Revista de Investigación Multidisciplinaria

CTSCAFE PARA CIUDADANOS.....

http://www.ctscafe.pe

ISSN 2521-8093

Volumen VII- Nº 20 Julio 2023

http://www.ctscafe.pe

Lima - Perú

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTS CAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VII- N° 20 Julio 2023

ISSN 2521-8093

Gestión de incidentes para la seguridad de la información en una empresa: una revisión sistemática.

Sr. Elvis Steve Ortiz Centurion
Universidad Nacional de Trujillo
Correo Electrónico: T023300220@unitru.edu.pe

Sr. Jack Edinson Portilla Rodriguez
Universidad Nacional de trujillo
Correo Electrónico: T023300220@unitru.edu.pe

Recibido:6 junio 2023
Aceptado: 20 Julio 2023

Resumen: La gestión de incidentes en seguridad de la información se plantea como un conjunto de actividades y procedimientos diseñados para identificar, responder y resolver los incidentes de seguridad que afectan a los sistemas y datos de una organización. Las empresas reconocen la necesidad de implementar una gestión de incidentes eficiente en la seguridad de su información para actuar de manera eficiente frente a cualquier incidente que se presente. El principal objetivo de este artículo de revisión es analizar y brindar una respuesta a la pregunta de investigación planteada que será el objeto de nuestro estudio: ¿Es relevante emplear la gestión de incidentes para asegurar la información en una empresa?

La metodología PRISMA fue empleada en esta revisión sistemática. Gracias a la búsqueda selectiva de información en diferentes bases de datos, se identificaron un total de 89 documentos, de los cuales solo se seleccionaron 16 aplicando los criterios de inclusión y exclusión. En conclusión, se determinó que la gestión de incidentes desempeña un papel crucial para garantizar la seguridad y protección de la información en las empresas, debido a que al implementar esta gestión, las empresas pueden minimizar riesgos, mejorar la capacidad de respuesta ante situaciones críticas y reducir los impactos negativos en la reputación y rentabilidad.

Palabras claves: Gestión de incidentes / Empresas / Seguridad de la información / Incidente en seguridad de la información

Abstract: Information security incident management is considered as a set of activities and procedures designed to identify, respond to, and resolve security incidents that affect an organization's systems and data. Companies recognize the need to implement efficient incident management in the security of their information in order to act efficiently against any incident that arises. The main objective of this review article is to analyze and provide an answer to the research question that will be the object of our study: Is it relevant to use incident management to secure information in a company?

The PRISMA methodology was used in this systematic review. Thanks to the selective search of information in different databases, a total of 89 documents were identified, of which only 16 were selected by applying the inclusion and exclusion criteria. In conclusion, it was determined that incident management plays a crucial role in

guaranteeing the security and protection of information in companies, because by implementing this management, companies can minimize risks, improve response capacity in critical situations and reduce negative impacts on reputation and profitability.

Keywords: Incident management / Companies / Information security / Information security incident

Résumé : La gestion des incidents de sécurité de l'information est considérée comme un ensemble d'activités et de procédures conçues pour identifier, répondre et résoudre les incidents de sécurité qui affectent les systèmes et les données d'une organisation. Les entreprises reconnaissent la nécessité de mettre en œuvre une gestion efficace des incidents dans la sécurité de leurs informations afin d'agir efficacement contre tout incident qui survient. L'objectif principal de cet article de synthèse est d'analyser et d'apporter une réponse à la question de recherche qui fera l'objet de notre étude : Est-il pertinent d'utiliser la gestion des incidents pour sécuriser l'information dans une entreprise ?

La méthodologie PRISMA a été utilisée dans cette revue systématique. Grâce à la recherche sélective d'informations dans différentes bases de données, un total de 89 documents ont été identifiés, dont seulement 16 ont été sélectionnés en appliquant les critères d'inclusion et d'exclusion. En conclusion, il a été déterminé que la gestion des incidents joue un rôle crucial pour garantir la sécurité et la protection des informations dans les entreprises, car en mettant en œuvre cette gestion, les entreprises peuvent minimiser les risques, améliorer la capacité de réponse dans les situations critiques et réduire les impacts négatifs sur la réputation et la rentabilité.

Mots-clés: Gestion des incidents / Entreprises / Sécurité de l'information / Incident de sécurité de l'information

1. Introducción

Los incidentes en las empresas se refieren a interrupciones en los servicios que pueden tener un impacto negativo en la productividad y el rendimiento de la organización. Con el fin de abordar estas interrupciones de manera eficiente y organizada, las empresas han desarrollado el campo de la gestión de incidencias. Esta práctica permite atender, manejar y resolver rápidamente dichos incidentes, con el objetivo de minimizar su impacto en los servicios que la empresa proporciona. (Sánchez & Valles,2021).

Debido a ello la seguridad de la información se ha convertido en un tema crítico en la actualidad, y las empresas no están exentas de ello. Estas a menudo enfrentan riesgos como la pérdida de datos, el robo de información y los ciberataques, lo que puede tener un gran impacto en su reputación y rentabilidad. Por esta razón, es fundamental tener una gestión efectiva de incidentes de seguridad de la información.

Sin embargo, muchas empresas carecen de estrategias efectivas de gestión de incidentes, lo que las hace más vulnerables a sufrir pérdidas financieras y de reputación. Por lo tanto, el objetivo principal de esta investigación es evaluar la gestión de incidentes en seguridad de la información en las empresas, para así determinar si estas estrategias están siendo

implementadas adecuadamente y si son beneficiosas para el crecimiento de la empresa. Además, como objetivo secundario, se busca identificar las principales barreras que impiden a las empresas implementar estrategias de gestión de incidentes eficaces.

Es esencial destacar que esta investigación puede ser de gran ayuda para las empresas, ya que les permitirá comprender la importancia de implementar estrategias de gestión de incidentes de seguridad de la información efectivas y las medidas necesarias para lograrlo.

2. Material y métodos

Para el desarrollo de la revisión sistemática se utilizó la metodología PRISMA, principalmente la declaración publicada en el año 2020, que es una guía actualizada para la publicación de revisiones sistemáticas, resumida y descrita por Bravo (2020).

La pregunta de investigación en la que se basó el proceso metodológico es la siguiente: ¿Es importante emplear la gestión de incidentes para la seguridad de la información en una empresa?

La metodología PRISMA 2020, según indica Bravo (2020), se ha establecido como un estándar de referencia para la presentación de revisiones sistemáticas y meta análisis en varios campos, incluyendo la investigación en salud, la tecnología, la educación y la psicología, cuyo principal objetivo es asegurar la transparencia en la recopilación y evaluación de la evidencia científica.

De acuerdo con (Barquero, 2022) esta metodología, se compone de una estructura de 27 ítems que se dividen en diferentes secciones como: El título, resumen, introducción, métodos, resultados, discusión, declaración de conflictos de interés, y referencias bibliográficas.

Cada uno de estos ítems cumple una función específica en la presentación de una revisión sistemática y es necesario incluirlos para asegurar la calidad y la transparencia de la revisión

Para iniciar con el proceso de investigación relacionada con nuestra pregunta de investigación, se emplearon términos específicos en la búsqueda selectiva, tales como "companies", "incident management", "information security" y "prisma".

Las bases de datos seleccionadas para la obtención de artículos fueron: Scopus, Dialnet, Redalyc, Google Scholar y Base. Las cuales fueron seleccionadas debido a su prestigio en el ámbito académico y la riqueza del contenido implícito que pueden proporcionar para enriquecer nuestra investigación. Asimismo, se empleó gestores de referencias bibliográficas como Mendeley y IEEE Xplore para obtener las fuentes bibliográficas.

En la tabla 01 se muestran las bases de datos y sus respectivas cadenas de búsqueda y/o palabras clave empleadas, para la selección de los artículos.

Tabla N°1: Bases de datos consultadas y su respectivo término de búsqueda.

Base de Datos	Término de búsqueda.
Base	information security, Incident management year: [2019 TO 2022]
Dialnet	Incident management, companies technology, language: [Español,Inglés y Portugués], year:[2019 A 2022],issue:[Technology y engineer]
Google Scholar	management of incidents in companies, information systems in companies year:[2019 TO 2022], kind of:[review articles],
Redalyc	Incident management, information systems, companies,], issue: [Technology y engineer], pag[10-20]
Scopus	(TITLE-ABS-KEY (incident AND management) AND TITLE-ABS-KEY (information AND security) AND TITLE-ABS-KEY (it))

Fuente: Elaboración propia.

En resumen, se efectuó un procedimiento de selección riguroso y metódico para obtener el contenido pertinente para el despliegue de la investigación, utilizando una variedad de fuentes confiables y enfatizando en las cadenas de búsqueda clave para poder profundizar en los aspectos más relevantes del tema de estudio.

Toda información se recopiló teniendo en cuenta los siguientes criterios de inclusión y exclusión que se detallan en la tabla 02.

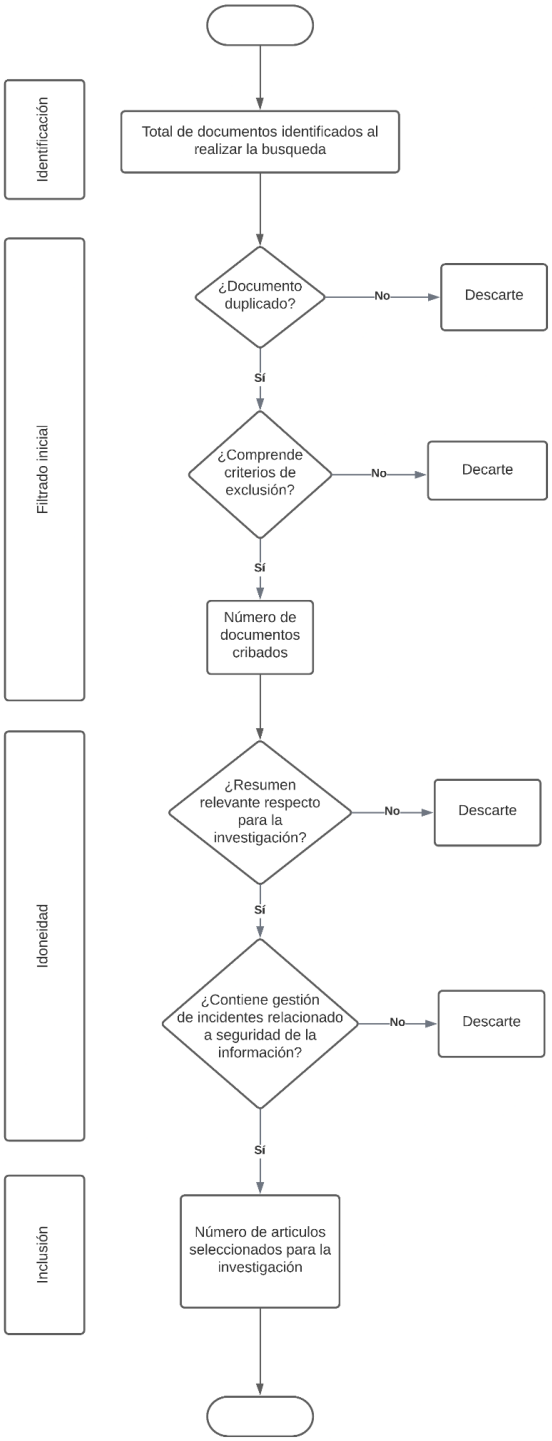
Tabla Nº2: Criterios de inclusión y exclusión

Criterios de inclusión	Descripción.
Ligado a tecnologías de la información.	Cualquier concepto, práctica o proceso que esté vinculado con el uso de tecnologías de la información.
Seguridad de la información	Este término se centra específicamente en la seguridad de la información en el ámbito TIC.
Documento de libre acceso.	Para poder visualizar el contenido.
Criterios de exclusión	Descripción
Desde 2019 a 2022.	Publicaciones que no comprendan los años desde 2019 a 2022.
Relacionado con el tema sanitario.	Tema, información, evento o situación que tenga una conexión directa o indirecta con la salud, bienestar o cuidado médico de las personas
Relacionado a seguridad vial.	Información que se centra en la prevención de incidentes de tránsito, o para la ayuda de una correcta seguridad vial.
Seguridad de hardware y software	Seguridad del hardware y software pueden incluir la instalación de cortafuegos, programas antivirus, el cifrado de datos y la autenticación de usuarios.

Fuente: Elaboración propia.

El desglose completo se muestra en la siguiente figura 01, en la que se detallan los procesos seguidos, hasta llegar a la selección del documento.

Figura N°1: Flujograma empleando Metodología PRISMA



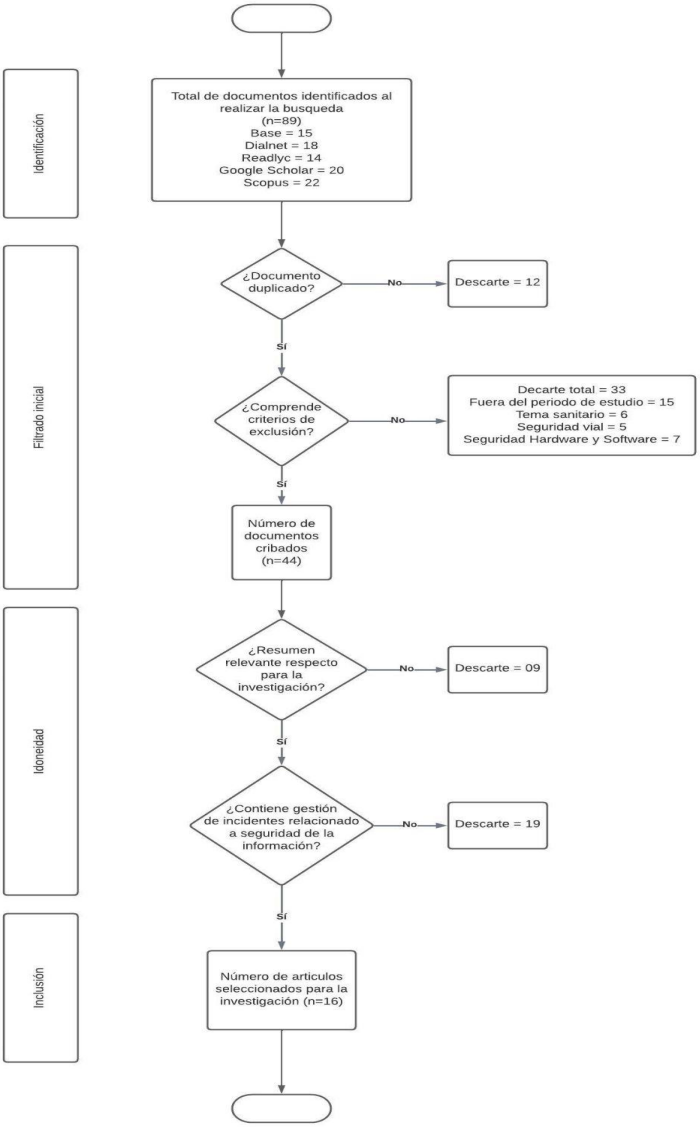
Fuente: Elaboración propia.

3. Resultados

Al buscar artículos en las distintas bases de datos mencionadas se registró un total de 89 artículos, desplegados de la siguiente manera: 20 en Google Scholar, por otro lado, en Scopus, 22, en cambio en Dialnet, 18, por el contrario, en Base, 15, no obstante, en Redalyc, 14. A partir de este número total, se eliminaron los artículos que no se encontraban en el periodo de 5 años desde 2019 a 2022 y tomando en cuenta los criterios de exclusión, dejando un valor final de 44. Posteriormente, de los 44 artículos remanentes se descartaron un total de 9, pues el resumen no mostraba relevancia para la investigación. Consecuentemente se descartaron 18 artículos tras leer el artículo, pues no incluían los criterios de inclusión establecidos.

Finalmente, el abanico de artículos quedó conformado por 16 artículos tal como se muestra en la figura 02:

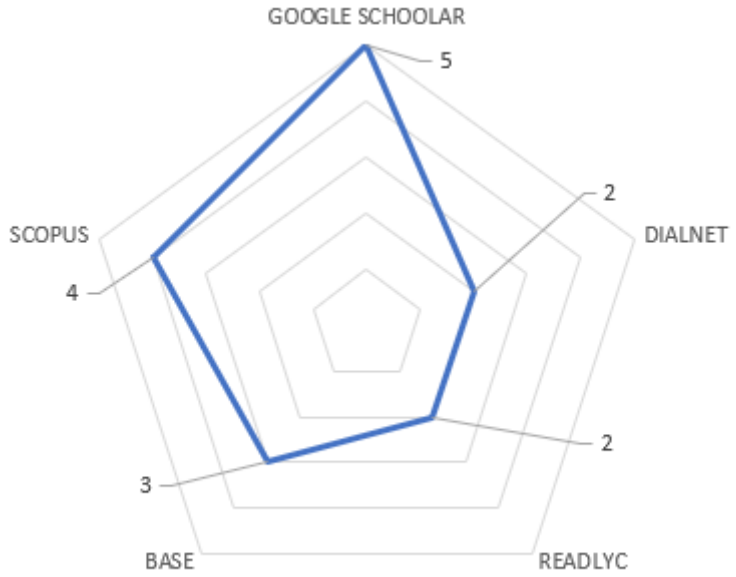
Figura N°2: Proceso de selección de artículos.



Fuente: Elaboración propia.

En adición luego de comprender las acciones que se desarrollaron en la investigación y de la depuración de artículos los cuales fueron descartados de acuerdo a los criterios de inclusión y exclusión se representa en la figura 03 el número total de documentos de información recogidos de cada base de datos seleccionadas anteriormente.

Figura N°3: Artículos seleccionador por base de datos



Fuente: Elaboración propia

La tabla 03 se exhibe los 16 artículos descubiertos que presentan información de autor, título, año y país.

Tabla N°3: Resultados de la búsqueda

N°	Autor	Título de investigación	Año	País
1	Morné Pretorius, Hombakazi Ngejane	Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)	2019	South África
2	R. Eswaran, G. Vinayagamoorthi	Cyber security and information security	2019	India
3	Fayzullajon Bakhtiyorovich Botirov, Sharifjon Rakhimovich Gafurov, Azam Anvorovich Gafurov	Identification of key persons in the information security incident and incident management process and the process and distribution of roles between them.	2021	República de Uzbekistán
4	Marastika Wicaksono Aji Bawono, Mohammad			

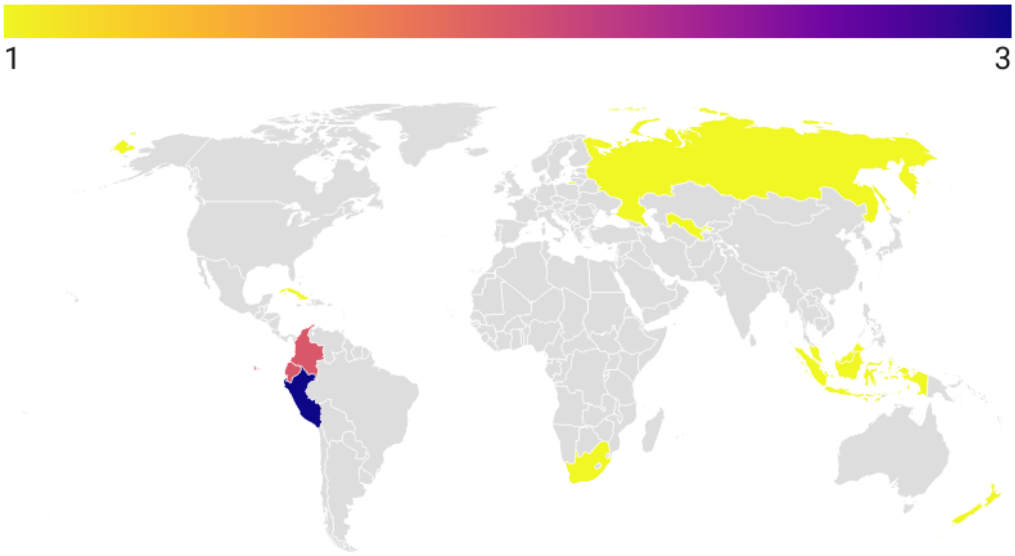
	Amin Soetomo, Thata Apriatin, Marastika Wicaksono, Aji Bawono, Mohammad Amin Soetomo, Eghbal Ghazizadeh, Moonjee Jeong, Juan Pablo JP Angel, Yehan Que.	IT Service Management and Incident Management: Literature Review and a Case Study	2019	Nueva Zelanda
5	Johan Reimon Batmetan, Julita Mamonto, Ronaldo Muyu, Christy Poluakan, Fabiola Natasya Wauran.	Evaluation of Incident Management in University using IT Infrastructure Library Framework	2022	Indonesia
6	María Elena Tasa Catanzaro, Henry George Maquera Quispe, John Fredy Rojas Bujaico, Marjorie Gabriela del Carmen Delgado Rospiglios.	Análisis de información de la gestión de incidentes de seguridad en organizaciones	2021	Perú
7	Yeny Yovana Segura Mancipe.	El contexto de la gestión de incidentes de seguridad de la información.	2018	Colombia
8	Oleg Nikiforov, L. R. Mukhametova.	Key aspects of implementing the Help Desk system in an educational institution	2020	Rusia
9	Perez Izquierdo, Torres Vivanco & Marques Dennis	Sistema informático para la gestión de incidencias del ministerio de comercio exterior	2021	Cuba
10	Sánchez Casanova & Valles Cora	Influencia de ITIL V3 en la gestión de incidencias de una municipalidad peruana	2021	Perú
11	García, J. A., & Gómez, J. M.	Gestión de la seguridad en entornos IoT: una revisión sistemática	2020	Ecuador
12	Awais, M., Asif, M., Nawaz, M. S., & Shahzad, M.	Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review to Identify the Transformation Process from Non-Compliance to Compliance Behavior. Applied Sciences	2021	Malasia
13	Vegas, N. , & Soto, A	La eficiencia de la gestión de incidencias en Cloud Services	2022	Perú
14	Penagos Montoya, J. A., Rentería Gil, K. K., Ibarguen Mena, Y., García Pineda, V., & Castro Ramírez, F	Implementación de políticas de seguridad en el sistema de información de la empresa Funtraev	2021	Colombia
15	Medina, P, Chango, N, Corella, M, & Guisado, D	Transformación digital en las empresas: una revisión conceptual	2022	Ecuador
16	Tasa Catanzaro, Rojas Bujaico, Maquera Quispe, Carmen delgado	Análisis de información de la gestión de incidentes de seguridad en organizaciones	2022	Perú

Fuente: Elaboración propia.

Adicionalmente se tomó en cuenta la procedencia de los artículos seleccionados, los cuales provenían de países como South África, India, República de Uzbekistán, Nueva Zelanda, Indonesia, Perú, Colombia, Rusia, Cuba, Ecuador y Malasia para la obtención de material relevante en la investigación.

La selección de estos artículos se realizó con el objetivo de obtener una muestra representativa y diversa de la información disponible en el tema de interés. Consecuentemente con el propósito de mostrar la ubicación de los países que publican las referencias utilizadas y las fuentes que indicaron dichas publicaciones en la figura 04 se muestra la ubicación de dichos países mencionados.

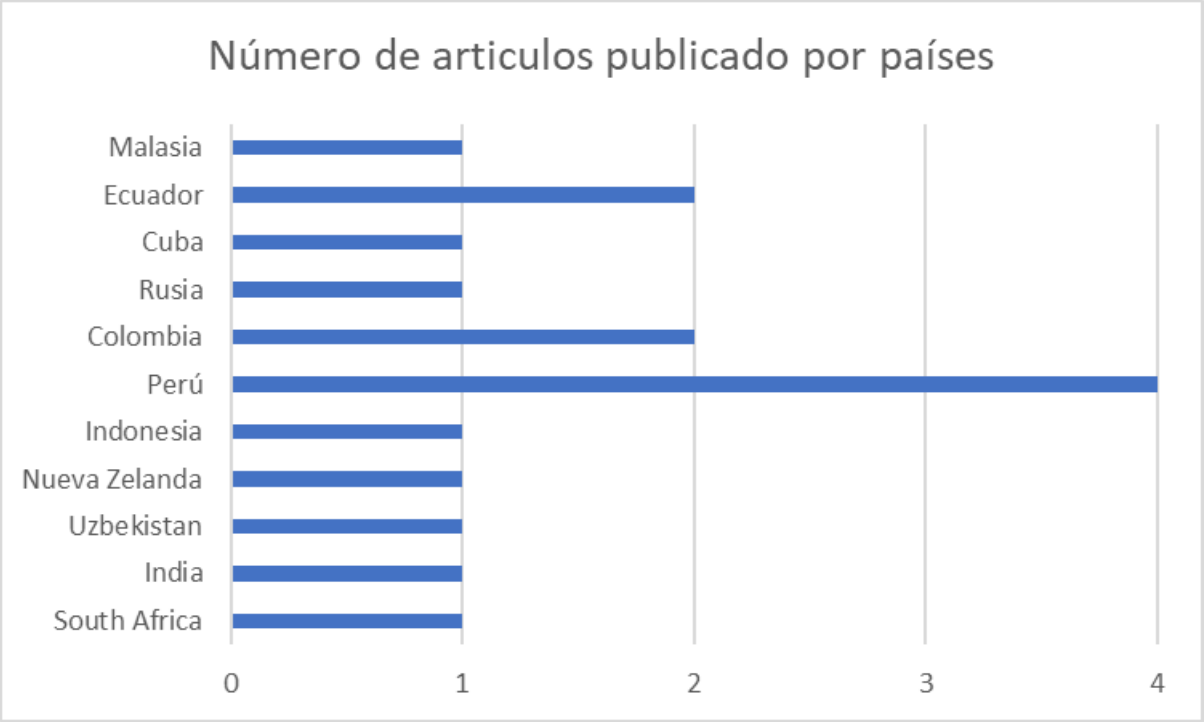
Figura N°4: Ubicación de países de los artículos seleccionados



Fuente: Elaboración propia

Respecto a los países con mayor presencia de artículos selecciones se encuentra; principalmente Perú con 4 artículos, Colombia y Ecuador con 2 artículos, y otros con 1 artículo, véase la Figura 05.

Figura N °5



Fuente: Elaboración propia.

En general los incidentes surgen a cada instante, pueden ser causados por entidades internas o externas de acuerdo con el contexto en el que se encuentre. Para Sánchez & Valles (2021), los incidentes en las organizaciones no son más que interrupciones en los servicios que pueden afectar a la eficiencia y el rendimiento de la organización.

En este sentido Ghazizadeh, Jeong, Ángel & Que, (2019), mencionan que un incidente se refiere a un informe presentado por un cliente interno o externo acerca de cualquier inconveniente, error o falla que experimenten mientras utilizan un servicio.

Un incidente es una parte importante en una organización, aunque en ocasiones no se percate de esta manera, según Catanzaro, Quispe, Bujaico, & Rospigliosi (2022), estos incidentes proporcionan información valiosa sobre posibles vulnerabilidades y debilidades en los sistemas de seguridad, permitiendo a las organizaciones identificar áreas de mejora y fortalecer sus medidas de protección de manera proactiva.

Con los diversos incidentes que surgen, los cuales afectan la seguridad de la información, es necesario prestar atención a la seguridad de este activo, Faizan Ali (2021), menciona que la seguridad de la información abarca todas las métricas y prácticas que se utilizan para proteger la información esencial de una empresa o entidad, incluyendo su confidencialidad, integridad y disponibilidad. Esto puede incluir medidas técnicas como el cifrado de datos y la autenticación de usuarios, así como políticas y procedimientos para garantizar que los empleados manejen la información de manera segura y responsable.

Complementando Segura (2018), nos indica que un incidente de seguridad de la información es un evento no deseado en seguridad de la información que compromete las actividades del negocio y amenaza la información

Es por ello que la seguridad de la información es independiente al ámbito y contexto en el que se encuentre, afirma Eswaran & Moorthi, (2019). Este mismo autor nos menciona que la seguridad de la información involucra accesos no autorizados, infracciones, con el fin de mantener la privacidad del usuario y/o cliente y la confidencialidad del activo.

Asimismo, el surgimiento de un incidente debe visualizarse como el inicio de un proceso en el cual lo que se busca es la seguridad de la información, tal como dice Catanzaro, Maquera, Quispe, Rojas, Rospigliosi (2022), los incidentes de seguridad en una organización son el paso inicial para una evaluación de los diversos controles de seguridad que puedan existir.

Segura (2018), indica que la norma ISO/IEC 27035 otorga a las organizaciones un enfoque estructurado el que comprende: Detectar incidentes de seguridad - responder a los incidentes - evaluar posibles vulnerabilidades - mejorar la seguridad de información.

Cuando se vulnera la seguridad de la información, las empresas pueden enfrentar riesgos extensos y variables que pueden dañar sus ingresos y su reputación. Las violaciones de datos pueden resultar en la pérdida o el robo de información confidencial, lo que puede tener un impacto negativo en la confianza del cliente y en la imagen pública de la empresa. Además, las investigaciones muestran que alrededor del 70% de los incidentes ocurrieron debido a negligencia humana (intencional o no), lo que significa que los empleados pueden ser una fuente importante de vulnerabilidades en la seguridad de la información (Faizan Ali et al., 2021)

Asimismo, como se encuentran incidentes en la seguridad de la información, encontramos vulnerabilidades, las cuales se detallan en la tabla 04:

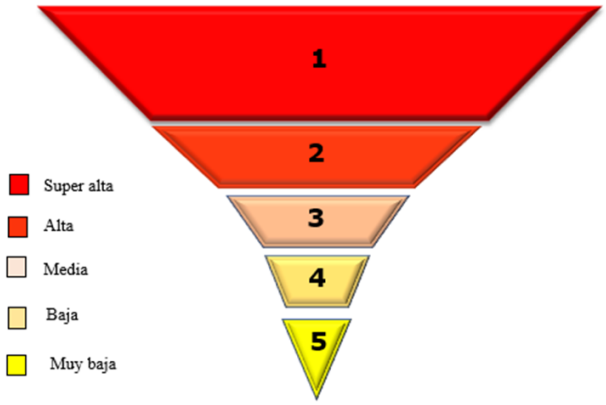
Tabla N°4: Vulnerabilidades en una empresa

N.º	Vulnerabilidades
1	Uso inadecuado o negligente por parte del personal.
2	La exposición a ataques externos
3	Falta de autenticación y autorización adecuadas
4	La falta de actualizaciones y parches de seguridad
5	El robo o pérdida de dispositivos móviles

Fuente: García & Gómez. (2022). Gestión de la seguridad en entornos IoT: una revisión sistemática

Al analizar los resultados que obtuvieron García y Gómez en su artículo "Gestión de la seguridad en entornos IoT: una revisión sistemática", elaboramos el siguiente gráfico de embudo, el cual nos permitirá tener una mayor comprensión del nivel de significancia, se muestra en la figura 06.

Figura N°06: Gráfico de embudo respecto al nivel de riesgo de la vulnerabilidad



Fuente: Elaboración propia

Este mismo autor afirma que para lograr la mejora y reducir sus impactos, las organizaciones deben adoptar un marco de gestión de incidentes en seguridad de la información.
Del mismo modo Batmetan, Mamonto, Muyu, Poluakan, Wauran (2022) indican que la gestión de incidentes es de máxima prioridad en cualquier organización pública o privada, ya que es la principal puerta de enlace entre los servicios de TI y sus usuarios finales previstos.

Para Vegas & Soto, (2022), la gestión de incidentes es un proceso dentro de la gestión de servicios que se enfoca en restaurar el servicio lo más rápido posible después de una interrupción o fallo.

Lo que se busca es reducir dicho impacto que surge una vez sucedido el incidente, afirma Nikiforov & Mukhametova, (2020), el objetivo principal del proceso de gestión de problemas es minimizar el impacto negativo en la actividad principal de la organización de incidentes y problemas que ocurren como resultado de errores en la infraestructura de TI, así como prevenir la recurrencia de incidentes asociados con estos errores.

Por consiguiente, Pretorius & Ngejane (2019), indican que la gestión de incidentes contiene al manejo de incidentes el cual se enfoca en tener una respuesta a los incidentes que se puedan presentar. Este mismo autor, señala que la gestión de incidentes ofrece servicios y apoyo mediante la prevención, detección y respuesta a incidentes de seguridad de la información.

En consonancia, Tasa, Marquera & Rojas (2022), argumentan que existen varias herramientas tecnológicas que se utilizan en la gestión de incidentes en las empresas, la cual les permite tener una mejor eficiencia, dichas tecnologías se detallan en la tabla 05.

Tabla N°5: Tecnologías para la gestión de incidentes en las empresas.

Tecnologías	Función
Sistemas de detección y prevención de intrusiones (IDS/IPS)	Vigilan la red en busca de comportamiento sospechoso.
Firewalls	Barrera entre la red interna y externa
Herramientas de análisis forense	Ayudan a los equipos de respuesta a incidentes a recopilar y analizar datos
Herramientas de gestión de registros	Permiten a las organizaciones registrar y almacenar registros de eventos
Plataformas SIEM	Estas plataformas recopilan y correlaciona datos de múltiples fuentes para detectar patrones sospechosos
Herramientas de gestión de vulnerabilidades	Escanean la red en busca de vulnerabilidades conocidas que podrían ser explotadas por atacantes.
Sistema antivirus	Protegen los sistemas contra malware, virus y otras amenazas conocidas.

Fuente: Tasa, Marquera & Rojas (2022), Análisis de información de la gestión de incidentes de seguridad en organizaciones

A su vez, Pérez, Torres & Marques (2021), señalan que la colaboración y coordinación tanto interna como externa son elementos claves en la gestión de incidentes en seguridad de la información, pues permiten un mejor uso de las herramientas tecnológicas. Estos aspectos aseguran una respuesta efectiva y una resolución adecuada de los incidentes. Este mismo autor sostiene que, las mejores prácticas y estrategias para la gestión de incidentes en seguridad de la información que debe seguir una empresa incluyen:

- Tener un plan de respuesta a incidentes bien definido y documentado.
- Identificar y clasificar los activos críticos de la organización para priorizar la respuesta a incidentes.

- Establecer un equipo de respuesta a incidentes (IRT) con roles y responsabilidades claramente definidos.
- Realizar simulaciones periódicas para probar el plan de respuesta a incidentes y mejorar la capacidad de respuesta del IRT.
- Implementar medidas preventivas, como sistemas de detección de intrusiones, firewalls, antivirus y software de monitoreo de red.
- Establecer procedimientos claros para notificar a las partes interesadas internas y externas sobre los incidentes.
- Llevar a cabo una indagación minuciosa posterior al incidente con el objetivo de identificar las causas fundamentales y adoptar acciones correctivas para prevenir futuros incidentes de índole similar.

En este sentido los altos mandos de la organización pueden percibir la importancia de una correcta gestión de incidentes en seguridad de la información, tal como señala Botirov, Rakhimovich & Anvorovich (2019), la gerencia de una organización logró resaltar la necesidad e importancia de la gestión de incidentes, es por ello que se procedió a identificar a personas clave en el proceso.

Del mismo modo se hace referencia a las personas claves, cuando Pérez, Torres & Marques (2021), indican que la colaboración y coordinación tanto interna como externa son elementos claves en la gestión de incidentes en seguridad de la información, pues permite un mejor uso de las herramientas tecnológicas. Estos aspectos aseguran una respuesta efectiva y una resolución adecuada de los incidentes.

Finalmente, Segura (2018), establece que luego de emplear un enfoque estructurado para la gestión de incidentes en seguridad de la información se obtuvo los siguientes beneficios: Mejora de la seguridad global de la información - Reducción de impactos negativos - Fortalecimiento de evidencia - Mejora en conciencia de seguridad de la información.

4. Discusión

La revisión sistemática nos brinda la oportunidad de profundizar en la comprensión de lo que implica un incidente en particular. En el estudio realizado por Sánchez & Valles (2021), se menciona que un incidente puede surgir tanto de fuentes externas como internas, esta idea se refuerza con más énfasis en la investigación de Ghazizadeh, Jeong, Ángel & Que (2019). Además, Eswaran & Moorthi (2019) aportan una perspectiva sobre la seguridad de la información, la cual se considera independiente del entorno o contexto en el que se desarrolle. En cualquier situación, la seguridad de la información siempre busca proteger los activos.

Por consiguiente se procedió a hablar sobre la seguridad de la información, con el estudio de García & Gómez , 2022 en la figura 6 se presentan las vulnerabilidades más resaltantes que presenta una organización cuando se trata de la seguridad de su información, las cuales agentes externos captan dichas vulnerabilidades y generan incidentes.
Además, se demuestra la estrecha relación entre los incidentes y las vulnerabilidades en la seguridad de la información. Los incidentes proporcionan información valiosa sobre posibles vulnerabilidades y debilidades en los sistemas de seguridad, permitiendo a las organizaciones identificar áreas de mejora y fortalecer sus medidas de protección, según

Catanzaro, Quispe, Bujaico & Rospigliosi (2022). Esta conexión enfatiza la importancia de la gestión de incidentes como una forma de identificar y abordar las vulnerabilidades existentes.

Se mencionan diversas buenas prácticas y estrategias para la gestión de incidentes en seguridad de la información. Estas incluyen tener un plan de respuesta a incidentes bien definidos y documentados, identificar y clasificar activos críticos, establecer un equipo de respuesta a incidentes con roles claros, realizar simulaciones periódicas, implementar medidas preventivas y establecer procedimientos claros de notificación y seguimiento, como señala Pérez, Torres & Marques (2021). Estas prácticas destacan la importancia de una planificación y preparación adecuadas.

5. Conclusiones

La gestión de incidentes se plantea como un conjunto de actividades y procedimientos diseñados para detectar, responder y resolver los incidentes de seguridad que afectan a los sistemas y datos de una organización. Las empresas tienen la necesidad de implementar gestión de incidentes en la seguridad de su información para responder de manera asertiva ante cualquier incidente.

En conclusión, se puede afirmar que la gestión de incidentes es de vital importancia para garantizar la seguridad y protección de la información en las empresas, puesto que ayuda a minimizar los riesgos, mejorar la capacidad de respuesta ante situaciones críticas y reducir en general todos los impactos negativos que pueden tener estos incidentes en la reputación y rentabilidad de la empresa.

Esta revisión sistemática representa un valioso recurso para aquellos interesados en profundizar en el campo de la gestión de riesgos en seguridad de la información. A través de la exploración de diversos conceptos, se espera que los futuros estudios y trabajos de investigación puedan construir sobre esta base y generar un mayor entendimiento en el ámbito de la gestión de riesgos en la seguridad de la información y su impacto en las utilidades de una empresa

6. Literatura citada

Awais, M., Asif, M., Nawaz, M. S., & Shahzad, M. (2021). Information security behavior and information security policy compliance: A systematic literature review to identify the transformation process from non-compliance to compliance behavior. Applied sciences, 11(8), 3383-3400. https://doi.org/10.3390/app11083383

Barquero Morales, W. G. (2022). Análisis de PRISMA como metodología para revisión sistemática: una aproximación general. Saúde Em Redes, 8(sup1), 339–360. https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Bravo T.R. (2020). La declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Sceciendiret, 7(2), 14. https://www.sciencedirect.com/science/article/pii/S0300893221002748

Botirov, F., Gafurov, S., & Gafurov, A. (2021). Identification of key persons in the information security inciden y incident management process and t process and distribution of roles between them. Technical science and innovation, 2021(3), 72–77. https://doi.org/10.51346/tstu-02.21.3-77-0023

Eswaran, R., & Vinayagamoorthi, G. (2019). Cyber security and information security. International Journal of Recent Technology and Engineering, 8(3 Special Issue), 372–374. https://doi.org/10.35940/ijrte.C1079.1083S19

García, J. A., & Gómez, J. M. (2020). Gestión de la seguridad en entornos IoT: una revisión sistemática. Revista Ingenio, 17(1), 56-64. ISSN 2011-642X / E-ISSN 2389-864X.

Nikiforov, O., & Mukhametova, L. R. (2020). Key aspects of implementing the help desk system in an educational institution. In ACM International Conference Proceeding Series. Association for Computing Machinery. https://doi.org/10.1145/3388984.3390876Barquero Morales, W. G. (2022). Análisis de Prisma como metodología para revisión sistemática: una aproximación general. Saúde Em Redes, 8(sup1), 339–360. https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Medina Chicaiza, P., Chango Guanoluisa, M., Corella Cobos, M., & Guizado Toscano, D. (2022). Transformación digital en las empresas: una revisión conceptual [Digital transformation in companies: a conceptual review]. Journal of Science and Research, 7(CININGEC II), 756-759. https://doi.org/10.5281/zenodo.7726439

Penagos Montoya, J. A., Rentería Gil, K. K., Ibarguen Mena, Y., García Pineda, V., & Castro Ramírez, F. (2021). Implementación de políticas de seguridad en el sistema de información de la empresa Funtraev [Implementation of security policies in the information system of the company Funtraev]. ICT Innovations and Societal Changes, 9(2), 189-200. https://doi.org/10.26495/icti.v9i2.2271

Perez Izquierdo J, Torres Vivanco A & Marques Dennis C (2021). Sistema informático para la gestión de incidencias del ministerio de comercio exterior. Redalyc , 8 (3), 14 . https://dialnet.unirioja.es/servlet/articulo?codigo=8590464

Pretorius, M., & Ngejane, H. (2019). Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC). The African Journal of Information and Communication (AJIC), (24). https://doi.org/10.23962/10539/28656

Reimon Batmetan, J., Mamonto, J., Muyu, R., Poluakan, C., & Wauran, F. N. (2022). Evaluation of incident management in university using it infrastructure library framework. International Journal of Information Technology and Education, 1(2), 103–108. Retrieved from https://www.neliti.com/publications/410927/

Sánchez Casanova, F. S., & Valles Coral, M. Á. (2021). Influencia de ITIL V3 en la gestión de incidencias de una municipalidad peruana [Influence of ITIL V3 in incident management of a peruvian municipality]. Revista Cubana de Ciencias Informáticas, 15(3), 1-19. Disponible en: https://www.redalyc.org/articulo.oa?id=378369292001

Tasa Catanzaro, M. E., Maquera Quispe, H. G., Rojas Bujaico, J. F., & Delgado Rospigliosi, M. G. del C. (2022). Análisis de información de la gestión de incidentes de seguridad en organizaciones. Puriq, 4, e196. https://doi.org/10.37073/puriq.4.1.196

Vegas, N. , & Soto, A. (2022). La eficiencia de la gestión de incidencias en Cloud Services. Campus, XXVII(34), 197-208. https://doi.org/10.24265/campus.2022.v27n34.03

Wicaksono Aji Bawono, M., Amin Soetomo, M., Apriatin, T., Wicaksono, M., Bawono, A., Soetomo, M. A., … Que, Y. (2019). IT Service management and incident management: Literature review and a case study. Management and information technology, 2020. Retrieved from https://acis2019.io/pdfs/ACIS2019_PaperFIN_067.pdf

Yovana, Y. (2018). Contexto de la gestión de incidentes de seguridad de la información. Universidad Piloto de Colombia, 11. Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8597/Contexto de la gestion de incidentes de seguridad de la informacion.pdf?sequence=1&isAllowed=y

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTSCAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VII- N° 20 Julio 2023

Contáctenos en nuestro correo electrónico
revistactscafe@ctscafe.pe

Página Web:
http://ctscafe.pe

Blog:
https://ctscafeparaciudadanos.blogspot.com/

Facebook
https://www.facebook.com/Revista-CTSCafe-1822923591364746/

latindex