Revista Científica Ciencias Ingenieriles (2024)

Vol. 4, Núm. 2, pp. 74 – 82

https://doi.org/10.54943/ricci.v4i2.516

ISSN: 2961-2357**(En línea)**
ISSN: 2961-2446**(Impreso**

ARTÍCULO DE REVISIÓN

Importancia de la implementación de ciberseguridad en la gestión de riesgos financieros: Clave para garantizar la confianza del cliente

Importance of implementing cybersecurity in financial risk management: key to ensuring customer trust

• Dominick Revilla [1] • Diego Rodriguez [2] • Alberto Mendoza [3]

[1] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t1023300421@unitru.edu.pe
ORCID: https://orcid.org/0009-0008-7902-5302
[2] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t1523300121@unitru.edu.pe
ORCID: https://orcid.org/0009-0001-7754-4343
[3] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: amendozad@unitru.edu.pe
ORCID: https://orcid.org/0000-0002-0469-915X

Recibido: 04 Julio del 2024 / **Revisado**: 24 Julio del 2024 / **Aprobado:** 28 Julio del 2024 / **Publicado:** 29de Agosto del 2024

RESUMEN

En la actualidad, las entidades financieras no solo se ven expuestas a riesgos físicos de seguridad como asaltos y robos sino también de manera cibernética, esto debido al continuo avance de las TI implementadas, las cuales les permiten ser más eficientes en cada una de sus transacciones para su desarrollo de tal manera que les permita sobresalir dentro del sector financiero, generando a su vez algún posible riesgo en sus operaciones y por ende en la confianza depositada por sus clientes. En ese contexto, en el presente artículo se ha decidido investigar sobre el impacto que ha producido la ciberseguridad implementada en la gestión de riesgo dentro de las instituciones financieras, optando por una revisión sistemática de la información que existe entre los años 2019-2024.

A través de un estudio dedicado de la literatura actual logramos tener una visión de las prácticas de ciberseguridad y su enfrentamiento con actos en contra de la integridad financiera.

Palabras claves: Ciberseguridad; sistema bancario; gestión de riesgos; bancos.

ABSTRACT

In today's landscape, financial institutions face not only physical security risks such as robberies and assaults but also cyber threats due to the continuous advancement of IT implementations. These technologies enhance efficiency in transactions, enabling institutions to excel in the financial sector but potentially introducing operational risks that affect client trust. This article explores the impact of cybersecurity on risk management within financial institutions through a systematic review of literature spanning 2019 to 2024.

Through dedicated study of current literature, we gain insights into cybersecurity practices and their effectiveness in safeguarding financial integrity.

Keywords: Cybersecurity; banking system; risk management; banks

1. INTRODUCCIÓN

El surgimiento de Internet y el uso masivo de los nuevos medios de comunicación en los últimos años como los smartphones o las computadoras personales han sido causante de una transformación digital y de la implementación de servicios de TI con el fin de mejorar la eficiencia y la accesibilidad de sus servicios, y empresas financieras no han sido la excepción, pero entrando en un dilema, mientras se aceptan estas novedosas tecnológicas, se enfrentan a una variedad de amenazas cibernéticas.

Un claro ejemplo está en la inversión de los bancos en el desarrollo de aplicaciones móviles para hacer transferencias electrónicas, pagos de facturas, etc.; la automatización de procesos al momento de verificar la identidad o el procesamiento de préstamos; o la analítica de datos el cual le permite identificar ciertos comportamientos o patrones en sus clientes con la finalidad de ofrecer ciertos servicios. Pero todas estas apuestas se ven amenazada por ciertos ataques cibernéticos como podrían ser el Phishing, el malware o ataques de ingeniería social.

En defensa a estos acontecimientos que atacan el equilibrio en finanzas, la implementación de la ciberseguridad y los mecanismos que conlleven se han convertido en la prioridad en las entidades financieras para la gestión de riesgos.

Según (Delgado Fernández, 2020), "Transformación Digital" es el desarrollo progresivo de la tecnología en el cual permite obtener habilidades e implementación mediante nuevos métodos para generar un mejor funcionamiento a las organizaciones con el fin de sobresalir dentro de una sociedad tanto social como cultural y económica.

Según (Lucio-Nieto et al., 2012) basado en ITIL, "Servicio de TI" es una formar de brindar una atención organizada de manera estratégica por las empresas, el cual se busca mantener un crecimiento.

Se entiende que la ciberseguridad es como el escudo protector de los bancos. Básicamente, se trata de un montón de técnicas y prácticas que se usan para mantener a salvo los sistemas, redes y datos de los ataques cibernéticos (Cisco, 2021). En el mundo de los bancos, donde la confianza de los clientes es crucial, tener buena ciberseguridad no es solo una necesidad, sino una prioridad. Las medidas de ciberseguridad no solo protegen el dinero, sino que también hacen que los clientes se sientan seguros al usar los servicios bancarios (Deloitte, 2020).

Con respecto a los bancos, hoy en día dependen mucho de la tecnología para ofrecer y garantizar la calidad de sus servicios. Desde manejar tus cuentas hasta procesar transacciones complicadas, todo se hace a través de sistemas tecnológicos avanzados (BCG, 2019). Aunque esto hace que todo sea más eficiente, también significa que los bancos están expuestos a hackers y otros ciberataques que pueden robar datos o causar problemas financieros graves (KPMG, 2021).

El objetivo de la gestión de riesgos en los bancos es como tener un plan B, C y hasta D para cualquier problema que pueda surgir. Se trata de identificar posibles amenazas, evaluar su impacto y tener estrategias y planes de contingencia para manejarlas (COSO, 2017). Aquí es donde entra en juego la ciberseguridad: proporciona las herramientas necesarias para anticiparse a los problemas y responder rápidamente si ocurre un ataque. Una buena gestión de riesgos no solo protege contra amenazas conocidas como malware y phishing, sino que también prepara a los bancos para futuras amenazas (PwC, 2020).

Es por ello que hay varios tipos de ataques cibernéticos que los bancos enfrentan a diario. Por ejemplo, el phishing es una técnica en la que los atacantes engañan a las personas para que revelen información sensible como contraseñas o números de tarjetas de crédito (Verizon, 2020). El malware es otro problema, y se refiere a programas maliciosos diseñados para infiltrarse en los sistemas y robar datos o causar daños (Symantec, 2021). Los ataques de ingeniería social son otro tipo, donde los hackers manipulan a los empleados o usuarios para obtener acceso a información confidencial (McAfee, 2019).

En resumen, la combinación de tecnología y ciberseguridad trae tanto ventajas como retos para los bancos. Adoptar medidas sólidas de ciberseguridad y tener una buena gestión de riesgos es esencial para que los bancos sigan funcionando sin problemas y con garantías manteniendo la confianza de sus clientes en este mundo digital tan dinámico el cual presenciamos en este siglo XXI.

2. MATERIALES Y MÉTODOS

Para el exhaustivo estudio realizado se optó por hacer una revisión sistemática fundamentado por la metodología PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses). Establecemos los siguientes planteamientos para llevar a cabo el proceso de revisión: ¿Cómo ha impactado la implementación de ciberseguridad en la gestión de riesgos de entidades financieras en los últimos cinco años, y de qué manera este impacto repercute en la seguridad y confianza de los usuarios?

Según (Kitchenham & Charters, 2007), una revisión sistemática es como una especie de búsqueda detallada u otra forma de estudio,

mirando hacia atrás y reuniendo información de diferentes estudios relacionada a una pregunta específica o a tal punto de ser similar en ciertas ocasiones.

Para (Moher et al. 2009), la metodología PRISMA ofrece pautas claras para hacer y presentar revisiones sistemáticas para que el lector haga un análisis profundo y pueda entender u evaluar eficazmente.

En cuanto a la búsqueda de información, hemos identificado las palabras clave relacionadas con nuestro tema de investigación. Estos términos son: "Ciberseguridad", "Gestión de Riesgos" y "Sistemas Bancarios". Además, una vez que identificamos las palabras clave, también buscamos sus traducciones al inglés y sus sinónimos.

La selección de términos en español que utilizamos para la búsqueda fue la siguiente: [("ciberseguridad") AND (("bancos") OR ("Sistemas Bancarios") OR ("Sistemas Financieros")) AND (("Gestión de Servicios") OR ("Gestión de Riesgos"))]

La selección de términos en ingles que utilizamos para la búsqueda fue la siguiente: [(cybersecurity") AND ((Banking) OR ("Banking systems")) AND (("management") OR ("Service Management") OR ("Risk Management"))]

Luego de ello se procedió a utilizar las palabras mencionadas en las siguientes bases de datos: SCOPUS, PUDMED Y GOOGLE ACEDEMICO, para el desarrollo de esta investigación se estableció parámetros, tales como: publicaciones de los últimos 5 años, para comprender el impacto del avance tecnología en la actualidad, y la búsqueda en países como India, Reino Unido, Estados Unidos, Rusia y Argentina ya que cada uno de estos países enfrenta desafíos y amenazas únicos en el ámbito de la ciberseguridad, y sus respuestas varían en función de sus recursos, políticas y enfoques estratégicos.

3. RESULTADOS

Para obtener resultados exactos en la búsqueda de la literatura a revisar, utilizamos criterios de exclusión como: No contiene palabras claves, no guardan relación la ciberseguridad con los sistemas bancarios y por duplicidad.

Por parte de los criterios de inclusión tomamos en cuenta que las publicaciones deben están comprendidas entre los últimos 5 años y que estén en inglés y español.

El total de publicaciones encontradas según los criterios antes mencionados fueron el total de 79 artículos comprendido entre los años 2019-2024 obtenidos de la siguiente forma: Google académico: 26 artículos, Scopus: 38 artículos y PubMed: 15 artículos.

Figura 1.
Resultados por tipo de Base de Datos

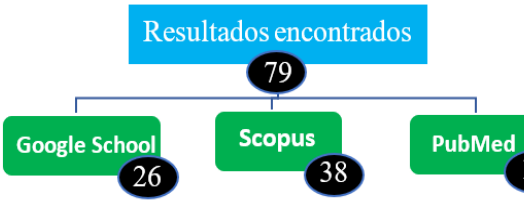
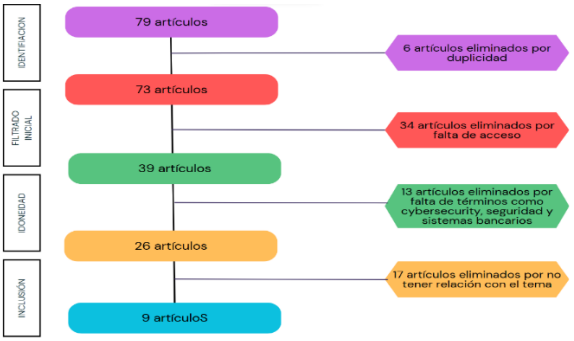


Figura 2.
Flujograma del proceso de selección de artículos



De un total de 79 artículos encontrados, siguiendo la metodología PRISMA que abarcan los criterios de exclusión y exclusión podemos observar en el flujograma la selección de 9 artículos, los cuales están ordenados en la **Tabla 1.**

Tabla 1
Cantidad de artículos por Base de Datos.

Bases de Datos	Cantidad	Porcentaje
Google Académico	2	22,22%
Scopus	5	55,56%
PubMed	*2*	22,22%

Tabla 2.
Detalle de los artículos seleccionados y su relevancia

id	Cita	Fuente	País	Año Publicación	Relevancia
1	(Carlos Vilchez, J., Asesor, V., Cecilia, K., & Burgos, R.,2022	Google Académico	Perú	2022	Incentivan y exigen la motivación de campañas de concientización en los entes bancarios explicando sobre el posible uso de datos sensibles sin restricciones y/o conocimiento del cliente y el peligro que esto representa en la actualidad,
2	(Fu, Zhengtang, Peiwu Dong, Siyao Li, y Yanbing Ju.,2021)	PubMed	Italia	2021	El Uso de una nueva tecnología en los Bancos como el Blockchain durante los últimos años ha ayudado a ejecutar transacciones bancarias de manera más segura y siguiendo cada uno de sus protocolos de manera instantánea, lo cual genera una relación de confianza mayor con el cliente.
3	(Johri & Kumar, 2023)	Scopus	India	2023	Resaltan la relación de la ciberseguridad y la importancia en relación a la satisfacción del cliente. Exigencia por parte de entes reguladores sobre los bancos en relación a campañas de concientización.
4	(Martinez Mesa & Martines de la Peña, 2022)	Google Académico	Colombia	2022	Con el incremento desmedido de transacciones financieras, la integridad de los datos y la lucha contra los ciberataques se convirtieron en retos críticos.
5	(Lavanya, B., & Dunstan Rajkumar, A.,2024)	Scopus	India	2024	Por el bien común de cada una de empresas, priorizan la comunicación y el apoyo mutuo ante casos de ataques de seguridad en línea para la implementación de un plan de contingencia y una mejor preparación para una mejor atención al cliente en caso de pérdida de datos.
6	(Saxena et al., 2023)	Scopus	India	2023	Datos confidenciales como los que son tratados por entidades financieras deben ser salvaguardados por estrategias de ciberseguridad.
7	(Tamanna et al., 2024)	Scopus	India	2024	Es imperativo la implementación de potentes sistemas de seguridad de la información, debido a la gran e

					importante cantidad de información de guardan los bancos sobre sus clientes.
8	(Uddin, M. H., Mollah, S., & Ali, M. H., 2020)	PubMed	Reino Unido	2020	Las inversiones realizadas para mejorar y actualizar sus tecnologías desarrolladas en sus sistemas para evitar fraudes cibernéticos no siempre les genera ganancias, muy por el contrario, generan pérdidas significativas, sin embargo, deben seguir invirtiendo para mantener la protección de datos de los clientes para su comodidad.
9	Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023)	Scopus	Reino Unido	2023	Priorizan la protección de datos dividiendo la atención del cliente en áreas de prevención, seguridad confidencialidad y operaciones.

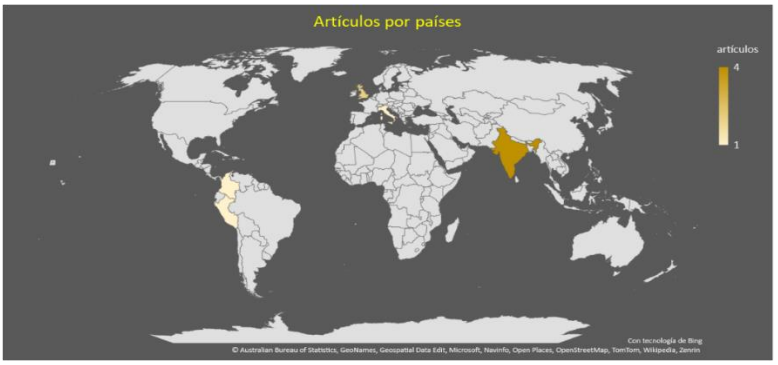
A continuación, se muestra una tabla donde se observa la cantidad de tesis y artículos elegidos finalmente. Ver Tabla 3

Tabla 3.
Total de artículos por países

India	4	44,45%
Reino unido	2	22,22%
Peru	1	11,11%
Colombia	1	11,11%
Italia	1	11,11%
Total	**9**	**100%**

Ahora se muestra la locación geográfica de los países de donde provienen los articulo seleccionados a revisar. Como resultado obtuvimos a La India como el país con más artículos publicados con 4 publicaciones, seguido por Reino Unido con 3 publicaciones, Perú, Italia y Colombia estos tres ultimo un artículo cada uno.

Figura 3
Representación de artículos por países



La importancia de la Implementación de ciberseguridad en la gestión de riesgos de entidades financieras: Clave para garantizar la Confianza del Cliente.

La literatura revisada nos deja ideas de autores en común como que los datos de los clientes están en manos de entidades bancarias las cuales sufren constantes ataques por parte de ciberdelincuentes, buscando los espacios más vulnerables donde atacar y robar esta información con el fin de obtener algún tipo de redito

El delito cibernético consiste en acceder de manera no autorizada a redes de computadoras para obtener datos, dañar el sistema operativo, el hardware o los programas a través de un ataque. La ciberseguridad es una herramienta fundamental para proteger datos e información confidencial (Saxena et al., 2023).

En los últimos tiempos las transacciones financieras se dispararon haciendo que la integridad de los datos y la defensa contra ciberataques se transforman en grandes retos críticos que deben abordarse de manera eficiente. (Martinez Mesa & Martines de la Peña, 2022).

Tamanna et al (2024) afirmaron que el riesgo es muy alto para las entidades financieras debido a la gran cantidad de información que guardan sobre sus clientes tales como sus nombres, dirección, patrimonio, etc; como consecuencia se vuelve imperativo que potentes sistemas de seguridad sean implementados en bancos y entidades financieras o cualquier otra institución con o sin fines de lucros, de ahí que la ciberseguridad sea altamente importante en las finanzas.

El papel de la concientización sobre la ciberseguridad debe entenderse por las instituciones financieras como parte de la satisfacción del cliente y de su respectiva seguridad. Además, los entes encargados de regular el sector bancario deben exigir y motivar campañas de concientización constantes sobre seguridad (Johri & Kumar, 2023).

Con el pasar del tiempo, se han estado actualizando las maneras de acceder a información o datos personales vulnerando la privacidad de los usuarios, por lo que es indispensable que todo usuario comprenda la magnitud de peligro que existe ahora comparado a años anteriores donde los usuarios solo identificaban la dirección de la página, y tomar nuevos criterios de verificación para detectar sitios web malicioso. (Carlos Vilchez, Cecilia, & Burgos, s. f.,2022)

Los gastos implementados para actualizar la tecnología por parte de las empresas bancarios son necesarios por el hecho de que ahora la humanidad está en constante interacción con la tecnología. Estas empresas requieren invertir en digitalización de los servicios financieros para buscar la mayor comodidad para el usuario, lo que a su vez genera mayores gastos en Cibertec ya que al estar vinculados a la tecnología corren el riesgo de sufrir violaciones informáticas. Y en muchas ocasiones, esos gastos no suelen ser rentables, pero se realiza continuamente para mostrar estabilidad en la administración de las cuentas de los usuarios.
Por otra parte, encontramos como medida de contraataque o defensa el uso de nuevas tecnologías como seria el Blockchain, la cual es utilizada en las criptomonedas y vienen siendo implementadas en algunas entidades financieras en los últimos años. (Uddin et al., 2020)

La implementación del blockchain ayuda a la integridad y seguridad de procesos de transacción en los bancos, manteniendo un equilibrio de satisfacción entre la empresa y los clientes; dejando de lado el proceso tradicional al momento de realizar un cambio de moneda o utilizar la moneda local según la comodidad del usuario para realizar una compra desde su banca móvil siendo un proceso de manera inmediata. (Fu et al., 2021)

El blockchain es una tecnología que ofrece sostenibilidad a las empresas del sector bancario. Así, las empresas financieras consolidan con cada usuario una relación de credibilidad, exhibiendo congruentemente los beneficios indicados en cada transacción asegurando autenticidad y reduciendo el riesgo de fraudes. Por lo que representa un cambio significativo en diversos sectores para un proceso más seguro interactuando con el cliente. (Fu et al., 2021)

Los múltiples ataques cibernéticos que suelen ocurrir en bancos crecen de manera exponencial y estar en la posibilidad de que información importante por parte de los clientes y de los bancos se encuentre en manos equivocadas resulta ser peligroso en todo los sentidos y ninguna empresa escapa de ello. Por lo que muchas entidades del sistema financiero están en contacto frecuente para compartir información importante de posibles ataques cibernéticos y ataques ocurridos para salvaguardar información que aún no se haya robado, y que las demás entidades ya pueden realizar un plan de contingencia de ciberseguridad y mostrar experiencia única en seguridad a cada cliente. Es fundamental también que el cliente siempre considere por más segura que sean la red y protección de datos, pueden llegar a ser víctimas de robo de información de sus cuentas ya sea por correos electrónicos o sitios web falsos. De esta manera se comprende que es importante la educación en usuarios del manejo de sus cuentas y generar la concientización, mejorando el nivel de satisfacción en cada uno de ellos. (Lavanya & Dunstan Rajkumar, 2024)

En países donde la tecnología ha logrado un crecimiento significativo, se dispone que cada empresa financiera por ley debe contemplar 4 áreas que prioricen la integridad de sus clientes a pesar de realizar grandes gastos operativos: (i) salvaguardia del consumidor, (ii) confidencialidad y seguridad de la información, (iii) operaciones digitales, y (iv) prevención de delitos informáticos. Por lo tanto, gestionan un servicio digital avanzado y un ambiente favorable para el cliente. (Uddin et al., 2023)

4. DISCUSIÓN

La presente revisión sistemática nos permite dar en cuenta que la implementación de la ciberseguridad en las entidades bancarias por más que demande grandes costos operativos siempre se buscará priorizar la seguridad de la información del cliente generando confianza en cada uno de ellos y por ende calidad al momento de ofrecer servicios colocándolas un escalón por encima de sus competencias , adicional a la gestión de los posibles riesgos que puede sufrir una empresa también es importante la concientización de los clientes del manejo de su información personal; es por ello que la continua formación ,capacitación y desarrollo, junto con el respaldo técnico del banco, incrementarían considerablemente su satisfacción con respecto a la ciberseguridad. (Johri & Kumar, 2023).

Además, la gestión aplicada para mantener activos los protocolos y mantener la ejecución de transacciones seguras para los usuarios respalda el buen servicio de atención brindado a cada uno de los individuos, incrementando de esta manera la afluencia de un mayor número de clientes a las empresas bancarias.

5. CONCLUSIÓN

El desarrollo de la revisión de múltiple literatura nos permitió comprender la magnitud de la importancia de la ciberseguridad en los últimos tiempos donde la era de la digitalización y del internet capturo los datos de muchos clientes, en especial la de los usuarios dentro del sistema financiero.

Cabe mencionar que a pesar del costo adicional que supone implementar planes de seguridad, son las entidades financieras las que tienen prioridad ejecutarlas debido a la magnitud de datos masivos de clientes, desde datos personales, fotos, correos, hasta la suma de activos de estos; además del grave impacto que implicaría que toda esa información personal sea eliminada o adulterada.

Tres bases de datos fueron las responsables de brindarnos las literaturas a revisar: Scopus, Google Académico y PubMed, cuyo filtro que hayan sido publicadas en los últimos 6 años.

El mayor número de publicaciones seleccionadas por país lo obtuvo La India, con 4 artículos.

Es importante mencionar que al momento de la búsqueda muchas literaturas no fueron de acceso posible ya que se encontraban en calidad de pago lo cual limitó al desarrollo del presente artículo.

Por último, esta revisión podría servir como referencia para otros investigadores en revisiones futuras pudiendo desarrollarse de manera más específicas seleccionando solo bancos de alguna región como podría ser Sudamérica o Europa , u otro tipo de sector el cual este expuesto a ataques y tengan que implementar el sus áreas de TI la ciberseguridad.

6. REFERENCIA BIBLIOGRAFICA

Delgado Fernández, T. (2020). Taxonomía de transformación digital (Vol. 1). https://orcid.org/0000-0002-4323-9674

Lucio-Nieto, T., Palacios, R. C., & Mora-Soto, A. (2012). Hacia una Oficina de Gestión de Servicios en el ámbito de ITIL. Cisco. (2021). What Is Cybersecurity? Recuperado de https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance. Recuperado de https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Deloitte. (2020). Future of Cybersecurity in Financial Services. Recuperado de https://www2.deloitte.com/global/en/pages/financial-services/articles/future-of-cybersecurity-in-financial-services.html

KPMG. (2021). Cyber Security: Financial Services. Recuperado de https://home.kpmg/xx/en/home/industries/financial-services/cyber-security.html

Lucio-Nieto, C., et al. (2012). ITIL: Servicio de TI. Revista de Investigación en Tecnologías de la Información, 19(2), 45-58.

McAfee. (2019). Understanding Social Engineering Attacks. Recuperado de https://www.mcafee.com/blogs/other-blogs/mcafee-labs/understanding-social-engineering-attacks/

PwC. (2020). Global Risk Management Survey. Recuperado de https://www.pwc.com/gx/en/services/advisory/consulting/risk/global-risk-survey.html

Symantec. (2021). What is Malware? Recuperado de https://www.symantec.com/blogs/feature-stories/what-is-malware

Verizon. (2020). Data Breach Investigations Report. Recuperado de https://enterprise.verizon.com/resources/reports/dbir/

BCG. (2019). The Digital Transformation of Banking. Recuperado de https://www.bcg.com/publications/2019/digital-transformation-banking

Tejada-Escobar, F., Murrieta-Marcillo, R., Villao-Santos, F., & Garzón-Balcázar, J. (2018). Big Data en la Educación: Beneficios e Impacto de la Analítica de Datos. Revista Científica y Tecnológica UPSE, 5(2), 80–88. https://doi.org/10.26423/rctu.v5i2.424

Sheila, M., Leguizamón, M., & Villanueva, M. M. (2015). EL PHISHING TRABAJO FINAL DE GRADO. GRADO EN CRIMINOLOGÍA Y SEGURIDAD.

Monje, G., & Alexander, R. (2017). SEGURIDAD INFORMÁTICA Y EL MALWARE.

Armando, L., Páez, G., Emiro, J., Arenas, T., Natalia, A., & Moreno, B. (2019). CIBERSEGURIDAD Y ETHICAL HACKING: LA IMPORTANCIA DE PROTEGER LOS DATOS DEL USUARIO.

Kitchenham B., & Charters S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J. A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J. J., Devereaux, P. J., Dickersin, K., Egger, M., Ernst, E., ... Tugwell, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement (Chinese edition). Journal of integrative medicine, 7(9), 889-896. https://doi.org/10.3736/jcim20090918

Carlos Vilchez, J., Asesor, V., Cecilia, K., & Burgos, R. (2022). UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO FACULTAD DE INGENIERÍA ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN Ciberseguridad y robo de información: Una revisión sistemática de la literatura. https://orcid.org/0000-0003-3520-5076

Fu, Z., Dong, P., Li, S., & Ju, Y. (2021). An intelligent cross-border transaction system based on consortium blockchain: A case study in shenzhen, China. PLoS ONE, 16(6 June). https://doi.org/10.1371/journal.pone.0252489

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Human Behavior and Emerging Technologies, 2023, 1–10. https://doi.org/10.1155/2023/2103442

Martinez Mesa, O. R., & Martines de la Peña, M. (2022). REGULACIÓN DE LA INNOVACIÓN FINANCIERA TECNOLÓGICA FINTECH EN LA INDUSTRIA BANCARIA COLOMBIANA: DESAFÍOS Y OPORTUNIDADES. AGLALA, 13, 215–237.

Lavanya, B., & Dunstan Rajkumar, A. (2024). Bibliometric insights on mapping the landscape of cybersecurity: Uncovering the research potential in banking industry. En Multidisciplinary Reviews (Vol. 7, Número 6). Malque Publishing. https://doi.org/10.31893/multirev.2024113

Saxena, R., Gayathri, E., & Surya Kumari, L. (2023). Semantic analysis of blockchain intelligence with proposed agenda for future issues. Int J Syst Assur Eng Manag, 14, 34–54.

Tamanna, C., Asmita, C., Shriya, P., Poojan, P., Daxal, P., & Manan, S. (2024). AComprehensiveStudyofArtificial IntelligenceandCybersecurity on Bitcoin, Crypto Currency and Banking System. Annals of Data Science, 11(1), 103–135.

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? International Review of Financial Analysis, 72. https://doi.org/10.1016/j.irfa.2020.101587

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? Technological Forecasting and Social Change, 197. https://doi.org/10.1016/j.techfore.2023.122919