REVISTA CIENTÍFICA

Vol. 21, No.1 (2025) enero-abril ISSN electrónico: 1683-8947

bibliotecas anales de investigación

BIBLIOTECA NACIONAL DE CUBA JOSÉ MARTÍ

COMPLEJIDADES EN SEGURIDAD DE INFORMACIÓN. ASPECTOS PERSPECTIVOS

COMPLEXITIES IN INFORMATION SECURITY. INTROSPECTIVE ASPECTS

Kterine Ríos Lozano*
Universidad Nacional de San Martín, Perú
krios@unsm.edu.pe
https://orcid.org/0000-0002-0671-8844

Silvestre Quintana Pumachoque
Universidad Nacional de San Martín, Perú
squintana@unsm.edu.pe
https://orcid.org/0000-0001-7172-5007

Augusto Ricardo Llontop-Reátegui
Universidad Nacional de San Martín, Perú
arllontop@unsm.edu.pe
https://orcid.org/0000-0002-5356-2264

Cesar Augusto Rocha Sandoval
Universidad Nacional de San Martín, Perú
carocha@unsm.edu.pe
https://orcid.org/0000-0002-1268-0096

Jaime Cuse Quispe
Universidad Nacional Amazónica de Madre de Dios, Perú
jcuseq@unamad.edu.pe
https://orcid.org/0000-0001-6424-4934

*Autor para la correspondencia: krios@unsm.edu.pe
Contribuciones de los autores: se representa al final del documento

Recibido: 21 de julio de 2024
Revisado: 10 de octubre de 2024
Aprobado: 7 de noviembre de 2024

Cómo citar: Ríos Lozano; K; Silvestre Quintana Pumachoque, S; Llontop-Reátegui, A.R; Rocha Sandoval, C. A. y Jaime Cuse Quispe (2025). Complejidades en seguridad de información. Aspectos perspectivos. *Bibliotecas. Anales de Investigacion;21*(1), 1-13 http://revistas.bnjm.sld.cu/index.php/BAI/article/view/963

RESUMEN

Objetivo: Tratar en esta investigación a la complejidad de la seguridad de la información desde dos interactuantes del entorno digital, es un reto ante el desarrollo de los procedimientos tecnológico: la Internet de las cosas, el interactuante potencial de la seguridad de la información, y la auditoria informática el proceso evaluador y de control para una óptima operatividad. **Metodología:** Con enfoque reflexivo y documental, apoyado en una revisión sistemática de la literatura, de alcance exploratorio, método y recursos de la investigación cualitativa, el análisis cualitativo con perspectiva teórica vincula diversos criterios entorno a la operatividad en la seguridad de la información, se seleccionaron bajo criterios de inclusión 32 artículos para el estudio. **Resultados y Discusión:** Los dos interactuantes implicados en la investigación aportan desde su actuar, criterios de análisis, los beneficios y dificultades que se plantean y que constituyen retos y desafíos a tener en cuenta, donde la seguridad y privacidad, es una condición de éxito o fracaso del proyecto informacional a nivel institucional, o público, por lo que se requiere de desarrolladores de sistemas de recolección y recopilación de datos seguros e interoperables en todos los ámbitos del IoT. **Conclusión:** En el ámbito del Ciberespacio y la necesaria seguridad de la información demanda de modelos, estándares legislativos y de protocolización de sus procesos para la internet de las cosas y en las auditorias. **Aporte**: se propone a partir de los criterios expuesto mantener un ambiente colaborativo con plataformas de ciberseguridad de la información, así como estar informado sobre las últimas vulnerabilidades y ataques, e incorporar estas acciones a nuestra cultura organizacional.
PALABRAS CLAVE: seguridad de la información, auditoría informática, internet de las cosas, ciberseguridad

ABSTRACT

Objective: In this research, addressing the complexity of information security from two interacting parties in the digital environment is a challenge in the face of the development of technological procedures: the Internet of Things, the potential interacting party of information security, and computer auditing, the evaluation and control process for optimal operation. **Methodology:** With a reflexive and documentary approach, supported by a systematic review of the literature, exploratory in scope, method and resources of qualitative research, qualitative analysis with a theoretical perspective links various criteria around the operation of information security. 32 articles were selected for the study under inclusion criteria. **Results and Discussion:** The two interacting parties involved in the research contribute from their actions, analysis criteria, the benefits and difficulties that arise and that constitute challenges and challenges to be taken into account, where security and privacy are a condition for success or failure of the information project at an institutional or public level, which is why developers of secure and interoperable data collection and compilation systems are required in all areas of the IoT. **Conclusion:** In the field of cyberspace and the necessary information security, there is a demand for models, legislative standards and protocols for its processes for the Internet of Things and audits. **Contribution:** based on the criteria outlined, it is proposed to maintain a collaborative environment with information cybersecurity platforms, as well as to be informed about the latest vulnerabilities and attacks, and to incorporate these actions into our organizational culture.
KEY WORDS: information security, computer audit, Internet of Things, cybersecurity

INTRODUCCIÓN

En un mundo cada vez más informatizado, digitalizado e interactivo, cada vez más dependiente con el desarrollo de las tecnologías en función del big data. Se retribuye la necesidad de crear y diseñar sistemas de seguridad informática y elaborar de estrategias que contribuyen al control, optimización y seguridad de los datos de estos entornos. Grandes retos se desarrollan, las tecnologías emergentes continúan evolucionando, por lo que surgen nuevos desafíos éticos y legales en el ámbito de la seguridad de la información asegura las investigaciones de Álvarez, (2021). El uso de tecnologías como la inteligencia artificial (IA), traza asuntos importantes para prácticas éticas y eficientes, en temas sobre la transparencia, la responsabilidad y el sesgo algorítmico, mientras que la Internet de las cosas (IoT) esboza preocupaciones sobre la privacidad y la seguridad de los datos personales. La computación en la nube y el aprendizaje automático (AA) o en sus siglas

en inglés (ML), son de los transformadores que de manera radical están determinando las formas en que las organizaciones gestionan sus sistemas de seguridad (Evans, 2011; Barrio, 2018; Martínez & Cruz, 2018).

El panorama de seguridad de la información, es cada vez más preocupante y determinante para la sociedad. Donde no es solo el proceder a nivel institucional, sino que se deben garantizar la seguridad de los sistemas de datos, pero también la privacidad y la integridad de la información de clientes y usuarios en general (Díaz et al., 2018). En este contexto, la colaboración y el intercambio de información entre empresas, gobiernos y organizaciones internacionales es esencial la valoración de esta situación de seguridad, es un frente común en constante estudio, donde sus miras se detienen en la ciberseguridad y privacidad de los datos de los usuarios y clientes Díaz y Molinari et al. (2018); Radanliev, P. (2023)

Diversas son ya las directrices que conforman modelos y sistemas de control, y que se han ido implementando en diferentes partes del mundo, con diferentes rango y alcances de implementación, como lo es:

. Reglamento General de Protección de Datos (GDPR) en la Unión Europea (UE). Se establecen requisitos específicos para las empresas y organizaciones sobre temas de recogida, almacenamiento y gestión de los datos personales Se implementa en organizaciones europeas que tratan datos personales de ciudadanos en la UE, y en las organizaciones con sede fuera de la UE, cuya actividad se dirige a personas que viven en la UE. Y se instrumenta cuando la organización trata datos personales, desde una sede en UE, aparte de dónde se traten de hecho los datos, y aunque tengan su sede fuera de la UE, y trata datos personales relativos a ofertas de bienes o servicios a ciudadanos en la UE, o supervisa el comportamiento de ciudadanos en la UE.

. En el contexto del artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos se establece “que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación”. El derecho a la privacidad es uno de los pilares de una sociedad democrática y desempeña un papel fundamental en la realización de una amplia gama de derechos humanos, inclusive en la esfera digital,

Como marco jurídico desde 2013, la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos han aprobado numerosas resoluciones sobre el derecho a la privacidad en la era digital. Las más reciente sobre el derecho a la privacidad en la era digital fue aprobada por el Consejo de Derechos Humanos en septiembre de 2019: A/HRC/RES/42/15. Y entre los aspectos que trata están sobre la privacidad en Internet, su protección; y reconoce que la utilización, el despliegue y el desarrollo ulterior de tecnologías nuevas y emergentes, como la inteligencia artificial, pueden afectar al disfrute del derecho a la privacidad y otros derechos humanos, especifica sus pautas.

. Política de acceso a la información de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) muestra una semejanza positiva en su alto nivel de correlación informativa, la transparencia, difusión de la información, y la participación pública en las actividades apoyadas por la Organización, distinguen su actuar como organización Mundial.

Su política promueve la libertad de información y considera que el acceso público a la información, un compromiso, sus recursos de información: la web de la UNESCO, el Portal de Datos de la UNESCO, la Biblioteca Digital de la UNESCO, entre otros espacios en la web. La confidencialidad y la protección de los datos, actúan coherentemente con las pautas relacionadas con la política de clasificación de la sensibilidad de la información de la UNESCO.

Uno de sus recursos destacado es el Portal de Datos de la UNESCO que publica datos, con arreglo a la norma de la Iniciativa Internacional para la Transparencia de la Ayuda (IATI). El Portal está concebido para facilitar el acceso público a la información, sobre las actividades de la Organización en los diferentes sectores, países y regiones, se puede acceder por https://core.unesco.org/en/home

Abordar la complejidad de la seguridad de la información desde dos implementos, actores o interactuantes del entorno digital; es un reto investigativo, que le acontece un acelerado desarrollo de sus procedimientos tecnológico: la Internet de las cosas, el interactuante potencial de la seguridad de la información, y la auditoria informática el proceso evaluador y de control para una óptima operatividad, se valoran en está investigación, que precisamente tiene este objetivo, en aras de contribuir a la conformación de criterios que propicien enriquecer el conocimiento en cuanto a seguridad de la información.

METODOLOGÍA

La investigación se basa en aspectos perspectivos y criterios que asume el entorno digital para la seguridad de la información y que son desarrolladas por diferentes autores. El enfoque utilizado es reflexivo y documental, apoyado en una revisión sistemática de la literatura, de alcance exploratorio, método y recurso de la investigación cualitativa, para evaluar estados y tendencias de la situación.

Mediante el análisis cualitativo con perspectiva teórica se vinculan diversos criterios entorno a la operatividad en la seguridad de la información desde las perspectivas de los interactuantes: Internet de las cosas y la auditoría informática, esto permitió identificar criterios y organizarlos en función de esta compleja problemática, la seguridad de la información.

El abordaje en la investigación como un estudio reflexivo, toma en cuenta las concepciones De la Cuesta-Benjumea (2011), quien afirma que este tipo de estudio, es un proceso en el cual el investigador examina críticamente su impacto en el estudio y en las interacciones con los participantes. La reflexividad, presente en las interacciones sociales, es fundamental en la investigación cualitativa y tiene un carácter formativo que persiste incluso después de concluido el estudio. Argumentación que se cumplimenta como objetivo de esta propuesta investigativa.

Además, se utilizó información de bases de datos como Scopus y Scielo. También se examinaron informes y documentos normativos y oficiales para ofrecer una visión general de la situación, y que permitan una comprensión más profunda de los factores que influyen en la seguridad y control de la información. Las palabras clave utilizadas en la ecuación de búsqueda, fueron: seguridad de información, ciberseguridad, internet de las cosas, auditoria informática.

Los criterios para la inclusión de los 32 documentos seleccionados para la investigación se sustento en:
. Documentos emitidos o publicados desde 2015, hasta la fecha
. Documentos de instituciones normalizadoras o reguladoras de carácter macro
. Como artículos o documentos científicos, los publicados en inglés y/o español en revistas, sitios web o editoriales especializadas

RESULTADOS Y DISCUSIÓ0N

Internet de las cosas

La Internet de las cosas (IdC) es un proceso tecnológico, todo un sistema que permite que los objetos físicos (o grupos de estos) a través de sus sensores, su capacidad de procesamiento, software y otras cualidades tecnológicas, conectarse estos entre sí y con internet, donde intercambian datos a través de redes de comunicación aseguran investigaciones de Alvear-Puertas, Rosero-Montalvo et al. (2017) y Ávila-Camacho & Moreno-Villalba (2023). Aunque existe una gran divergencia en cuanto al término, se ha desarrollado este campo dado a la convergencia de variadas tecnologías, como la informática ubicua, los sensores, los sistemas integrados cada vez más potentes y el aprendizaje automático. Es todo un ventajoso ecosistema que conecta casi todo, y donde el usuario puede controlar sus dispositivos desde cualquier lugar, (Ávila-Camacho & Moreno-Villalba, 2023)

En el mercado de consumo, la tecnología del IdC se identifica desde el concepto de “hogar inteligente”, que incluye dispositivos de iluminación, sistemas de seguridad del hogar, cámaras termostatos y otros

electrodomésticos que se controlan a través de dispositivos asociados a ese ecosistema, como los móviles y altavoces inteligentes. Otras aplicaciones están dadas en los sistemas sanitarios, servicios turísticos y bancarios entre otros, (Alvear-Puertas, Rosero-Montalvo et al. 2017). Zanella y Castellani et al. (2014).

Entorno a la privacidad y la seguridad de datos hay muchas interrogantes sobre los riesgos en el crecimiento de las tecnologías y los productos del IdC, y se toman medidas, como normas internacionales y locales, directrices y marcos regulatorios, ante el desarrollo de estas tecnologías, ejemplo el ya mencionado GDPR por parte de la Unión Europea Hu, et al. 2022)

Las aplicaciones en función de los dispositivos conectados a internet son vastas. La interconectividad desde todos los ámbitos de la sociedad, es cada vez más evidente. (Gubbi, & Rajkumar, et al,. (2013). La actual revolución de la información, manifestada precisamente por el nivel de interconectividad de todo, es un manifiesto del actual desarrollo en la recolección de información, desde ecosistemas estructurales, que propician un exponencial impulso al tratamiento al dato, que se propicia en todo ámbito de la sociedad: el institucional, organizacional y el público, permitiendo un importante nivel de actuación, como por el ejemplo para el monitoreo ambiental y planeamiento urbanístico, Laplante, et al. (2018).

El diseño es crucial para el éxito de las soluciones IoT centrado en el usuario, donde la finalidad es poner las necesidades y deseos del usuario en el centro del proceso de diseño, de ahí su premisa, donde todo puede estar conectado a la red, todo este proceso se hace potencial, con el procesamiento de datos por parte de múltiples desarrolladores interconectados, donde los soportes o dispositivos sean funcionales, intuitivos y agradables de usar, (Ávila-Camacho & Moreno-Villalba, 2023)

El Internet de las Cosas (IoT, por sus siglas en inglés) transforma la forma de interactuar en la sociedad; revoluciona todos los aspectos de la sociedad: hogares inteligentes, ciudades conectadas, aplicaciones generativas, es visible una multiaplicabilidad del Internet de las Cosas. (Gubbi, & Rajkumar, et al,. 2013; Ávila-Camacho & Moreno-Villalba, 2023)

El IoT está en constante evolución y los avances tecnológicos e innovaciones actuales, están potenciando el conocimiento y sus capacidades, que están haciendo que sus capacidades, sean cada vez más determinante para los ámbitos de progreso en la sociedad, (Gubbi, & Rajkumar, et al,. 2013; Ávila-Camacho & Moreno-Villalba, 2023), por lo se evidencia en:

Sensores evolucionados, que permite una mayor recolección de datos, demostrando más precisión y niveles de sensibilidad, adecuados para una mejora en la toma de decisiones en tiempo real.

Redes 5G. Esta tecnología permite ganar una conectividad más rápida, eficiente y a su vez optima, potenciando el desarrollo de nuevos dispositivos con mayor ancho de banda.

Edge Computing: para crear ámbitos de mejoras en la velocidad de respuesta y por ende reducir los costes de transmisión, esta tecnología reduce la carga en la nube al procesar los datos con mejores perspectivas.

Inteligencia Artificial (IA). Todos los sectores disponen de desarrolladores de conocimiento gracias a esta tecnología, que se integra con más poder de decisión sobre el IoT, con un alto nivel de análisis de datos en tiempo real.

Realidad Virtual (AR) y realidad virtual (VR) van en creciente desarrollo, tecnologías que se integran y propician incorporarse en consolas de videojuegos y juegos en línea, pero, también, se integran con herramientas educativas y a la interactuación de compras en línea, además reducción en los costos de los dispositivos, es una singularidad para los públicos.

Seguridad potenciada. Con el crecimiento del IoT, el entorno de ciberseguridad se prioriza, con avanzadas políticas y protocolos, en aras de proteger a los dispositivos y a los datos. (Ávila-Camacho & Moreno-Villalba, 2023)

El Internet de las cosas propicia beneficios y ventajas a sector empresarial, ante retos y desafíos a tener en cuenta. La seguridad y privacidad, es una condición de éxito o fracaso del proyecto informacional a nivel institucional, al igual lo es a nivel público, por lo que se requiere de desarrolladores de sistemas de recolección y recopilación de datos seguros e interoperables en todos los ámbitos del IoT.

Auditoría informática

La auditoría informática se ha vuelto cada vez más en un proceso más distinguido en el ámbito de la seguridad de la información o la ciberseguridad, el sector empresarial lo ha tomado como parte de su flujo operativo debido a la creciente interactuación con las tecnologías de información (Antunes et al., 2022).

Este contexto de revisión informática en aras de buenas prácticas, es esencial para garantizar la privacidad, confidencialidad, coherencia y accesibilidad de los datos e información, en aras que se cumple con las normativas y regulaciones aplicables en cuanto a la seguridad de la información (Politou et al., 2019).

El proceso de auditar informática en el entorno digital, es fundamental para la evaluación y el control de los sistemas informáticos y sus actores (software y hardware), es desde donde se establecen criterios para identificar riesgos, vulnerabilidades y oportunidades en la mejora del ámbito de las tecnologías de la información y por ende a su seguridad para la eficiencia de la información, afirman Proaño y Saguay et al. (2017).. Por lo que el objetivo principal de la auditoría informática precisamente es garantizar que los sistemas y las infraestructuras de TI estén diseñados, implementados y mantenidos de manera eficiente y efectiva, y en respuesta a los objetivos y metas de la organización, un proceso complejo, protocolizado y esencial, resultados de las investigaciones de Serna y Montoya et al. (2020); Progoulakis y Rohmeyer et al. (2021).

En el ámbito del Ciberespacio se desarrollan varios modelos de seguridad para servir como referente en el desarrollo de una auditoría informática en las organizaciones, algunos de ellos son y que acreditan Sabillón et al. (2019); Randall & Allen (2021).

. COBIT, (Objetivos de control para la información y tecnologías relacionadas) garantizan procesos y controles de TI, para que sean adecuados, eficientes y estén alineados con los objetivos estratégicos de la organización (Schmitz et al., 2021). Cuando se realizan las auditorias en este marco: COBIT, se contribuye igual a verificar el cumplimiento de políticas y directrices aplicables, así como aportar recomendaciones que fortalezcan la seguridad y su gestión de riesgos en el entorno de TI (Paredes et al., 2018).

. LCCI, La Cámara de Comercio e Industria de Londres (LCCI) es esta entidad emite certificaciones y calificaciones en diversos campos, y en la auditoría informática valida y reconoce las habilidades y competencias de los profesionales en la realización de auditorías de sistemas y seguridad informática, al cumplir estos los estándares y sus buenas prácticas, que son de amplio reconocimiento a nivel mundial y abarca aspectos como la evaluación de riesgos, la gestión de incidentes, la detección de vulnerabilidades, y la revisión de controles internos (Pawar et al., 2022)

. CSF es el marco de ciberseguridad, que son en sí un conjunto de pautas esenciales para la auditoría informática que contribuye a las organizaciones a establecer, implementar y mantener un sistema efectivo de seguridad de la información. Su estructura proporciona identificar y gestionar riesgos, garantizar el cumplimiento normativo, proteger los activos de información y fortalecer las políticas de seguridad, por ende, su defensa (Alruwaili et al., 2018).

. ISG, es la gobernanza de seguridad de la información un componente integral en el ámbito de la auditoría informática, que se centra en establecer y mantener un marco para garantizar que la organización cumpla con los requisitos internos y externos en materia de seguridad de la información (Sulistyowati et al., 2020).

. D4I este enfoque proporciona una estructura integral para tratar aspectos clave de la auditoría informática, propiciando una evaluación profunda de los sistemas y tecnologías de la información, que va desde el proceso de auditoría informática, la detección de problemas, la generación de informes, pasando por la investigación y la implementación de medidas correctivas. Los auditores al utilizar esta guía, pueden eficientemente identificar y analizar riesgos y vulnerabilidades, investigar incidentes de seguridad, implementar soluciones adecuadas y documentar los resultados en informes detallados (Dimitriadis et al., 2019).

. ISO/IEC 27001, está norma parte de la Organización Internacional de Normalización, es un estándar global que garantiza la protección, confiabilidad e integridad de la información, así como de los procesos involucrados, además. proporciona a las organizaciones la capacidad de evaluar los riesgos y establecer los controles necesarios para mitigar o eliminar dichos riesgos, asegura Chifla (2020).

La complejidad

Los temas de información, su tratamiento y conservación se van redimensionando en su clasificación, y esencialmente por su aplicabilidad de uso: consumidores, empresarial, e infraestructura, donde la internet de las cosas es su fase revolucionaria en la información, donde se prescribe a la interconectividad de todo: desde el transporte urbano, gestión médica, electrodomésticos, seguridad pública, privada e institucional, entre otros ámbitos que pronto se harán la mayoría (Burgos-Rojas y Haro-Polo, et al. 2024). La capacidad de conectar dispositivos embebidos con capacidades limitadas de CPU, memoria y energía significa que la internet de las cosas (IdC) puede tener aplicaciones en casi cualquier área.

Estos sistemas interconectados podrían encargarse de recolectar información en todo ámbito, por ejemplo, en los ecosistemas naturales, edificios y fábricas, se generaría información sobre monitoreo ambiental y planeamiento urbanístico.

Ya con la incidencia de la inteligencia artificial los sistemas de compra inteligentes, siguen los hábitos de compra de sus usuarios rastreando su teléfono móvil y su conexión con las redes, estos usuarios disponen de ofertas especiales. Y así por ejemplo en el uso de aplicaciones que se encargan de la calefacción, el suministro de agua, electricidad, la administración de energía e incluso sistemas inteligentes de transporte que asistan al conductor. Ya hay estudios referentes al uso ADN, y condiciones patológicas de los seres humanos para la toma de decisiones (Burgos-Rojas y Haro-Polo, et al. 2024).

Las claves para un éxito en la gestión en la seguridad de la información, esta en el establecimientos de un plan de seguridad de las TIC que debe existir en cada una de las organizaciones para proteger los sistemas y datos de una organización contra posibles amenazas de ciberseguridad en las organizaciones, donde se incluya, describir y aplicar políticas, medidas y procedimientos diseñados para esta a partir una estimación de riesgos y establecer las responsabilidades de los diferentes actores, todo un proceso donde se garantice la seguridad tanto de la información de los consumidores como de las organizaciones según expresan Cano & Monsalve (2023). No disponer de un plan de seguridad informática expone a riesgos de fuga de información a incumplimiento de responsabilidades legales. Amen que se priorizan acciones para enfrentar y prevenir ataques de terceros, como hackers y ciberdelincuentes.

Algunos de los elementos claves para el plan de seguridad de las TI. Están en:

- Definir el radio de acción de dicho plan
- Caracterizar al sistema informático, particularidades, y componentes
- Análisis de riesgo, proceso continuo en interacción con efectos y probabilidades
- Políticas de seguridad informática, este conjunto de normas, reglas y directrices garantizarían la confidencialidad, integridad y disponibilidad de la información, al tiempo que minimizan los riesgos asociados al uso de la tecnología en una organización.
- Desarrollar estrategias de evaluación de vulnerabilidades y gestión de riesgos
- Estrategias para la formación en ciberseguridad, potenciando una fuerza laboral competente y consciente, con capacitación también en herramientas efectivas que fortalezcan la resiliencia de la organización ante los posibles ataques cibernéticos. Tsohou, y Diamantopoulou et al. (2023). Yadav & Kumar (2023).

La complejidad estará dada precisamente en la capacidad institucional para la creación de un plan de seguridad tecnológica que garantice la seguridad de la información a todos los niveles y permita gestionar riesgos de manera efectiva, que implicaría ante las vulnerabilidades, identificar y analizar las debilidades en los sistemas, redes y aplicaciones que involucran al trabajo de la organización, posible esto, mediante pruebas de penetración, análisis de seguridad y asiduas auditorías. La detección de las vulnerabilidades, implicaría tomar medidas proactivas para atajar toda irregularidad en el ciberespacio.

La gestión de riesgos constituye un proceso fundamental que puede conllevar a la adopción de políticas de seguridad y dictámenes en cuanto a controles de acceso y autenticación, segmentación de redes y la protocolización de copias de seguridad de datos, este accionar conlleva a plantear un enfoque integral en la

gestión de riesgos, y reducir así la probabilidad de ataque cibernético u otro impacto negativo en su entorno web, (Burgos-Rojas y Haro-Polo, et al. 2024); Zboril, M., & Svatá, V. (2022).

Los ransomware, código maligno que infecta e inutiliza al equipo, es otro de los malware en informática , donde el ciberdelincuente toma el control del equipo cifrando la información , bloqueando al equipo , es una amenazas más persistentes, que se dirige con precisión a infraestructuras críticas, ataques que buscan beneficios económicos, pero también amenazan la estabilidad de la organización, lo que se procura de estrategias robustas y proactivas, donde el entrono web, es determinante para el desarrollo y supervivencia de la organización.(Gourisetti & Mylrea (2020); Progoulakis & Rohmeyer (2021); Radanliev, (2023).

El espacio de la ciberseguridad, es crucial y comprende no solo la implementación de tecnologías de avanzada, sino también de empoderar a las usuarios y clientes, y a la sociedad en sí, en la formación e identificación de amenazas, y a mejores prácticas para fortalezcan la actitud de seguridad de la organización como parte de un ecosistema. La utilización de herramientas efectivas para fortalecer la resiliencia de una organización ante los ataques cibernéticos., es determinante para el éxito institucional. Como parte de la preparación, simular los phishing implican enviar correos falsos a los empleados, imitando las técnicas utilizadas por los ciberdelincuentes, y así se evalúa la preparación y conciencia de la organización frente a las amenazas Radanliev, (2023). Con estos simulacros se identifican las áreas de mejora y brindar una retroalimentación individualizada a los empleados, para su capacitación y conocimiento ante posibles ataques de phishing. Propiciando un ambiente seguro de aprendizaje y práctica, fortaleciendo las defensas de la organización, potenciando la seguridad de su información.

CONCLUSIONES

La interconectividad desde todos los ámbitos de la sociedad, hace de la funcionalidad de la internet de las cosas, todo un modelo de actuación en el ciberespacio, cada vez más eficiente. La actual revolución de la información, su nivel de interconectividad, hace todo un manifiesto del actual desarrollo en las colecciones de información, ecosistemas estructurales, que propician un exponencial impulso al tratamiento al dato, que se propicia en todo ámbito de la sociedad: el institucional, organizacional y el público, los que demandan de todos los mecanismos de seguridad posible y en perspectiva.

El proceso de auditar informática garantiza que los sistemas y las infraestructuras de TI estén diseñados, implementados y mantenidos de manera eficiente y efectiva, cumplimentando todo un proceso complejo, de protocolización para su optima utilización.

En el ámbito del Ciberespacio se desarrollan varios modelos de seguridad para servir como referente en el desarrollo de una auditoría informática en las organizaciones Ante un mundo cada vez más digitalmente globalizado, se plantea por los decisores, concientizar implementando programas de capacitación que eduquen sobre las amenazas cibernéticas más comunes y poténcienlas mejores prácticas, programas continuos, que eduquen en función de las tácticas utilizadas por los ciberdelincuentes.

Los clasificados como phishing y/o ransomware son de las amenazas más persistentes, en el entorno digital, la necesidad de estrategias de defensa más robustas y proactivas, se hace inminente e imprescindible para el éxito organizacional, y la gestión privada y de la sociedad en sí, ante la desarrollada incidencia de las tecnologías en nuestro quehacer constante.

El monitoreo continuamente de las actividades en la red para detectar comportamientos inusuales, es un indicador ante las amenazas potenciales del ciberespacio y por una seguridad de información optima. Proteger a los sistemas de información, incluyendo hardware, software y datos, es comprometer a confidencialidad, integridad y disponibilidad de la información, ante su rol por una seguridad informática centrada en la protección de los sistemas interconectados de la red.

Mantener un ambiente colaborativo con plataformas de ciberseguridad contra ataques y compartición de información sobre amenazas, y mantenerse informado sobre las últimas vulnerabilidades y ataques, son de las acciones constante a implementar en nuestra cultura organizacional.

REFRENCIAS BIBBLIOGRÁFICAS

Álvarez, O. D. J. J. (2021). Las Tecnologías Emergentes en la Sociedad del Aprendizaje. Revista Científica Hallazgos21, 6(1), 101-110.

Arango Gomez, O. D. (2023). El ABC de la seguridad informática: guía práctica para entender la seguridad digital. https://www.autoreseditores.com/libro/22997/oscar-dario-arango-gomez/el-abc-de-la-seguridad-informatica-guia-practica-para-entender.html

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946. https://doi.org/10.1016/J.COMNET.2019.106946

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing. Procedia Computer Science, 196, 36–43. https://doi.org/10.1016/J.PROCS.2021.11.070

Alvear-Puertas, V., Rosero-Montalvo, P., Peluffo-Ordóñez, D., & Pijal-Rojas, J. (2017). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura. Enfoque UTE, 8, 244-256. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-65422017000100244&script=sci_abstract&tlng=pt

Ávila-Camacho, F. J., & Moreno-Villalba, L. M. (2023). Internet de las Cosas (IoT) Retos para las Empresas en la era de la Industria 4.0. Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI, 10(20), 10-16. https://repository.uaeh.edu.mx/revistas/index.php/icbi/article/view/9516

Barrio, M. (2018). Internet de las cosas. Madrid: Reus. https://proyectodescartes.org/iCartesiLibri/PDF/IoT.pdf

Bailon Lourido, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. CIENCIAMATRIA, 5(1), 73–87. https://doi.org/10.35381/cm.v5i1.248

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Education and Information Technologies, 27(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Burgos-Rojas, M. A; Haro-Polo, C. A; Mendoza-de los Santos, A. C. (2024) Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática. Revista Científica de la UCSA, (11) 2, 103-115 https://doi.org/10.18004/ucsa/2409-8752/2024.011.02.0103

Castro-Maldonado, J. J., & Villar-Vega, H. F. (2021). Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. Revista modum, 3.

Calle García, A.J; Conforme Merchan, Y. M; Magallanes Bueno, E. L. y Guaranda Bravo. J. Y. (2024) Importancia de la Ciberseguridad en la investigación de mercados digital. Ciencia y Desarrollo 27 (2) http://revistas.uap.edu.pe/ojs/index.php/CYD/index

Calder, A. (2020). The Cyber Security Handbook: Prepare for, respond to and recover from cyber attacks with the IT Governance Cyber Resilience Framework (CRF). IT Governance Publishing. https://doi.org/10.2307/j.ctv19shhms

Cano, W. D., & Monsalve, S. (2023). Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual. [Tesis, Universidad Pontificia Bolivariana]: https://repository.upb.edu.co/handle/20.500.11912/11318

Checco, J. C. (2022). Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management. The Cyber Defense Review, 7(4), 69–90. https://www.jstor.org/stable/48703292

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Cybersecurity Certification Validates Programs. (2020). Computer Security Update, 21(2), 2–4. https://www.jstor.org/stable/48597909

De la Cuesta-Benjumea, C. (2011). La reflexividad: un asunto crítico en la investigación cualitativa. Enfermería clínica, 21(3), 163-167. https://doi.org/10.1016/j.enfcli.2011.02.005

Díaz, F. J., Molinari, L. H., Venosa, P., Macia, N., Lanfranco, E. F., & Sabolansky, A. J. (2018). Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización. In XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015

Evans, D. (2011). Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG, 11(1), 4-11. https://audentia-gestion.fr/cisco/IoT/internet-of-things-iot-ibsg.pdf

Fairview health selects Cynergistek Security. (2020). Computer Security Update, 21(11), 7–8. https://www.jstor.org/stable/48597898

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC, 10(2), 123–141. https://doi.org/10.17993/3ctic.2021.102.123-141

Gillis, Alexander (2021). What is internet of things (IoT)? https://www.rtsrl.eu/blog/what-is-internet-of-things-iot/

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems, 105, 410–431. https://doi.org/10.1016/j.future.2019.12.018

Gubbi, Jayavardhana, G; Rajkumar, B; Slaven, M; Marimuthu, P. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29 (7): 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas

universitarias. Información Tecnológica, 32(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

Hu, J.; Lennox, B.; Arvin, F. (2022) Robust formation control for networked robotic systems using Negative Imaginary dynamics Automatica, https://doi.org/10.1016/j.automatica.2022.110235

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

Internet of Things Global Standards Initiative https://www.lx-group.com.au/blogs/iot-global-standards-initiative .

Internet of Things (IoT) (2024). National Ciberseguryty Center of Excellence https://www.nccoe.nist.gov/iot

Laplante, Phillip A.; Kassab, Mohamad; Laplante, Nancy L.; Voas, Jeffrey M. (2018). «Building Caring Healthcare Systems in the Internet of Things». IEEE Systems Journal 12 (3): 3030-3037.. https://doi.org/doi:10.1109/JSYST.2017.2662602 .

Martínez Santander, C. J., & Cruz Gavilanez, Y. D. L. N. (2018). Tendencias tecnológicas y desafíos de la seguridad informática. Polo del conocimiento, 3, (5), p. 269-279.

Mero Paredes, G. D., & Zambrano González, S. K. (2018). Auditoría informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil. [Tesis Universidad Católica de Santiago de Guayaquil]. http://repositorio.ucsg.edu.ec/handle/3317/10431

Normas internacionales relativas a la privacidad digital. El ACNUDH y la privacidad en la era digital https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1). https://doi.org/10.1016/j.jjimei.2022.100080

Política de acceso a la información de la UNESCO https://www.unesco.org/es/unesco-access-information-policy

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law and Security Review, 34(6), 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Protegemos la información y los sistemas bibliotecarios. https://www.oclc.org/es/trust/security.html

Proaño Escalante, R. A., Saguay Chafla, C. N., Jácome Canchig, S. B., & Sandoval Zambrano, F. (2017). Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información. Enfoque UTE.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. Journal of Marine Science and Engineering, 9(12). https://doi.org/10.3390/JMSE9121384

Radanliev, P. (2023). Review and Comparison of US, EU, and UK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint from 2023. The Review of Socionetwork Strategies 2023, 1–25. https://doi.org/10.1007/S12626-023-00139-X

Randall, R. G., & Allen, S. (2021). Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry. International Journal of Critical Infrastructure Protection, 34, 100454. https://doi.org/10.1016/J.IJCIP.2021.100454

Radanliev, P. (2023). Review and Comparison of US, EU, and UK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint from 2023. The Review of Socionetwork Strategies 1–25. https://doi.org/10.1007/S12626-023-00139-X

Reglamento General de Protección de Datos (GDPR) en la Unión Europea (consultado el 21 de diciembre de 2024 https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Rubén, A., & Guerra, M. (n.d.). Gestión de seguridad de la información con la norma ISO 27001:2013 Information security management with ISO 27001: 2013 standard (39).

Russell, S., & Jackson, S. (2018). Operating in the Dark: Cyber Decision-Making from First Principles. Journal of Information Warfare, 17(1), 1–15. https://www.jstor.org/stable/26504126

Sabillón, R., & M., J. J. C. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 32, 33–48. https://doi.org/10.17013/risti.32.33-48

Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. Computers and Security, 108. https://doi.org/10.1016/j.cose.2021.102306

Serna Ramírez, S., Montoya Londoño, Á., Quintero Barco, Y. A., Henao Villa, C. F., & Castro Ramírez, F. D. J. (2022). Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial. INGENIERÍA: Ciencia, Tecnología e Innovación, 9(2), 135–151. https://doi.org/10.26495/icti.v9i2.2267

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. International Journal on Informatics Visualization, 4(4), 225–230. https://doi.org/10.30630/JOIV.4.4.482

Sohou, A., Diamantopoulou, V., Stefanos Gritzalis, ·, & Lambrinoudakis, · Costas. (2023). Cyber insurance: state of the art, trends and future directions. International Journal of Information Security, 22, 737–48. https://doi.org/10.1007/s10207-023-00660-8

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, · Edmond, Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. SN Computer Science, 3, 127. https://doi.org/10.1007/s42979-022-01020-4

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 1–32. https://doi.org/10.1007/S10462-023-10454-Y/TABLES/17

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 22-32.

Zboril, M., & Svatá, V. (2022). Cloud Adoption Framework. Procedia Computer Science, 207, 483–493. https://doi.org/10.1016/j.procs.2022.09.103

Zhu, P., & Liyanage, J. P. (123 C.E.). Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems. European Journal for Security Research, 6, 125–149. https://doi.org/10.1007/s41125-021-00076-2

Contribuciones de los autores:

Kterine Ríos Lozano: Marco teórico – 21%
Augusto Ricardo Llontop-Reátegui: Metodología – 19%
Silvestre Quintana Pumachoque: Curación de datos – 21%
Cesar Augusto Rocha Sandoval : Triangulación de datos – 21%
Jaime Cuse Quispe: Luna: validación y redacción – 18%