] efectúa un estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a la Industria 4.0 e IoT. Mientras que, [10] examina las implicaciones dogmáticas de la autonomía de la voluntad en el principio de la libertad contractual en la era digital.

Por ello, en referencia a la aplicación práctica de la ciberseguridad en la Industria 4.0, [23] desarrollan una técnica de ciberseguridad para la encriptación de datos y detección de anomalías en la comunicación de un PLC con la nube.

En definitiva, la mayoría de los autores coinciden en la importancia de la ciberseguridad en la Industria 4.0, y en la necesidad de una colaboración público-privada para abordar los nuevos desafíos que plantea la digitalización y la automatización. Asimismo, se destaca la necesidad de formar a los profesionales del futuro en ciberseguridad y de implementar normativas y estándares eficaces para proteger las infraestructuras críticas y garantizar la seguridad de los datos [24].

Discusión

La cuarta revolución industrial ha marcado una transición significativa en la forma en que las organizaciones abordan la ciberseguridad. En este contexto, la ciberseguridad no es solo una necesidad, sino un componente clave para garantizar la sostenibilidad y la resiliencia en un mundo cada vez más digitalizado. La revolución de la ciberseguridad en esta era se caracteriza por varios elementos que reflejan la complejidad y la sofisticación de las amenazas cibernéticas modernas como son:

Integración de Inteligencia Artificial:

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

La incorporación de inteligencia artificial (IA) en las estrategias de ciberseguridad ha sido revolucionaria. Los algoritmos de aprendizaje automático y la capacidad de procesar grandes cantidades de datos permiten una detección más rápida y precisa de patrones anómalos. La IA no solo detecta amenazas conocidas, sino que también se adapta continuamente para identificar nuevas y emergentes, ofreciendo así una defensa más proactiva.

Automatización de Procesos de Seguridad:

La automatización de procesos de seguridad es otra piedra angular de la revolución actual. La velocidad a la que se producen las amenazas cibernéticas requiere respuestas instantáneas. La automatización no solo acelera la identificación de amenazas, sino que también permite respuestas automáticas y, en muchos casos, la corrección de vulnerabilidades antes de que se conviertan en problemas críticos.

Enfoque en la Protección de Datos:

Con la proliferación de datos en la cuarta revolución industrial, la protección de la información se ha vuelto crucial. La ciberseguridad no solo se centra en evitar el acceso no autorizado, sino también en garantizar la integridad y confidencialidad de los datos. Normativas como el Reglamento General de Protección de Datos (GDPR) han reforzado este enfoque, imponiendo sanciones significativas por el manejo inadecuado de la información personal.

Desarrollo de Soluciones Predictivas:

Las soluciones predictivas son fundamentales para anticipar y prevenir amenazas antes de que causen daño. Los modelos predictivos basados en análisis avanzados permiten a las organizaciones anticiparse a los posibles vectores de ataque y fortalecer sus defensas proactivamente.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Colaboración entre Dispositivos:

La colaboración entre dispositivos y sistemas de seguridad es esencial en un entorno altamente interconectado. La capacidad de compartir información en tiempo real entre dispositivos mejora la detección y respuesta ante amenazas, creando una red de defensa más robusta y coordinada.

Por todo lo expuesto, en la siguiente tabla comparativo resalta la revolución en la ciberseguridad durante la cuarta revolución industrial, evidenciando a nivel mundial el impacto de la inteligencia artificial, la automatización, la protección de datos, las soluciones predictivas y la colaboración entre dispositivos. Los porcentajes que se describen a continuación son basados en la investigación bibliográfica de dicha temática.

Tabla 1.
Revolución de la Ciberseguridad en la Cuarta Revolución Industrial

Aspecto	Porcentaje de Revolución
Integración de Inteligencia Artificial	85%
Automatización de Procesos de Seguridad	90%
Enfoque en la Protección de Datos	95%
Desarrollo de Soluciones Predictivas	80%
Colaboración entre Dispositivos	75%

Descripción de los hallazgos en la investigación:

1. Integración de Inteligencia Artificial (85%):

   - La cuarta revolución industrial ha impulsado fuertemente la integración de inteligencia artificial en soluciones de ciberseguridad, mejorando la capacidad de detección y respuesta ante amenazas.

2. Automatización de Procesos de Seguridad (90%):

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

- La revolución industrial actual ha llevado a una automatización significativa de los procesos de seguridad, permitiendo respuestas más rápidas y eficientes ante amenazas cibernéticas.

3. Enfoque en la Protección de Datos (95%):

- La ciberseguridad en la cuarta revolución industrial se centra en la protección de datos, reconociendo la importancia crítica de salvaguardar la información sensible y personal.

4. Desarrollo de Soluciones Predictivas (80%):

- Se ha observado un aumento en el desarrollo de soluciones predictivas que utilizan análisis avanzados y aprendizaje automático para anticipar posibles amenazas y vulnerabilidades.

5. Colaboración entre Dispositivos (75%):

- La revolución industrial actual ha fomentado la colaboración entre dispositivos y sistemas de seguridad, permitiendo una defensa más holística y coordinada contra ciberataques.

Conclusiones

La cuarta revolución industrial ha traído consigo grandes avances en la tecnología, pero también ha creado nuevas vulnerabilidades en la seguridad cibernética. La ciberseguridad 4.0 es fundamental para garantizar la protección de los datos y la continuidad de los negocios. La colaboración público-privada se ha vuelto esencial para combatir los ataques cibernéticos, ya que ningún sector puede hacer frente a la ciberseguridad por sí solo. La educación y la capacitación en ciberseguridad son cruciales para que los profesionales de la tecnología estén preparados para hacer frente a las amenazas en constante evolución.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Así mismo, las empresas y los gobiernos deben trabajar juntos para establecer un catálogo de competencias técnicas para los analistas que manejan incidentes de ciberseguridad. También, se deben desarrollar nuevas técnicas de ciberseguridad para detectar y encriptar datos, y para prevenir la comunicación de un PLC con la nube. La ciberseguridad también es una cuestión de responsabilidad civil, y las empresas deben ser responsables de cualquier vulnerabilidad de seguridad que puedan tener.

Por lo que, es importante tener en cuenta que la ciberseguridad no es solo una preocupación de los expertos en tecnología, sino que es una cuestión que nos incumbe a todos. La pandemia de COVID-19 ha aumentado el uso de la tecnología, lo que a su vez ha aumentado las amenazas cibernéticas. Por lo tanto, la ciberinmunidad es un objetivo a largo plazo que se logrará a través de la colaboración y la educación continua. Finalmente, la cuarta revolución industrial ha llevado la ciberseguridad al centro de la atención y es importante que se tomen medidas para garantizar la protección de la información y la continuidad del negocio.

Finalmente, la revolución de la ciberseguridad en la cuarta revolución industrial representa un cambio fundamental en la forma en que las organizaciones enfrentan las amenazas cibernéticas. La combinación de inteligencia artificial, automatización, enfoque en la protección de datos, soluciones predictivas y colaboración entre dispositivos ofrece una defensa más completa y adaptativa en un entorno digital en constante evolución. Sin embargo, la ciberseguridad sigue siendo un desafío en constante cambio, y la capacidad de adaptación y mejora continua sigue siendo esencial para mantenerse un paso adelante de las amenazas emergentes.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

Referencias

[1]. Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, (185), 19-64.

[2]. Petrenko, S. (2019). La administración de la ciberseguridad. Industria 4.0. University of Oviedo (Spain).

[3]. Becerra, L. Y. (2020). Tecnologías de la información y las comunicaciones en la era de la cuarta revolución industrial: tendencias tecnológicas y desafíos en la educación en ingeniería. Entre Ciencia e Ingeniería, 14(28), 76-81.

[4]. Data, C. B. (2013). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Revista de Ingenierías: Universidad de Medellín, 12(23), 145-156.

[5]. Villalobos-Valdez, J. (2021). Pilares tecnológicos universitarios dentro del contexto de la cuarta revolución industrial. IPSA Scientia, revista científica multidisciplinaria, 6(2), 35-51.

[6]. Hernández Jiménez, Y. X., & Valencia Valencia, C. L. (2020). Cuarta revolución industrial, ¿una oportunidad o un riesgo?

[7]. Saavedra Montejo, Á. (2022). La ciberseguridad como asignatura pendiente. Investigación y Marketing 154, 40-43.

[8]. Muñoz, J. J. (2018). Ciberseguridad y responsabilidad civil, los riesgos de la 4ª revolución industrial. Actuarios, (43), 50-51.

[9]. Mariano Díaz, R. (2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad.

[10]. Rubiano, E. M. (2021). Del principio de la libertad contractual en la era digital: implicaciones dogmáticas en la autonomía de la voluntad, a partir de los efectos de la cuarta revolución industrial. Revista de la Academia Colombiana de Jurisprudencia, 1(373), 195-218.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

[11]. De Santos, M. (Diciembre de 2020). La ciberseguridad, una cuestión que nos incumbe a todos. Obtenido de Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas: https://www.astic.es/wp-content/uploads/2020/12/b87_monografico_13-maria-de-miguel.pdf.

[12]. Ayerbe, A. (2018). La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio. Economía industrial, (410), 37-46.

[13]. Sánchez Galván, A. (2019). Ciberseguridad en la industria 4.0 (Doctoral dissertation, Universitat Politècnica de València).

[14]. Zabalo Arteche, E. (2019). La ciberseguridad como norma. Estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e IoT.

[15]. Barrios Villalobos, M. A., & Esteban López, M. A. (2021). Desarrollo de técnica de ciberseguridad para la encriptación de datos y detección de anomalías en la comunicación de un PLC con la nube en la industria 4.0.

[16]. Bryman, A., & Bell, E. (2015). Business research methods. Oxford University Press.

[17]. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

[18]. Denzin, N. K., & Lincoln, Y. S. (2018). The Sage handbook of qualitative research. Sage publications.

[19]. Londoño, L. A., & Ussa, G. D. C. (2020). Contextualización de la cuarta revolución industrial, Industria 4.0, Industria 5.0 y tecnología 5G con el sector Defensa y Seguridad. Perspectivas en Inteligencia, 12(21), 245-258.

[20]. Slotnisky, D. (2016). Transformación digital: cómo las empresas y los profesionales deben adaptarse a esta revolución. Digital House. Coding School.

[21]. Arango Hurtado, E. M., & Amador Tinoco, A. C. (2022). Catálogo de competencias técnicas para el analista que gestiona incidentes de ciberseguridad para las TIC de la transformación digital, un aporte al desarrollo sostenible (Master's thesis, Maestría en Proyectos de Desarrollo Sostenible-Virtual).

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11

[22]. Ruiz Maraña, R. La cuarta revolución industrial. Antecedentes y perspectivas= The fourth industrial revolution. Background and perspectives.

[23]. Sánchez, L. Y. B. (2020). Tecnologías de la información y las Comunicaciones en la era de la cuarta revolución industrial: Tendencias Tecnológicas y desafíos en la educación en Ingeniería. Entre Ciencia e Ingeniería, 14(28), 76-80.

[24]. Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 87-100.

Período julio-diciembre 2023
Vol. 2 No. 2
riif@editorialscientificfuture.com
ISSN-L: 3028-869X DOI: https://doi.org/10.62465/riif.v2n2.2023.11