zRevista Científica Ciencias Ingenieriles

(2024) Vol. 4, Núm. 1, pp. 79 – 90

https://doi.org/10.54943/ricci.v4i1.384

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

ARTÍCULO DE REVISIÓN

Mecanismos de seguridad de la información en una organización: una revisión sistemática.

Information Security Mechanisms in an Organisation: A Systematic Review.

• Julio Marreros [1] • Diego Acosta [2] • Alberto Mendoza [3]

[1] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t043300520@unitru.edu.pe
ORCID: https://orcid.org/0009-0009-8767-4633
[2] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t023300620@unitru.edu.pe
ORCID: https://orcid.org/0009-0002-1031-7098
[3] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: amendozad@unitru.edu.pe
ORCID: https://orcid.org/0000-0002-0469-915X

Recibido: 09 octubre del 2023 / **Revisado**: 05 noviembre del 2023 / **Aprobado:** 07 diciembre del 2023 / **Publicado:** 22 de enero del 2024

RESUMEN

La información es necesaria en las empresas para el desarrollo de las estrategias organizacionales con bases sólidas, cualquier brecha de seguridad puede comprometer los datos sensibles de la organización y perjudicar gravemente a la misma. Partiendo de aquello, se hizo una revisión sistemática con el objetivo de señalar aquellos mecanismos desarrollados para la protección de la seguridad de la información organizacional que son de gran utilidad con en un contexto donde las herramientas digitales van tomando mayor presencia al almacenar información sensible, así mismo clasificar estos mecanismos en base al activo de información a proteger. Para la búsqueda de documentos se hizo uso de la metodología PRISMA y se tomaron en cuenta investigaciones publicadas en base de datos como: Scopus, Dialnet, SciELO. Se aplicaron criterios de exclusión e inclusión que redujeron los resultados a 19 artículos que serán herramienta de análisis. Al interpretar resultados se observó que hay mecanismos que al aplicarse no solo cumplen con fortalecer un aspecto de la organización, sino que también guardan relación con otros mecanismos. Para finalizar se identificaron estos resultados dentro de 3 capas correspondientes al software, hardware y capital humano de las organizaciones.

Palabras clave: Robo de datos; privacidad de información; protección en empresas; encriptación; políticas de seguridad.

ABSTRACT

Information is necessary in companies for the development of organisational strategies with solid foundations; any security breach can compromise the organisation's sensitive data and seriously damage it. Based on this, a systematic review has been carried out with the aim of pointing out those mechanisms developed for the protection of organisational information security that are very useful in a context in which digital tools are increasingly present when storing sensitive information, as well as classifying these mechanisms according to the information asset to be protected. The PRISMA methodology was used for the documentary search and research published in databases such as Scopus, Dialnet and SciELO was taken into account. Exclusion and inclusion criteria were applied, which reduced the results to 19 articles that will be used as an analysis tool. When interpreting the results, it was observed that there are mechanisms that, when applied, not only strengthen one aspect of the organisation, but also relate to other mechanisms. Finally, these results were identified within 3 layers corresponding to software, hardware and human capital of the organisations.

Keywords: Data theft; information privacy; enterprise protection; encryption; security policies

1. INTRODUCCIÓN

La seguridad de la información es fundamental en el funcionamiento de cualquier organización en la era digital actual. Consiste en la implementación de medidas y procedimientos diseñados para proteger la confidencialidad, integridad y también la disponibilidad de los datos. Según Svintsytskyi y Fernandez (2022) indica que el avance de las tecnologías digitales ha llevado al aumento de los ciberataques y al desarrollo de métodos para interferir en los sistemas de información automatizados.

La realidad problemática de esta revisión señala el hecho de conocer aquellas técnicas más útiles que hacen frente a las amenazas relacionadas a la filtración de información en las organizaciones. Rodriguez et al. (2020) indica que la información es clave en el entorno empresarial actual, donde la gestión adecuada de los datos y la protección de la información confidencial son imperativos para el éxito de las organizaciones; caso contrario, se tendrían graves consecuencias debido a la naturaleza de las propias organizaciones: cuentan con una basta cantidad de datos de diferentes dimensiones, por ejemplo: clientes, productos, ventas, socios; y cualquier brecha de seguridad no solo filtraría información propia de las transacciones de la empresa sino que también compromete a las personas ajenas que son parte de dichas transacciones, lo cual desemboca en diferentes problemas ya que, como menciona Cumbreras (2020), la ausencia de medidas de seguridad (o la implementación de medidas no adecuadas) puede ser motivo de sanción a la empresa al violar la confidencialidad de los afectados.

Otro aspecto importante es la diferenciación establecida por Rodriguez et al. (2020) al mencionar que "la información física y digital desempeña un rol importante" (p. 3). Como establece Ordóñez (2020), el principal padecimiento de la información digital se debe al desarrollo de nuevas tecnologías que cada vez más es adoptado por los negocios con la finalidad de acelerar los procesos gracias a la globalización; sin embargo, esta aceptación rápida genera desorden y muchas veces se pasa por alto las amenazas a la información que existen en estas innovaciones. Por otro lado, la información física abordaría los documentos archivados y hardware; los cuales, por su naturaleza, involucran otro tipo de mecanismos de protección diferentes a las técnicas digitales de resguardo de datos.

Gené et al. (2018) indican que estos mecanismos ayudan a proteger la privacidad de la información sensible, evitando que personas no autorizadas accedan, modifiquen o divulguen dicha información. Todo esto evidencia la importancia de proteger la información debido a la multiplicidad de amenazas y consecuencias negativas que afectan a las empresas, lo que lleva a plantearse la siguiente interrogante: ¿cuáles son los mecanismos desarrollados para protección de la seguridad de la información organizacional? En este artículo se abordará dicha problemática con la finalidad de señalar las mejores prácticas que hacen frente a las brechas de seguridad existentes y cómo se clasifican dependiendo del activo de información involucrado.

Rodriguez et al. (2020) se hace mención a la restricción de acceso a la información (privilegios mínimos) dependiendo de las necesidades del personal, es decir, establecer roles o perfiles de seguridad. Un punto importante de este mecanismo es el cuidado que se le debe dar a las credenciales de los usuarios ya que la filtración de esto por parte de los empleados puede desembocar en casos de robo de identidad graves. Si bien el impacto se disminuye al restringir los cambios maliciosos que se puedan realizar por algún agente externo: el peligro es mayor si dicho usuario es de alto rango (aquel que tenga acceso a mayor cantidad de funciones en la empresa). Debido a eso, Garcia y Moreno (2021) señalan la gestión de contraseñas como un complemento de seguridad que se resumen en llevar el mantenimiento de las mismas a través de procesos formales, para su documentación, y una revisión periódica de las credenciales para su renovación. Además, otro método que ayuda a reducir este problema es la autenticación de doble factor señalado por Estrada et al. (2021) el cuál se resumen en usar una clave extra a la contraseña. Este método es muy útil dado que agrega un control más para ingresar al sistema y dificultar el robo de identidad de los empleados porque cuenta con varias opciones de autenticación que, a medida que avanza la tecnología, van aumentado; por ejemplo, los empleados pueden corroborar su identidad a través de un SMS, e-mail, biometría, etc. También es importante señalar el cifrado de datos mencionado por Altamirano de la Borda (2021), que consiste en transformar los datos para que solo sean reconocibles a través de un método de desencriptación conocido por la empresa. Esto funciona como control para complicar la lectura de la información por parte de un agente malicioso y evitar la filtración.

Un apartado importante respecto al software es el tema de las versiones, es de suma importancia mantener el software actualizado para evitar brechas de seguridad (Sánchez et al., 2021). El desarrollo de los programas se ve limitado por la tecnología de su momento; por eso, mientras más conocimiento se vaya adquiriendo, los atacantes

encontrarán la mejor forma de robar información: ya sea a través de nuevos métodos de ataque o la mejora de los programas ya desarrollados. Salvo casos puntuales de compatibilidad que exijan determinada versión de un programa, lo ideal es que las empresas mantengan la buena práctica de mantener actualizado el software propio o ajeno con la finalidad de estar protegidos de las nuevas amenazas; sin embargo, los beneficios no solo se reducen a eso, otros aspectos importantes son las nuevas funciones agregadas o la optimización del software.

Como una medida de seguridad útil tras la brecha de seguridad, tenemos a las copias de seguridad mencionadas por Tonysé (2021) las cuales sirven como respaldo al duplicar la información para su futura consulta o reposición. Es importante señalar que las copias de seguridad no solo se hacen en entornos virtuales, como por ejemplo a una base de datos, sino que también se relaciona a el duplicado de documentos físicos que posteriormente serán archivados. Dado que este mecanismo se basa en almacenar la misma información 2 o más veces, es que se visualiza la necesidad de priorizar los datos que serán duplicados para un mejor uso de los recursos de la organización.

Por otro lado, en el documento de Espinoza (2019) se hace mención al uso de distintas herramientas relacionadas con las brechas al navegar por la red. Esto se fortalece con el resultado obtenido por Morales et al. (2020) que una reducción de tras la aplicación de firewall en una empresa pública. Además con el documento de More et al.(2023) indica que es importante adoptar marcos de trabajo en el entorno de tecnologías de información, así como la construcción de herramientas y sistemas de información para los procesos organizacionales. También se hace referencia que se debe contar con licencias de software válidas y de implementar controles relacionados con la seguridad de los sistemas informáticos.

Respecto a la red de la organización, Chimbo (2023) propone una forma segura de compartir la red corporativa con terceros, a través de una red de invitados, de esta forma los agentes externos a la empresa pueden hacer uso de la red sin poner en grave riesgo la red privada. Sin embargo, Valencia et al. (2018) hacen referencia que es importante tener en cuenta que la seguridad de información en el software no es un proceso único, sino que debe ser considerada a lo largo de todo su ciclo de vida, desde el diseño y desarrollo hasta la implementación y mantenimiento. Además, esto debe ser una preocupación constante, ya que las amenazas y los ataques evolucionan constantemente.

Según Altamirano (2019) menciona que el hardware también juega un papel importante en la protección de los datos almacenados en él. Esto implica el uso de técnicas de encriptación para proteger la confidencialidad de los datos, así como la implementación de copias de seguridad y recuperación de datos en caso de pérdida o daño del hardware. En la investigación de Astudillo y Cabrera (2019) se resalta la importancia de que la construcción del entorno físico donde se almacenará la información sea unas zonas seguras y con su respectivo control de acceso. Esto hace referencia a otro entorno en el cual se manipula la información: el físico; a través de la selección de zonas alejadas o resistentes frente a inundaciones, terremotos, incendios, etc.; se busca proteger, por ejemplo, al centro de procesamiento de datos. Además, Imbaquingo et al. (2020) mencionan que existen diversas amenazas de seguridad de la información relacionadas con el hardware, y para eso es necesario la implementación de un monitoreo continuo. A partir de este punto se puede señalar la importancia no solo de las medidas preventivas digitales, sino de proteger el entorno sobre el cuál se soportan los programas. Asimismo, Tundidor et al. (2019) indican que se debe limitar el acceso físico a los dispositivos y componentes de hardware a personas autorizadas, también realizar copias de seguridad periódicas de los datos almacenados en el hardware. Es importante tener un plan preventivo en caso el hardware sea dañado y se necesite su pronta disponibilidad. Un claro ejemplo de esto último lo tenemos en los niveles RAID, a través de discos de almacenamiento que trabajan en conjunto para recuperar información en caso uno salga dañado.

Por otro lado, encontramos otro enfoque de seguridad respecto al siguiente activo de la organización: las personas. Muñoz (2021) indica como de las funciones relacionadas al apoyo de los directivos a la capacitación del personal. La capacitación de un trabajador nuevo en la empresa es importante porque hace que se familiarice con el entorno al que está ingresando, parte de esta capacitación no debe ser sólo respecto a las prácticas específicas de sus funciones, sino que también sirvan para advertirle de las amenazas que pueden explotar las vulnerabilidades del sistema. De hecho, la capacitación tiene que ser frecuente dado que la tecnología va mejorando y con ello los ataques a la organización (Londoño et al., 2022). Si las personas, al hacer uso del software y hardware, llegasen a cometer cualquier error entonces tendría consecuencias en la empresa, por ejemplo, las filtraciones de información. La información no solo se almacena en la base de datos, sino que también es conocida por los empleados y los hace blancos de ataques. A

menudo las personas pueden ser contactadas a través de distintos medios como el correo electrónico donde a través de mensajes fraudulentos o similares pueden ser engañadas. Parte de la contención de daños ya lo hemos abordado anteriormente: los privilegios mínimos; estos ayudan a que las personas desconocen información sensible y por lo tanto que, en caso filtren información, no resulte en graves consecuencias para la empresa. Aun así, la capacitación sigue siendo un gran aditivo de prevención dado que Milio (2021) señala a las personas como el eslabón más débil de la seguridad de la información y la importancia de contar con personal competente, además, indica que de no capacitar correctamente al personal sería imposible mitigar los riesgos. Asimismo, Guijarro et al. (2018) asegura que las personas que trabajan en las organizaciones deben ser conscientes de la ingeniería social es decir estar alerta ante posibles intentos de engaño o manipulación por parte de personas externas que intentan obtener información confidencial.

2. METODOLOGÍA

Esta revisión fue realizada con ayuda del procedimiento PRISMA, qué es un conjunto de directrices que se utilizan para la realización de revisiones sistemáticas. La interrogante sobre la cual empezó esta investigación es la siguiente: ¿Cuáles son los mecanismos de seguridad de la información que una organización puede utilizar para prevenir amenazas cibernéticas?, Se recopiló un total de 804 artículos científicos, para poder buscar estos artículos utilizamos la siguiente sintaxis de búsqueda: security AND of AND the AND information", "information AND security AND mechanisms", " information security in organizations", "Seguridad de la información en organizaciones", "Mecanismos de seguridad de información", de las siguientes base de datos: Scopus, DialNet, SciELO y Otros.

2.1. Criterios de inclusión y de exclusion

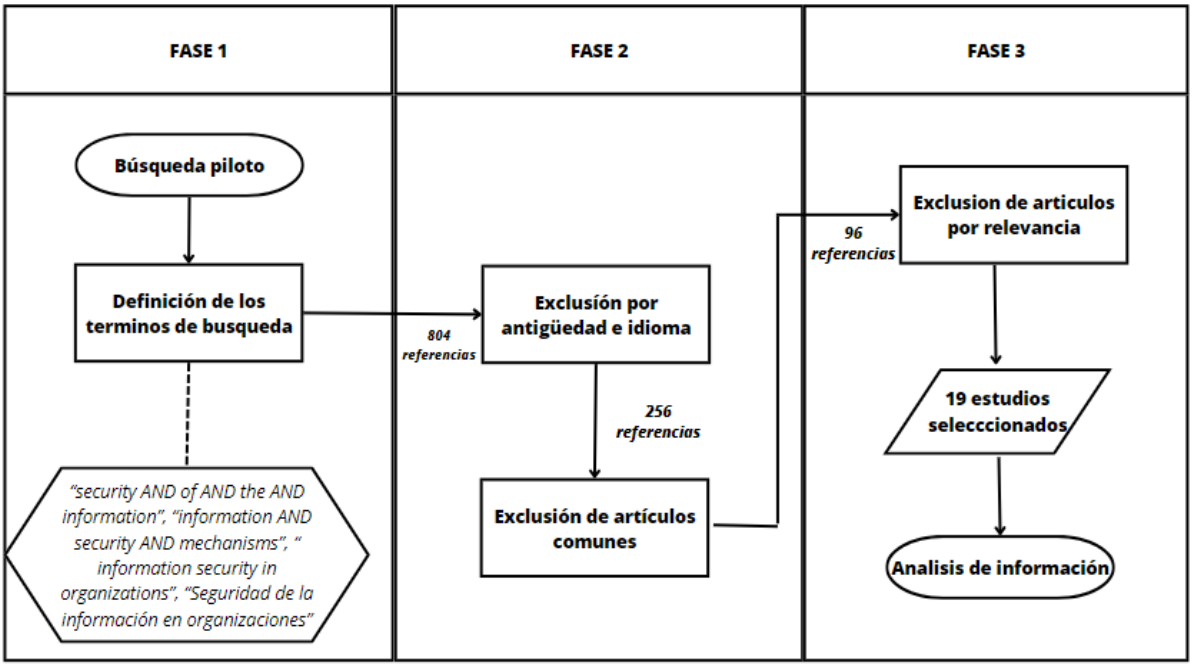
Tabla 1
Criterios de inclusión y exclusion

		Criterios
Inclusión	**I01**	Artículos publicados entre el año 2018 y 2023
	I02	Artículos relacionados con la seguridad de la información
	I03	Artículos en idioma inglés y español
Exclusión	**E01**	Artículos comunes, o que no están relacionados con la seguridad de la información
	E02	Artículos publicados antiguos
	E03	Artículos en otros idiomas distintos al inglés y español
	E04	Artículos por su menor relevancia

De la misma forma el proceso de exclusión se muestra en la Figura 1, en la fase 1, se inicia con la búsqueda respecto al tema de investigación y se definen los términos de búsqueda. Asimismo, en la fase 2, se realiza una reducción de los artículos tomando en cuenta, artículos que son semejantes, artículos que son muy antiguos y artículos que tienen otro idioma distinto al español y al inglés. y finalmente en la fase 3 se realiza una eliminación a los artículos que tienen menos relevancia quedándonos con 19 artículos para el análisis de la información.

Figura 1

Proceso de exclusion



3. DESARROLLO

3.1. Resultados

Para llevar a cabo la exploración y análisis exhaustivo del tema de revisión sistemática, Tras completar el análisis, se presenta una descripción y los mecanismos de seguridad de la información obtenidos en la Tabla 2 a continuación:

Tabla 2
Resumen de los aportes relevantes

N°	Autores	Descripción	Mecanismos
1	Sánchez S. Paola, Garcia G. José, Triana Antony, Perez C. Leydi (2021)	Este artículo consiste en el diseño de una herramienta que permite evaluar el nivel de seguridad informática (PYMEs) en Colombia, asimismo algunos mecanismos y recomendaciones ante vulnerabilidades de riesgo cibernético	• Actualización de software • Búsqueda exhaustiva de vulnerabilidades y exposiciones riesgosas en los sistemas y programas utilizados por la organización. • Gestión de riesgos • Implementación de medidas de protección (firewalls, antivirus y cifrado de datos)
2	Rodriguez B. Liset, Cruzado P. Carlos, Mejia C. Carolina, Diaz A. Mitchell (2020)	Este documento analiza el impacto de la implementación de la normativa ISO 27001 en la protección de la información de una entidad en Perú. También aborda cómo esto contribuye a elevar los niveles de confidencialidad, integridad y disponibilidad de los datos.	• El acceso a la información debe estar restringido a usuarios con autorización, teniendo en cuenta su posición o función dentro de la organización.

			• Asegurar que la información esté permanentemente disponible para apoyar la toma de decisiones • Monitoreo y detección de intrucciones
3	Altamirano Kadu	El documento analiza la relevancia de la seguridad de la información en el ámbito de la administración pública, resaltando la imperativa protección para asegurar la confidencialidad, integridad y accesibilidad de la misma.	• Cifrado de datos • Control de acceso • Implementación de políticas de seguridad de información • Auditorías y revisiones periódicas
4	Tonysé, Martín	Este trabajo se encarga de describir requisitos básicos para implementar y documentar un Sistema de gestión de seguridad de la información (SGSI).	• Copias de seguridad para la recuperación ante ataques o catástrofes. • Uso de antivirus
5	Estrada E. Royer, Únas G. José, Floréz R, Oleskyenio	Este estudio de caso se enfoca en las prácticas de seguridad de la información en la Universidad del Valle, sede Tuluá, durante la pandemia. Asimismo, se menciona que se necesita implementar estrategias de sensibilización para promover una mejor higiene digital.	• Autenticación de doble factor • Métodos de encriptación • Actualización de software • Copias de seguridad • Protección contra malware
6	Morales Flavio, Toapanta Sergio, Toasa Renato	El documento analiza la implementación de un sistema de seguridad perimetral como estrategia para proteger la integridad, confidencialidad y disponibilidad de la información en una institución. Se destaca la importancia de la seguridad de la información en un contexto donde las amenazas cibernéticas continúan creciendo a nivel mundial.	• Firewall • Implementación y supervisión de los controles de seguridad de TI • Protección contra malware • Control de acceso
7	Altamirano Marlon	El documento analiza la gestión de la seguridad de la información y los riesgos asociados a su uso en redes de computadoras. El documento también destaca la importancia de la gestión de riesgos y menciona otros modelos y estándares utilizados en el campo de la seguridad de la información.	• Implementación de estándares de seguridad • sistemas de detección de intrusiones • Cifrado de datos • Gestión de riesgos
8	Chimbo Henry	Estudio realizado para dar a conocer técnicas de seguridad con el fin de mejorar las técnicas empresariales	• Diferenciación entre red de invitados y red corporative
9	Espinoza M. Marco	El documento analiza la relevancia de los marcos de gobierno de la seguridad de la información, subrayando que en la actualidad, la información representa uno de los recursos más cruciales para las organizaciones. Además, se hace mención de herramientas y métodos destinados a asegurar la seguridad de la información.	• Implementación de medidas técnicas de seguridad (como firewalls, sistemas de detección de intrusiones y software antivirus). • Enfocarse en la sensibilización a través de

			la educación y la formación de los empleados • Implementación de prácticas y modelos como ISO, COBIT, ITIL, CMMI, PMBOK
10	Londoño C. José, Dorado G. Daniel, Giraldo R. Daniela	El documento analiza la importancia de la seguridad de la información en las organizaciones y la necesidad de implementar estrategias de protección. Se destaca que, aunque la digitalización ha facilitado el almacenamiento y acceso a la información, también ha aumentado los riesgos de violación y fraude.	• Implementar sistemas de monitoreo y detección de posibles amenazas para identificar comportamientos atípicos. • Mantener actualizados de forma regular los sistemas y software con las últimas actualizaciones de seguridad. • Ofrecer formación recurrente a los empleados sobre las políticas de seguridad de la información.
11	Tundidor M. Lázaro, Medina L. Alberto, Nogueira R. Dianelys, Serrate A. Annia	El documento analiza la evaluación del sistema de seguridad de la información en empresas de proyectos del sector de la construcción en Cuba. Además, se mencionan las exigencias de la normativa cubana del Sistema de Gestión de Seguridad de la Información.	• Aplicación de cuestionarios para recopilar información primaria sobre los sistemas informativos y se utilizan escalas de Likert para evaluar los datos obtenidos. • Aplicación de cifrado de datos: a. Cifrado en reposo b. Cifrado en tránsito c. Cifrado en uso
12	Astudillo G. Cesar, Cabrera D. Augusto	El documento evalúa las políticas de administración de la seguridad de la información en un centro de datos. También enfatiza la relevancia de establecer políticas de seguridad de la información en los centros de datos, dado que estos tienen la responsabilidad de asegurar la disponibilidad de los servicios que utilizan los sistemas.	• Protección del centro de datos físicos. • Control de acceso obligatorio a. Autenticación de usuarios b. Autorización de acceso c. Auditoria de actividades • Realizar evaluaciones de riesgos
13	Milo Claudio	El documento trata sobre la importancia de la información como un activo crucial para las organizaciones, y cómo esta suele ser generada por sistemas automatizados. Se mencionan métodos para proteger los datos de los distintos riesgos informáticos que existan.	• Implementar políticas de seguridad • Realizar capacitación a los empleados • Realizar pruebas de penetración para identificar debilidades y vulnerabilidades. • Encriptación de datos

14	Muñoz C. Peter	En este documento se analizan diferentes modelos y normas existentes, como COBIT, ITIL y los modelos ISO 17799, 27001 y 27002. El objetivo es establecer un modelo general de seguridad que permita a las organizaciones evitar ataques informáticos y adoptar protocolos de seguridad adecuados.	• Proporcionar a los empleados formación periódica sobre las mejores prácticas de seguridad de la información. • Mantener al día los sistemas y aplicaciones con las últimas actualizaciones de seguridad. • Realizar respaldos regulares de la información.
15	Moreno D. Henry & Garcia M. Belisario	Este informe analiza los posibles peligros relacionados con la gestión del acceso a la red en una compañía, así como los beneficios derivados de la implementación de listas de control de acceso. También se hace referencia a las medidas de control y otros dispositivos adoptados para reducir los riesgos detectados.	• Implementación de listas de control de acceso • Implementación de un servidor con servicio proxy para filtrar y crear restricciones hacia los sitios de internet a los que se pueden conectar los usuarios. • Implementación de medidas de seguridad en puertos y Network Access Control
16	More V. Ruben, Sandoval M. Corina, Infante S. Carmen, Correa C. Teofilo & Jaramillo A. Javier	Este documento analiza temas relacionados con la optimización y organización de la red de comunicación, la seguridad de los datos y la gestión de riesgos en las organizaciones. Además, se destaca la importancia de algunos mecanismos que garanticen la seguridad de la información	• Optimización y organización de la red de comunicación y seguridad del servidor y centro de datos. • Implementación de planes de contingencia
17	Imbanquigo E. Daysi, Diaz Francisco, Saltos E. Tatyana, Rosario Arciniega S.	El trabajo realiza una revisión sistemática de la literatura para identificar los problemas de seguridad, las medidas de seguridad utilizadas y las herramientas utilizadas para detectar y combatir los ataques informáticos en las instituciones	• Establecer políticas de seguridad • Control de accesos • Implementar firewalls, sistemas de detección y prevención de intrusiones • Establecer procesos de monitoreo continuo
18	Guijarro R. Alfonso, Yepez H. Jessica, Peralta G. Tania & Ortiz Z. Mirella	Este documento trata sobre la aplicación de la defensa en profundidad en un entorno empresarial. Además, se propone algunos mecanismos para reducir las posibilidades de ataques y fallos de seguridad	• Firewalls y sistemas de detección de intrusos • Encriptación de datos • Acceso y control de usuarios • Capacitación a empleados
19	Valencia Liliana, Guarda Teresa, Arias	El documento trata sobre la seguridad de la información en las redes de sensores inalámbricos aplicadas a sistemas de medición inteligentes en empresas. Además, se enfoca en la importancia de	• Encriptación asimétrica • Monitorización y detección de intrusiones • Control de acceso

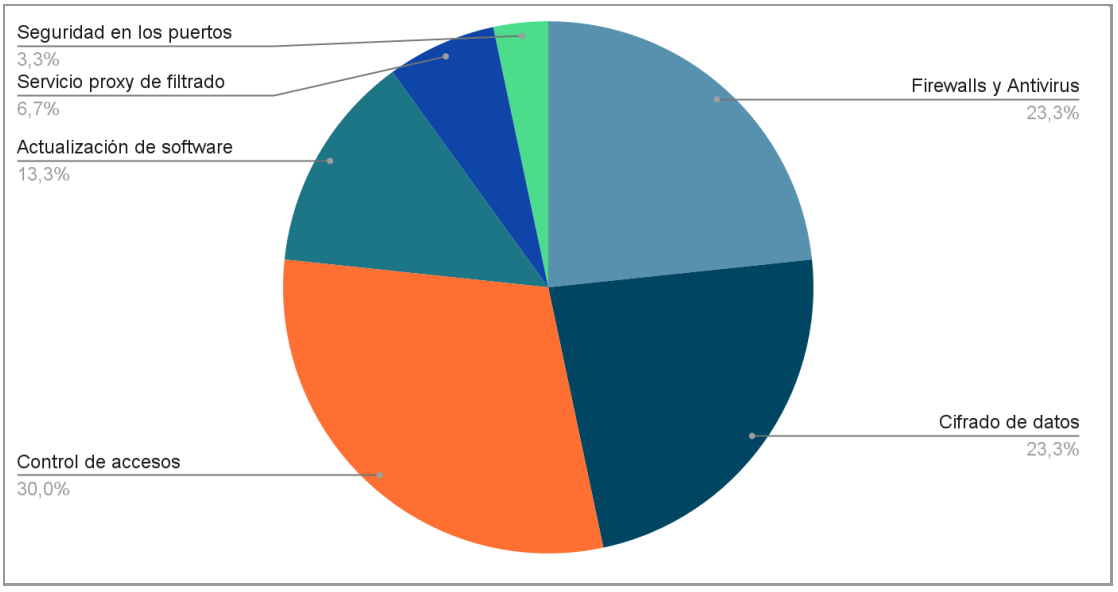
Gabriel, Quiña Gueovanni	garantizar la integridad y disponibilidad de los datos recolectados en estos sistemas	• Implementar parches de seguridad

Nota: La table 2 presenta los 19 artículos seleccionados tras aplicar los respectivos filtros. Además, muestra los resultados obtenidos tras analizar cada estudio de investigación.

Con los resultados obtenidos de los artículos analizados de la tabla 2, se pudo realizar el siguiente diagrama circular el cual nos muestra los mecanismos de seguridad de la información en una organización en todo lo referente al software

Figura 2

Mecanismos de seguridad de la información en una organización, Software

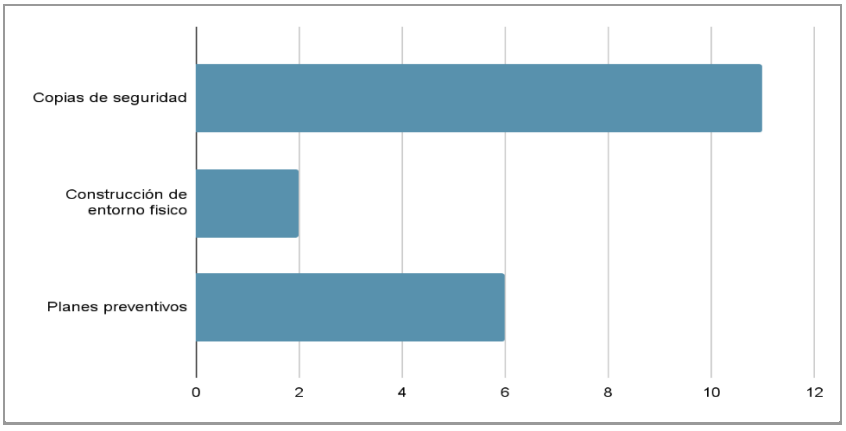


Al analizar la figura 2, observamos que mayor prioridad tiene la implementación de control de accesos con un 30%, porque esto ayuda a garantizar que solo las personas autorizadas tengan acceso a ciertos sistemas o información es esencial para prevenir violaciones de seguridad. Asimismo, otro mecanismo que se menciona es la implementación de la seguridad en los puertos, como se muestra solo tiene una presencia de un 3,3% se considera importante, pero puede que se vea como un elemento complementario a otras medidas más prioritarias.

También con los datos de la tabla 2, podemos observar el siguiente gráfico de barras que nos muestra los mecanismos de seguridad de la información en una organización en todo lo referente al hardware.

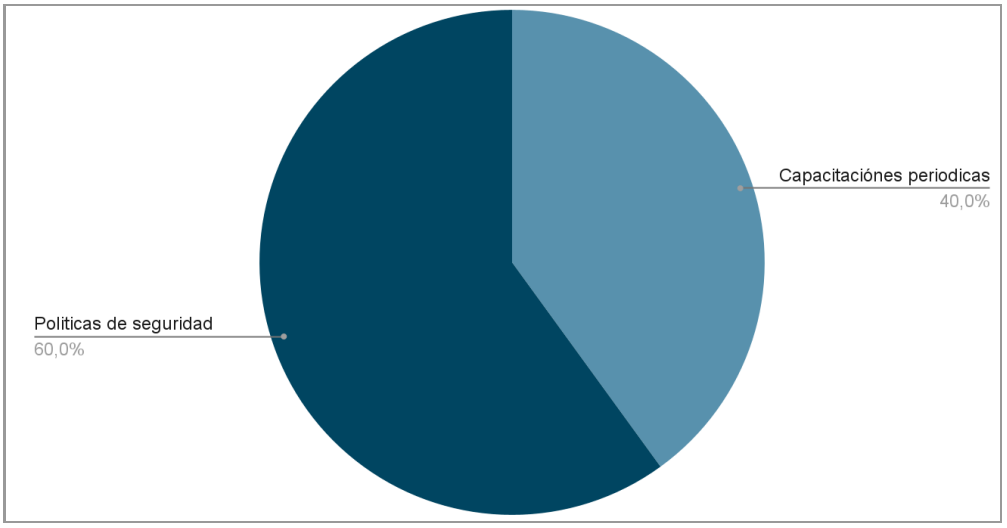
Figura 3

Mecanismos de seguridad de la información en una organización, Hardware



Al analizar la figura 3, observamos que mayor prioridad tiene la realización de copias de seguridad, porque esto proporciona una capa de seguridad crucial ante una amplia variedad de situaciones adversas que pueden afectar al hardware. Asimismo, la construcción de un entorno físico diferente no tiene mucha prioridad porque no todas las organizaciones cuentan con un presupuesto para poder realizarlo.
Asimismo, se realizó el siguiente gráfico circular, este nos indica los mecanismos de seguridad de la información en una organización en todo lo referente a la persona.

Figura 4
Mecanismos de seguridad de la información en una organización, Personas



Al analizar la figura 4, observamos que mayor prioridad tiene la implementación de políticas de seguridad, porque garantiza la protección de la privacidad, cumple con regulaciones legales, construye confianza con los clientes, previene pérdidas financieras y daños a la reputación, y establece procedimientos claros para responder a incidentes de seguridad.

4. CONCLUSION

Se logró obtener varios mecanismos desarrollados para protección de la seguridad de la información organizacional. Esta multiplicidad de mecanismos responde a 3 aspectos clave de una organización actual: el software, hardware y las personas; de esta forma se agruparon los resultados y se encontró que hay mecanismos que se relacionan y/o se fortalecen entre sí; tal es el caso de los privilegios mínimos con la gestión de contraseñas y autenticación de doble factor. Incluso este método digital de privilegios mínimos se extiende al hardware a través del acceso físico limitado por los tipos de empleados, lo que se fortalece con lo mencionado sobre la capacitación del personal. En resumen, se concluye que la protección de la información requiere una aproximación multifacética que considere tanto aspectos tecnológicos como humanos. El establecimiento de políticas de seguridad, la restricción de acceso a la información, la gestión de contraseñas, el mantenimiento actualizado del software y la infraestructura física segura son piezas clave para prevenir brechas de seguridad y posterior pérdida de información. Adicionalmente, la capacitación continua del personal emerge como una herramienta crítica para mitigar riesgos, dado que las personas constituyen el eslabón más vulnerable en la cadena de seguridad de la organización. Su preparación y conciencia son fundamentales para mantener un entorno seguro y proteger los activos de información de la organización en el entorno actual altamente dinámico y tecnológicamente avanzado.
Para finalizar, se resalta la importancia de investigar aquellos métodos de capacitación al personal que han arrojado los mejores resultados, es decir, los mecanismos que disminuyen considerablemente el error humano relacionado con la pérdida de información sensible de la empresa.

5. REFERENCIA BIBLIOGRÁFICA

Altamirano de la Borda, K. J. (2021). *La seguridad de la información en la administración pública*. Actas Del Congreso Internacional De Ingeniería De Sistemas, 77-95. https://doi.org/10.26439/ciis2020.5480.

Altamirano, M. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso*. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568.

Astudillo, C. W., & Cabrera, A. E. (2019). *Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942*. Dominio de Las Ciencias, 5(3), 132. https://doi.org/10.23857/dc.v5i3.929.

Chimbo, H. (2023). *Análisis de equipos de comunicación y la privacidad en redes inalámbricas aplicado a la Empresa Artefacta del cantón Baba*. http://dspace.utb.edu.ec/handle/49000/14165.

Cumbreras, A. M. (2020). *La seguridad de los datos personales y la obligación de notificar las brechas de seguridad*. Revista de Derecho, Empresa y Sociedad (REDS), 16, 151-162. https://dialnet.unirioja.es/servlet/articulo?codigo=7631166.

Espinoza, M. A. (2019). *Importancia de los modelos para el gobierno de la seguridad de la información en las empresas. Una revisión sistemática de la literatura*. Revista ESPACIOS, 40(25). https://www.revistaespacios.com/a19v40n25/19402505.html.

Estrada, R. D., Unás, J. L., & Flórez, O. E. (2021). *Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá*. Revista logos ciencia & tecnología, 13(3), 98–110. https://doi.org/10.22335/rlct.v13i3.1446.

García, B. A., & Moreno, H. A. (2021). *Análisis de la implementación de listas de control de acceso (ACL), para mejorar la seguridad de la información en la empresa Crawford Colombia Ltda*. https://repository.ucatolica.edu.co/handle/10983/26240.

Gené, J., Gallo de Puelles, P., & De Lecuona, I. (2018). *Big data y seguridad de la información. Atención primaria*, 50(1), 3–5. https://doi.org/10.1016/j.aprim.2017.10.004.

Guijarro, A. A., Yepez, J. M., Peralta, T. J., & Zambrano, M. C. (2018). *Defensa en profundidad aplicado a un entorno empresarial*. Revista ESPACIOS, 39(42). https://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf.

Imbaquingo, D. E., Diaz, F. J., Echeverria, T. K., Hidrobo, S. R., Villavicencio, D. A., & Ordonez, A. R. (2020). *Information security issues in educational institutions. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. http://dx.doi.org/10.23919/CISTI49556.2020.9141014.

Londoño, J. L., Dorado, D. R., & Giraldo, D. (2022). *Gerencia de la seguridad en la información de las organizaciones*. https://digitk.areandina.edu.co/handle/areandina/4535.

Morales, F., Toapanta, S., & Toasa, R. (2020). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 27, 553–565. https://www.proquest.com/docview/2385756526?pq-origsite=gscholar&fromopenview=true.

More, R. A., Sandoval, C., Infante, C. L., Correa, T. R., & Jaramillo, J. E. (2023). *Seguridad de la Información en Procesos de Organización para una Asociación de Profesionales con la Metodología del Marco de Trabajo COSO*. Memorias de la Décima Tercera Conferencia Iberoamericana de Complejidad, Informática y Cibernética: CICIC 2023, 159-164. https://doi.org/10.54808/CICIC2023.01.159.

Milio, C. (2021). *Homo Sapiens, el eslabón débil de la seguridad de la información*. Revista Abierta de Informática Aplicada, 4. http://portalreviscien.uai.edu.ar/OjS/index.php/RAIA/article/view/12.

Muñoz, P. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos*: Una revisión sistemática. http://dspace.ups.edu.ec/handle/123456789/20932.

Ordoñez, D. (2020). *Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2*. Ingenius, 25, 94–103. https://doi.org/10.17163/ings.n25.2021.09.

Rodriguez, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana*. Propósitos y Representaciones, 8(3). http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011&lng=es&nrm=iso&tlng=es.

Sánchez, P. A., Garcia, J. R., Triana, A., & Coronell, L. P. (2021). *Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia*. CIT Informacion Tecnologica, 32(5), 121–128. https://dialnet.unirioja.es/servlet/articulo?codigo=8088673.

Svintsytskyi, A., & Fernandez, A. E. (2022). *Protection of national security in the information and cyberspace*. Revista Científica General José María Córdova, 20(38), 243–244. https://doi.org/10.21830/19006586.954.

Tonysé, M. (2021). *Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001*. http://scielo.sld.cu/scielo.php?pid=S2218-36202021000500495&script=sci_arttext.

Tundidor, L., Medina, A., Nogueira, D., & Serrate, A., (2019). *Evaluación del sistema de seguridad de la información para empresas de proyectos*. Redalyc.org. Retrieved September 27, 2023, from https://www.redalyc.org/journal/1815/181560147001/181560147001.pdf.

Valencia, L., Guarda, T., Arias, G. P. L., & Quiña, G. N. (2019). *Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 17, 393–406. https://www.proquest.com/docview/2195126520?pq-orgsite=gscholar&fromopenview=true.