ISSN: 2788 - 6549 | ISSN-L: 2788 - 6549
https://doi.org/ en trámite

REVISTA MAYA
ADMINISTRACIÓN Y TURISMO
www.revistamaya.org

Volumen 6
No. 2 Julio - diciembre 2024
Páginas 14 - 26

Ciberseguridad: Protección de la empresa en la era digital

Cybersecurity. Protecting your company in the digital age

Rubén Carlos Tunqui Cruz
carlostunqui@gmail.com
https://orcid.org/0000-0002-7450-3765
Universidad Autónoma Tomas Frías, Potosí, Bolivia

Artículo recibido en 01 de febrero 2024 / Arbitrado en 05 de marzo 2024 / Aceptado en 10 de abril 2024 / Publicado en 01 de julio 2024

RESUMEN

La ciberseguridad se ha convertido en prioridad para las empresas en la era digital, donde la protección de los sistemas informáticos es vital en la continuidad del negocio y la confianza del cliente. En este contexto, la adopción de medidas preventivas de ciberseguridad se vuelve crucial en el marco de la investigación de mercados digital. El objetivo de la investigación fue reflexionar acerca de la teoría encontrada referente a la ciberseguridad y su trascendencia en el ámbito empresarial. Se llevó a cabo una revisión sistemática de artículos desde 2010 hasta 2024, utilizando bases de datos como Scielo, Web of Science y Scopus. Los criterios de inclusión abarcaron artículos indexados, con acceso abierto, de cualquier país, metodología y cantidad de muestra, mientras que se excluyeron aquellos que no abordaban las incidencias en la ciberseguridad empresarial. Estos hallazgos ofrecen una perspectiva para la visualización de un panorama favorable nacional e internacional de la ciberseguridad.

Palabras clave: Ámbito empresarial; Ciberseguridad; Prevención; Protección; Sistemas informáticos

ABSTRACT

Cybersecurity has become a priority for companies in the digital age, where the protection of computer systems is vital for business continuity and customer trust. In this context, the adoption of preventive cybersecurity measures becomes crucial in the framework of digital market research. The objective is to reflect on the theory found regarding cybersecurity and its significance in the business field. A systematic review of articles from 2010 to 2024 was carried out, using databases such as Scielo, Web of Science and Scopus. The inclusion criteria included indexed articles, with open access, from any country, methodology and sample size, while those that did not address the incidents in business cybersecurity were excluded. These findings offer a perspective for the visualization of a favorable national and international panorama of cybersecurity.

Key words: Business field; Cybersecurity; Prevention; Protection; Computer systems

INTRODUCCIÓN

La difusión y desarrollo del sistema tecnológico ha cambiado la base material de nuestras vidas, por tanto la vida misma, en todos sus aspectos: en cómo producimos, cómo y en qué trabajamos, cómo y qué consumimos, cómo nos educamos, cómo nos informamos-entretenemos, cómo vendemos, cómo nos arruinamos, cómo gobernamos, cómo hacemos la guerra y la paz, cómo nacemos y cómo morimos, y quién manda, quién se enriquece, quién explota, quién sufre y quién se margina.

Las nuevas tecnologías de información no determinan lo que pasa en la sociedad, pero cambian tan profundamente las reglas del juego que debemos aprender de nuevo, colectivamente, cuál es nuestra nueva realidad, o sufriremos, individualmente, el control de los pocos (países o personas) que conozcan los códigos de acceso a las fuentes de saber y poder.

La importancia de la ciberseguridad en la era digital y en la investigación de mercados digitales radica en la necesidad apremiante de proteger la integridad, confidencialidad y disponibilidad de la información recopilada durante este proceso. El término ciberseguridad se define como la habilidad de proteger y defender las redes o sistemas de los ciberataques (Saroka, 2002). No obstante, este concepto ha tenido una evolución significativa en los últimos treinta años.

En el ámbito empresarial, es innegable que la continuidad de negocios depende en gran medida de la estabilidad, seguridad y protección de los sistemas digitales. Un ataque cibernético exitoso puede paralizar por completo las operaciones de una empresa, lo que resulta en pérdidas financieras significativas y daños irreparables a la reputación (Madeo, 2023). Por lo tanto, la implementación de medidas efectivas de ciberseguridad se convierte en una necesidad imperiosa para garantizar la resiliencia y sostenibilidad de las organizaciones en un entorno digital altamente interconectado y vulnerable.

Esta actividad, tan necesaria en la actualidad, sigue facilitándole al empresario todo tipo de procesos. Sin embargo, la empresa es vulnerable ante los riesgos técnicos y legales relativos a la protección de la privacidad de la información y datos personales de quienes la integran. La privacidad comprende una serie de situaciones relacionadas con el estatus personal y particular de cada individuo, por ello es importante analizar algunas de ellas para determinar hasta donde llegan los derechos y las obligaciones que atañen a cada una de las partes involucradas en un contexto empresarial.

Estudiar las amenazas de ciberseguridad y prepararnos para enfrentarlas en el mundo empresarial, es entender cuál es el entorno de amenazas de ciberseguridad en el que se mueve su negocio y, para ello, sobre quiénes son los actores de amenazas y cuáles son sus motivaciones, qué tipos de ataques existen de ellos estamos más expuestos y con qué probabilidad e impacto en la era digital empresarial. Esto implica no solo prepararse para lo que se espera, sino para las incertidumbres que puedan surgir. Una organización que estudia y se prepara frente a las amenazas de ciberseguridad puede estar mejor preparada para salir victoriosa ante una ciberadversidad.

Estos problemas se derivan principalmente por el uso inapropiado de los medios electrónicos o errores y negligencias en el manejo de la información que derivan en la comisión de hechos ilícitos. Actualmente, las empresas, pequeñas, medianas o grandes, utilizan la tecnología para todo tipo de procesos, así como una gran cantidad de información que requiere resguardo y protección. Es a partir de esta premisa como se abordará esta temática en el presente análisis.

De acuerdo con lo anterior, se destaca la importancia de la aplicación de tecnología en negocios que ya cuenta con trayectoria para modernizar sus procesos, adicionalmente, esto necesita de la formación y concienciación de los empleados en las empresas sobre aspectos fundamentales para que comprendan los riesgos de los ciberataques y cómo pueden contribuir a la protección de la empresa.

Por lo antes expuesto, esta investigación se centra en el estudio de la ciberseguridad y su trascendencia en el ámbito empresarial, con el objetivo principal de determinarlas de manera precisa y exhaustiva.

MÉTODO

El presente estudio se basó en un enfoque cualitativo para llevar a cabo la investigación. En este estudio, se empleó una metodología de la revisión sistemática de la literatura existente con el análisis detallado de casos prácticos para investigar la importancia de la ciberseguridad en la investigación de la era digital empresarial.

Dentro de este enfoque, se reconoce que la revisión bibliográfica desempeña un papel fundamental en la identificación de las últimas tendencias y en la síntesis de los fundamentos necesarios para consolidar una disciplina (Tramullas, 2020). Por lo tanto, se optó por utilizar la revisión sistemática de la literatura como método de investigación, siguiendo el enfoque propuesto por (Ferreras, 2016).

Al adoptar la revisión sistemática de la literatura como método de investigación, se realiza la revisión de literatura, la cual se centró en comprender los conceptos fundamentales de la ciberseguridad en entornos digitales, los avances tecnológicos en el campo empresarial y la intersección entre la ciberseguridad y la investigación de mercados digitales. Se analizaron los últimos desarrollos en materia de seguridad informática, así como los casos de estudio y las mejores prácticas en la implementación de medidas de seguridad en entornos digitales. Esto contribuye a la objetividad y la replicabilidad del estudio, al tiempo que proporciona una base sólida de conocimientos existentes para respaldar los hallazgos y las conclusiones del estudio.

Para realizar la revisión sistémica, se ha adoptado cuatro fases, las cuales responde a: búsqueda, evaluación, análisis y síntesis (Codina, 2018).

1. Fase de Búsqueda:

a) Se realizó una búsqueda en la base de datos de Google Académico utilizando palabras clave relevantes como: “ámbito empresarial”; “ciberseguridad”; “prevención”; “protección”; “sistemas informáticos”.

b) Se aplicó el filtro de idioma para incluir tanto artículos en inglés como en español.

c) Se estableció un rango de fechas de publicación entre los años 2010 y 2024 para asegurar la inclusión de investigaciones recientes.

d) Se consideraron artículos científicos originales y de revisión, excluyendo informes de tesis.

e) Se buscó en revistas reconocidas e indexadas en Scielo, ProQuest y Scopus.

2. Fase de Evaluación:

a) Se revisaron los títulos y resúmenes de los artículos obtenidos en la búsqueda inicial para determinar su relevancia.

b) Se aplicaron los criterios de inclusión establecidos, como la longitud de los artículos entre 10 y 20 páginas y la exclusión de informes de tesis.

c) Los artículos que no cumplían con los criterios de inclusión fueron descartados.

3. Fase de Análisis:

a) Se realizó una lectura detallada de los artículos seleccionados para extraer la información relevante sobre la ciberseguridad en la era digital en el contexto empresarial.

b) Se registraron los datos importantes, como el diseño de la investigación, la población estudiada, los métodos utilizados y los hallazgos principales.

4. Fase de Síntesis:

a) Se analizaron y resumieron los hallazgos de los artículos seleccionados en relación con la ciberseguridad en la era digital en el contexto empresarial.

b) Se identificaron patrones, temas comunes y discrepancias entre los estudios.

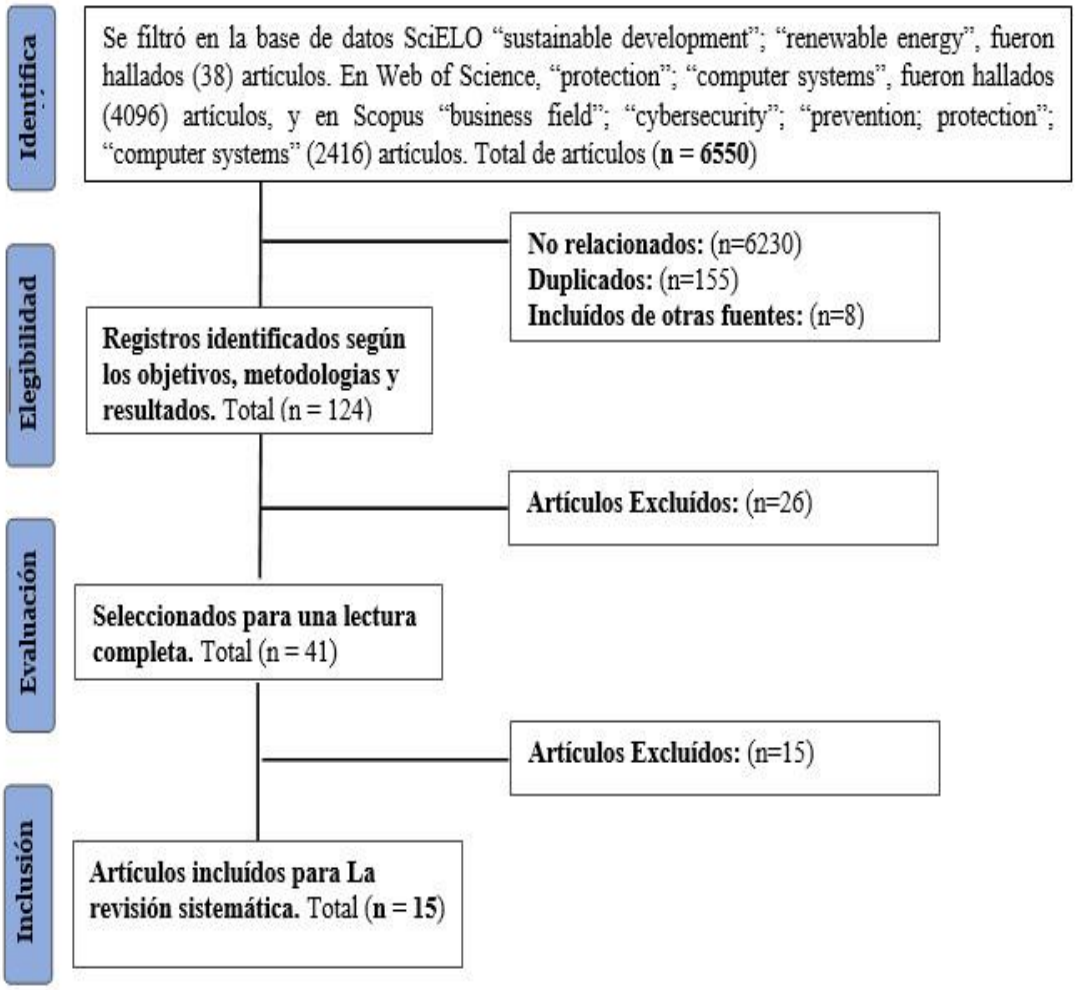
c) Se elaboraron conclusiones generales y se destacaron las implicaciones para la práctica educativa y las recomendaciones para futuras investigaciones.

El rastreo de la información se realizó a través de las plataformas desde donde se tuvo acceso a las fuentes confiables como Scielo, Web of Science y Scopus. En tal sentido, la revisión sistemática se realizó en la base de datos de Scielo utilizando las palabras clave “sustainable development”; “renewable energy”, con las que obtuvo 38 artículos. En el caso del buscador Web of Science, se utilizaron las palabras clave: “protection”; “computer systems”; con un resultado de 4096 artículos. Asimismo, en la base de datos Scopus con la búsqueda de palabras claves: “business field”; “cybersecurity”; “prevention; protection”;

"computer systems", fueron hallados 2416 resultados. Así, se obtuvo un total de 6550 artículos, de los cuales se descartaron 6230 por no considerarse relacionados y 155 por repetirse entre las bases de datos.

En esta primera fase de identificación se obtuvo un total de 165 artículos que continuaron a la fase de cribado, donde 124 fueron destacados de acuerdo a sus objetivos, metodología y resultados. Quedaron 41 artículos en la fase de idoneidad para la realización de lecturas completas, pudiéndose hallar los análisis respectivos en los que se busca 26 artículos no relevantes para el estudio en desarrollo y, finalmente, 15 artículos para determinar los presupuestos sobre las energías renovables como base de los tres pilares del desarrollo sostenible: económico, social y calidad medioambiental. Posteriormente, se incorporaron 10 investigaciones de bases de datos como Redalyc y Science Direct. Los resultados de la búsqueda, evaluación y selección pueden observar en la Figura 1.

Figura 1. *Diagrama del método PRISMA*



RESULTADOS

Una vez realizada la selección con base en criterios de inclusión y exclusión, se organizaron de la siguiente manera:

Tabla 1. *Resultados de los artículos analizados*

N.°	Título	Autor/año	Hallazgo
1	Preservación documental digital y seguridad informática.	Voutssas M. (2010).	En sus estudios aporta indicadores medibles para lograr un mayor control y protección de los recursos informáticos que conforman el sistema informático empresarial
2	Auditoría con Informática a Sistemas Contables	Martínez, A. & Marichal, L. (2012)	En sus estudios sostiene la tesis de seguridad por defecto en los sistemas (articulando esquemas de certificación para el internet de las cosas, los servicios en nube, las tarjetas inteligentes o los sistemas que soportan servicios esenciales) y auditoría y vigilancia.
3	EU cyber-defence: a work in progress.	Robinson, N. (2014)	Profundiza en la elección de alternativas relacionadas con la seguridad de las redes o los equipos.
3	EU cyber-defence: a work in progress.	Robinson, N. (2014)	Profundiza en la elección de alternativas relacionadas con la seguridad de las redes o los equipos.
4	Digital Transformation Strategies	Matt, C., Hess, T., & Benlian, A. (2015)	Aborda la tesis estrategias para la transformación digtal.
5	Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.	Álvarez-Caro, M. (2015)	Aborda desde sus estudios el Derecho al olvido en internet como el nuevo paradigma de la privacidad en la era digital.
6	La informática y la seguridad. Un tema de importancia para el directivo.	García, G. & Vidal M. (2016)	Sus hallazgos indican que la Tecnología permite conectar diferentes equipos informáticos a través de una red inalámbrica de banda ancha, utilizando la informática y la seguridad
7	Seguridad en Informática: consideraciones y Dominio de las ciencias	Quiroz-Zambrano, S. y Macías-Valencia, D. (2017)	Demuestran en sus estudios la relación conducente entre la seguridad Informática y las ciencias afines.
8	Los sistemas de información de costos en empresas vitivinícolas	Sánchez, E. & Lettry, R. (2018)	Aporta desde sus investigaciones los factores que influyen en los sistemas de información de costos en empresas vitivinícolas
9	La transformación digital en el Sector Financiero	Arguedas, R., Sánchez, Á., & García, R. (2019)	La investigación y el desarrollo de tecnologías para la transformación digital en el Sector Financiero
10	Legal Tech: La transformación digital de la abogacía	Barrio, M. (2019)	Desarrolla una metodología para La transformación digital de la abogacía
11	Transformación digital de los departamentos de relaciones	Cuenca, J., Matilla, K., & Compte, M.	Desarrolló un conjunto de indicadores relacionados con

	públicas y comunicación de una muestra de empresas españolas.	(2020)	transformación digital de los departamentos de relaciones públicas y comunicación de una muestra de empresas españolas
12	Las 5 tendencias en ciberseguridad de las que se hablarán en 2022	Cloud, A. & Cyber, R. (2020)	Aborda acerca de las 5 tendencias en ciberseguridad de las que se hablarán en 2022
13	Conoce las herramientas de ciberseguridad para proteger tu empresa.	Bello, E. (2022)	Se pronuncia por fomentar las herramientas de ciberseguridad para proteger tu empresa.
14	La importancia de la ciberseguridad en la era digital	Castro, J. M. (2023)	Apuesta en sus estudios por la importancia de la ciberseguridad en la era digital.
15	La importancia de la ciberseguridad en la era digital	Barrios, J. (2024)	Profundiza en el fenómeno "internet" y "la era digital" en la sociedad, y en el alcance de ciertos derechos fundamentales que necesitan estar reconocidos y gozar de un marco protectorio.

En relación con las investigaciones sobre las energías renovables como modelo sostenible de la generación de energía desde la conservación del medio ambiente, se identificó que el mayor número de investigaciones halladas datan entre el 2010 al 2024. Asimismo, estas investigaciones se habrían realizado en el área de Europa y América Latina generalmente.

Destaca una predominancia de estudios cualitativos, como se muestra en la Tabla 1.

Como parte de los resultados de esta investigación, se relacionan a continuación en la cuadro 1, los tipos de investigaciones que fueron incluidas para la revisión sistemática.

Cuadro 1. *Tipo de investigaciones seleccionadas*

No. de investigaciones	Tipo de investigaciones seleccionadas por categorías		
	Cualitativas	Cuantitativas	Mixtas
1		X	
2			X
3			X
4	X		
5		X	
6	X		
7	X		
8		X	
9	X		
10	X		
11	X		
12			X
13	X		
14	X		
15	X		
Total	9	3	3

En cuanto al origen de los artículos seleccionados, se destacan: EUA (2); México (3); España (4); Argentina (3); Colombia (3).

Los resultados de la búsqueda bibliográfica se analizan para cada uno de los conceptos fundamentales y dimensiones que deben tomarse en cuenta en el estudio de los presupuestos sobre la teoría de la ciberseguridad. A continuación, examinaremos brevemente los conceptos fundamentales:

Ciberseguridad: el término ciberseguridad se define como la habilidad de proteger y defender las redes o sistemas de los ciberataques. No obstante, este concepto ha tenido una evolución significativa en los últimos treinta años.

Transformación digital: el concepto de transformación digital y la utilización de las nuevas tecnologías digitales para cambiar las relaciones con los clientes, los procesos internos y las propuestas de valor es una realidad que muchos ejecutivos han convertido en su actividad cotidiana.

Al ver el rápido progreso de la utilización de las tecnologías digitales en sus sectores de actividad, han tomado conciencia de que del éxito de la transformación digital dependerá en gran medida la competitividad de su empresa en el futuro próximo. La transformación digital se está convirtiendo cada vez más en el medio generalmente aceptado para alcanzar las metas de la organización. Incluye transformaciones de las operaciones clave de los negocios, que afectan a los productos y procesos de la organización, así como a su estructura y conceptos de negocio.

Digitalización: término que se utiliza para describir diversos fenómenos sociales y técnicos, y procesos de adopción y uso de las tecnologías digitales en un amplio contexto individual, organizacional y social. A nivel empresarial la digitalización está, en gran parte, relacionada con las operaciones comerciales y cómo las tecnologías digitales pueden transformar los procesos comerciales. Además, la digitalización tiene el potencial de inducir cambios, transformación en los modelos de negocio y en la creación de valor en la empresa, que es lo que se denomina transformación digital. La digitación y digitalización tienen que ver básicamente con la tecnología, mientras que la transformación digital está relacionada con la cultura empresarial y el modelo de negocio.

Digital: el término "digital" hace referencia a la utilización de las nuevas tecnologías digitales SMACiT en tres áreas fundamentales de las empresas: a nivel externo, mejorando la experiencia del cliente y alterando todo su ciclo de vida; internamente, afectando las operaciones comerciales, la toma de decisiones y las estructuras organizativas; y en conjunto, afectando al funcionamiento de la empresa, generando a menudo nuevos modelos de negocio.

Ciberespacio: conjunto de dispositivos conectados por redes en las que se almacena y se utiliza la información electrónica así como el espacio donde diversos actos comunicativos tienen lugar. Otro enfoque que debemos dar a la definición del ciberespacio es la comprensión de la naturaleza del mismo y el propósito de este, siendo este último el procesamiento, manipulación y la explotación de la información, la facilitación y el aumento de la comunicación entre los individuos y la interacción entre personas y la información. De ahí se desprende la idea de que tanto la información como las personas son elementos fundamentales en la composición del ciberespacio, por tanto, individuos e información son susceptibles de sufrir amenazas o presentar vulnerabilidades.

Las dimensiones que deben tomarse en cuenta en el estudio de los presupuestos sobre la ciberseguridad son:

Principales teorías de la transformación digital

Tomando en cuenta las investigaciones analizadas se destaca (Cabezas & De la Peña, 2015), en la cual se señala que la transformación digital se relaciona con la transición que una empresa debe aplicar para desarrollarse en el mundo digital, donde se combina el conocimiento digital y algunos procesos tradicionales de las industrias con el objetivo de generar diferenciación en lo que se ofrece a los clientes y obtener altos niveles de eficiencia, competitividad y rentabilidad. No obstante, autores como (Huichalaf, 2016) manifiestan que la revolución digital no solo se relaciona con el ámbito empresarial sino que esta temática en particular tiene una óptica que va más

allá de las compañías y la tecnología ya que permite observar las desigualdades que existen en la sociedad y el país, y que con una adecuada aplicación de la transformación digital se lograría superar.

Así mismo, Aguilera, (2016) asegura que la transformación tecnológica aporta un nuevo modelo en la valoración de las personas ya que establece relaciones y valores que guían a los mismo que son totalmente diferentes a los tradicionales; por ejemplo: la hiperconectividad y modelos colaborativos. Lo expuesto es reafirmado por Montes, (2021), el cual se concentra en señalar como las cadenas de suministro usuales se llevaban a cabo con información incompleta y aislada que provocaba problemas en la productividad de las actividades individuales.

En este sentido, la transformación digital se ha convertido en algo fundamental en el avance de la sociedad con el surgimiento de cambios trascendentales en la tecnología. En particular, la digitalización para (Cabezas & De la Peña, 2015) hace hincapié en la transición de datos, imágenes y palabras al código binario, es decir, cero y uno; este término puede ser comparado con la adaptación y evolución que tuvo que pasar el planeta Tierra y sus elementos en sus primeras eras geológicas ya que, al igual que en ese caso, las empresas deben acoplarse y anticiparse a la "era digital". Es decir, los autores señalan que el éxito y progreso empresarial está dado por la capacidad que poseen las entidades para hacer frente a los cambios y dar paso a la digitalización en los procesos productivos. Esta idea es complementada por (Páez, Sanabria, Gauthier, et al. ,2022) al exponer que la comunidad hispanohablante aún no cuenta con los recursos necesarios para comprender apropiadamente las implicaciones de la era digital ya que son países tercermundistas que son participes de atrasos tecnológicos.

En cuanto a los dominios de la transformación digital, Rogers, (2016) destaca que existen cinco elementos para describir una visión amplia de la digitalización, los cuales son: clientes, competencia, valor agregado, datos e innovación; el autor categoriza a estos dominios como tecnologías digitales que redefinen las reglas de éxito empresarial. De esta forma, se manifiesta que existen cambios constantes en los cinco supuestos señalados para que las empresas transciendan de una era analógica al nuevo mundo digital con actualizaciones continuas. Esto es respaldado en la obra del autor Rodríguez (2020), el cual se enfoca en tres aspectos organizacionales que toma a la organización como un todo virtual y es la base para alcanzar un adecuado nivel de madurez: estructura organizacional, agile mindset y gobierno corporativo de las tecnologías de la información (TI).

Principales medidas preventivas de ciberseguridad

Para garantizar la seguridad de los sistemas informáticos, las empresas pueden adoptar diversas medidas preventivas. Entre ellas, establecer un plan de seguridad informática resulta esencial, este plan define claramente los objetivos de seguridad de la empresa y las estrategias que se implementarán para alcanzarlos (Acosta, 2024).

En un estudio realizado por IBM Security, se encontró que el tiempo promedio para identificar y contener una brecha de seguridad se redujo significativamente cuando las empresas tenían un plan de respuesta a incidentes establecido, con un promedio de 233 días para las empresas sin plan, en comparación con 147 días para las que tenían un plan implementado (Acosta, 2024). Además, es fundamental emplear software de seguridad confiable. Utilizar herramientas como antivirus y sistemas de detección de intrusiones ayuda a proteger los sistemas informáticos de los ataques cibernéticos.

Educar a los empleados sobre ciberseguridad también es esencial. La formación y concienciación de los empleados son aspectos fundamentales para que comprendan los riesgos de los ciberataques y cómo pueden contribuir a la protección de la empresa. Según un informe de Verizon, el 85% de las violaciones de datos fueron causadas por errores humanos, lo que destaca la necesidad de una capacitación continua en ciberseguridad para todos los miembros del personal.

Además de estas prácticas fundamentales, existen consejos adicionales que pueden ayudar a las empresas a fortalecer su postura de

ciberseguridad. Por ejemplo, el uso de contraseñas seguras y únicas para todos los sistemas es crucial.

La primera línea de defensa en la gestión de la ciberseguridad es el establecimiento de un plan de seguridad informática. Este plan no solo define los objetivos de seguridad de la empresa, sino que también traza las estrategias que se implementarán para alcanzarlos. Además del plan de seguridad, es fundamental emplear software de seguridad confiable para proteger los sistemas informáticos de posibles ataques cibernéticos. Herramientas como antivirus y sistemas de detección de intrusiones ayudan a identificar y prevenir posibles amenazas.

La empresa en la Era Digital

Las empresas son las entidades más vulnerables frente a las actividades cibernéticas delictivas. Esto se debe a la cantidad de información privilegiada que almacenan en sus dispositivos electrónicos.

La seguridad informática aporta una serie de ventajas para la mejora de la actividad de las compañías y de toda persona que posea un equipo informático. La influencia de la empresa en la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos. Como ha señalado el relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, los avances tecnológicos entrañan que la eficacia de la vigilancia realizada por la empresa ya no se ve limitada por su magnitud o duración. La disminución de los costos de tecnología y almacenamiento de datos ha eliminado los inconvenientes financieros o prácticos de la vigilancia. La empresa no había tenido nunca la capacidad de que dispone actualmente para realizar actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala. Es decir, las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla.

Los ejemplos de actividades de vigilancia digital declaradas y encubiertas en jurisdicciones de todo el mundo se han multiplicado, y la vigilancia en masa por parte de las empresas se ha revelado como un hábito peligroso, y no una medida excepcional. Según se ha informado, distintos gobiernos han amenazado con prohibir los servicios de las empresas de telecomunicaciones y de dispositivos inalámbricos a menos que les permitieran un acceso directo al tráfico de las comunicaciones, han intervenido los cables de fibra óptica con fines de vigilancia y han obligado sistemáticamente a las empresas a revelarles información a granel sobre sus clientes y empleados.

El derecho a la privacidad en la era digital a nivel empresarial constituye un instrumento legal internacional que consagra estándares mínimos en la materia, sentando los lineamientos básicos en torno a cuestiones de vital importancia como la tipificación de los delitos informáticos, la vigilancia de las redes de telecomunicaciones y el entorno de amenazas de ciberseguridad en el que se mueve la empresa.

Riesgos y amenazas de la ciberseguridad

En el contexto internacional actual, podemos observar que los ataques cibernéticos pueden afectar tanto a ordenadores, teléfonos móviles como a redes informáticas inalámbricas. No existe límite ni barrera que impida a los ciberatacantes introducirse en todos aquellos entes que tengan una conexión con el ciberespacio.

Los ciberataques utilizan las brechas de seguridad presentes en las tecnologías de información para pasar a copiar, borrar o reescribir la información de la víctima y se aprovechan de las vulnerabilidades que presentan la mayor parte de las estructuras cibernéticas como, por ejemplo, las redes sociales. En el siglo XXI los bits y los bytes pueden ser tan amenazantes como las balas y las bombas. El número y variedad de los ciberataques puede llegar a ser extremadamente alto, debido a la continua evolución y metamorfosis de los instrumentos informáticos cuya complejidad es cada vez más elevada. En consecuencia, hemos elaborado una lista en la que se van a describir las amenazas o ciberataques más extendidos hasta la fecha:

a) Código dañino: se trata de la amenaza más común dentro del ciberespacio. Conocido también como código malicioso o malware, tiene su fin principal en dañar el funcionamiento correcto de cualquier equipo informático, ya sea inutilizando el sistema operativo o haciéndose con el control de la memoria.

b) Gusano: se trata de códigos dañinos calificados como independientes, al estar diseñados para reproducirse a sí mismos, es decir, realizar copias de sí mismo y enviarlas a todos aquellos ordenadores que estén conectados a través de la red.

c) Virus: consiste en un programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.

d) Troyano: es un software que suele aparentar ser inofensivo o incluso realizar tareas necesarias para el usuario, pero que en realidad su objetivo es el robo o destrucción de la información acumulada en el dispositivo.

e) Botnet: es un conjunto de software que permite llevar a cabo ataques de denegación de servicio, fraudes, robos de información, la inutilización de los sistemas de antivirus o detección de intrusos o la perturbación del comercio electrónico.

f) Bomba lógica: son ciberataques cuya finalidad no es extenderse ni actuar continuamente, sino pasar a la acción en un momento determinado preestablecido por el atacante. En consecuencia, su duración es limitada en el tiempo al realizar sus funciones dañinas únicamente cuando se ha llegado al momento o cantidad de visitas preestablecidas.

Los atacantes pueden clasificarse atendiendo a diversas categorías como la autoría o la motivación. Pero es desde la autoría desde donde podemos, de forma más contundente y operativa, trazar una posible clasificación de los atacantes que nos permita una lectura de este nuevo escenario de conflicto. Nos referiremos sólo a las empresas para no alejarnos del objetivo de esta revisión sistemática:

a) Empresas: no se debe olvidar a estos agentes económicos como una de las principales fuentes de ciberataques: El espionaje industrial y el espionaje comercial.

Según el Instituto de Ciberseguridad (INCIBE), en 2021 en España se produjo una media de 40.000 ciberataques al día, de los cuales el 75% van dirigidos a Pymes. Esto supone un incremento del 125% con respecto al 2020. La evolución global hacia las nuevas tecnologías ha causado un impacto en el sector agroalimentario, ayudando a aumentar su rentabilidad y llevar a cabo una digitalización del mundo rural. Esta transformación favorece a la ecologización y al cambio climático, pero es necesario tener en cuenta las posibles amenazas cibernéticas que atentan contra las fases de la cadena agroalimentaria (producción, industrialización, distribución y venta).

DISCUSIÓN

En la revisión realizada se identificaron aspectos conceptuales que justifican la teoría referente a la ciberseguridad y su trascendencia en el ámbito empresarial, la cual está generando una transformación digital de las mismas. Es por esto que la transformación digital empresarial implica una serie de retos o desafíos. Se ha comprobado que éstos son diversos y que aún no han sido lo suficientemente estudiados. Por ello, se han identificado los retos más relevantes, dentro de los cuales se reconocen los hallazgos de (Quiroz-Zambrano y Macías-Valencia, 2017) quienes en sus estudios profundizan en la relación conducente entre la seguridad Informática y las ciencias afines. En este escenario, han emergido como una herramienta valiosa para mejorar la experiencia del cliente, dado que permiten una comunicación instantánea y personalizada, ofreciendo respuestas automáticas a consultas comunes y facilitando la navegación en sitios web y aplicaciones. Coincidimos con los citados autores en que todas las formas, el conocimiento y la consciencia sobre la seguridad informática no se deben circunscribir solo a los profesionales contables sino que abarcan a todas las personas que integran una organización. El bajo nivel de seguridad de la información existente en las empresas se debe a la falta de conocimiento, de cultura, de compromiso y de entendimiento de las personas con respecto a la seguridad informática, y también a la escasa inversión empresarial en seguridad.

En esta misma línea de pensamiento se pronuncia Voutssas, (2010) al referirse a la preservación documental digital y seguridad informática a nivel empresarial a través de indicadores medibles para lograr un mayor control y protección de todos los recursos informáticos que conforman el sistema informático empresarial. Considera además, establecer de manera documentada un plan de seguridad que permita saber cómo se debe actuar para prevenir, detectar y corregir cualquier amenaza o riesgo. Del mismo modo, se debe establecer un plan de contingencia que contemple las medidas correctivas a aplicar en caso de desastres, los recursos que serán necesarios y los roles y responsabilidades del personal.

Asimismo, la investigación desarrollada por (Sánchez, & Lettry, 2018) profundizan en los sistemas de información de costos en empresas vitivinícolas. Desde una perspectiva de negocios, un sistema de información es una solución organizacional y administrativa basada en tecnología de información para resolver problemas y desafíos del entorno. Es importante comprender las tres dimensiones que le dan forma a los sistemas y permiten que los mismos funcionen efectivamente y generen valor.

De la misma forma, cabe mencionar los resultados de (Arguedas, Sánchez, & García, 2019) al referirse a la transformación digital en el Sector Financiero, el cual se caracteriza por su constante desarrollo, adaptación y reconversión de procedimientos que involucran el manejo de dinero y datos con el objetivo de proporcionar soluciones seguras, dinámicas, flexibles y competitivas a los usuarios. En este sentido, el sector bancario se muestra como pionero en utilizar herramientas para

digitalizar sus actividades económicas, desde apoyarse con tecnologías como el Big Data, servicios de la nube hasta utilizar gestores financieros automatizados o Robo Advisors que ofrecen a los consumidores seguridad en materia financiera, integridad y protección al consumidor.

En consecuencia, siempre que hablemos de transformación digital, somos consecuentes también existen conflictos en este proceso de cambio ya que no es cuestión de solo modernizar máquinas y sistemas también requiere de alteraciones en la forma de pensar y actuar de las personas, lo que se convierte en un reto de gestión administrativa para los líderes de una organización, además, las empresas que inician esta transición a la digitalización quedan expuestas en el ciberespacio a padecer de ataques, daños o acceso no autorizado a sistemas, redes, plataformas o programas.

Al referirse a las herramientas de ciberseguridad para proteger la empresa, es fundamental emplear software de seguridad confiable para proteger los sistemas informáticos de posibles ataques cibernéticos. Herramientas como antivirus y sistemas de detección de intrusiones ayudan a identificar y prevenir posibles amenazas (Bello, 2022). Otro aspecto es la protección de los datos empresariales es la realización de copias de seguridad regulares. Las copias de seguridad actúan como un salvavidas en caso de pérdida o daño de datos debido a un ciberataque, permitiendo su recuperación (Castro, 2023).

La innovación digital en las empresas requiere revisar todos los procesos actuales para realizar los cambios necesarios para conseguir los objetivos que se están buscando. La confusión actual radica en si las empresas se quedan en la digitalización de los procesos de negocio o realmente realizan una transformación digital del negocio, de ahí la importancia de la ciberseguridad en la era digital Barrios, (2024). De esta manera, la importancia de la ciberseguridad en la investigación de mercados digitales radica en la necesidad apremiante de proteger la integridad, confidencialidad y disponibilidad de la información recopilada durante este proceso. En un entorno donde la recopilación y el análisis de datos se realizan principalmente en plataformas digitales, la seguridad de la información se convierte en un factor determinante para el éxito y la credibilidad de las investigaciones de mercado. Sin embargo, en la actualidad, la empresa es vulnerable ante los riesgos técnicos y legales relativos a la protección de la privacidad de la información y datos personales de quienes la integran.

CONCLUSIONES

En los resultados obtenidos en este artículo científico de revisión sistemática, se encontró que la comunidad científica investiga sobre la ciberseguridad en la era digital en el contexto empresarial. Además, se consideraron aspectos relacionados con la transformación digital en el contexto empresarial como proceso de reconversión y adaptación de tecnologías digitales, las mismas que están inmersas en la rutina diaria de las personas, lo que motiva a las instituciones u empresas a incorporar procedimientos innovadores para cubrir la demanda de sus clientes con productos o servicios novedosos que satisfagan sus necesidades.

De la misma manera, si se quiere una transformación digital plena y segura en el sector empresarial, esta debe ir acompañada de un componente de ciberseguridad que garantice que la información y procesos críticos tienen la mejor protección posible y que seremos capaces de responder ante cualquier eventualidad. Este análisis ha puesto de manifiesto que la ciberseguridad sigue siendo uno de los pilares fundamentales para cualquier empresa, organismo o institución. Es un sector en constante crecimiento, con agentes de amenaza cada vez más preparados, capaces de orquestar ataques de un alto nivel de complejidad e impacto.

Finalmente, se requiere capacitar al personal de servicio al cliente para reconocer y responder adecuadamente a posibles amenazas cibernéticas. Solo mediante un enfoque integral que aborde tanto las medidas técnicas como las acciones de concientización y capacitación, las empresas pueden proteger efectivamente sus activos digitales en un entorno digital en constante evolución.

REFERENCIAS

Aguilera, I. (2016). Lo que estaba por llegar, ya está aquí: La transformación digital inteligente. La Esfera de los Libros. https://www. anahuac.mx/méxico/noticias/lo-que-estaba-por-llegar- ya- aquí-la- transformación-digital- inteligente

Acosta, N. (2024). Impacto de la inteligencia artificial en la ciberseguridad empresarial: un análisis crítico de la evolución de amenazas y medidas preventivas. Obtenido de [Tesis, Universidad Técnica de Babahoyo]: http://190.15.129.146/handle/49000/15738

Álvarez-Caro, M. (2015). *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Madrid, Reus

Arguedas, R., Sánchez, Á., & García, R. (2019). La transformación digital en el Sector Financiero. *Revista Universidad Nacional de Educación a Distancia*. https://elibro.net/es/ereader/uta/113347?page=11

Barrios, J. (2024). La importancia de la ciberseguridad en la era digital. https://www.olam.com/olam/la-importancia-de-la-ciberseguridad-en-la-era-digital/

Barrio, M. (2019). Legal Tech: *La transformación digital de la abogacía*. Wolters Kluwer España. https://elibro.net/es/ereader/uta/130769?page=75

Bello, E. (2022). Conoce las herramientas de ciberseguridad para proteger tu empresa. https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/

Cabezas, M., & De la Peña, J. (2015). *La gran oportunidad: Claves para liderar la transformación digital en las empresas y en la economía*. Gesti??n 2000. España. https://elibro.net/es/ereader/uta/130769?page=75

Codina, L. (2018). *Revisiones bibliográficas sistematizadas: procedimientos generales y Framework para Ciencias Humanas y sociales*. Universitat pompeu Fabra. https://doi.org/10.1016/j.rser.2018.05.009.

Castro, J. (2023). La importancia de la ciberseguridad en la era digital. https://www.linkedin.com/pulse/la-importancia-de-ciberseguridad-en-era-digital-castro-huerta-pywve/

Cuenca, J., Matilla, K., & Compte, M. (2020). Transformación digital de los departamentos de relaciones públicas y comunicación de una muestra de empresas españolas. *Revista de Comunicación, 19(1)*, 75-92. https://doi.org/10.26441/RC19.1-2020-A5

Cloud, A. & Cyber, R. (2020). Las 5 tendencias en ciberseguridad de las que se hablarán en 2022. *Security Expo Madrid*. https://www.cybersecurityworld.es/noticias/5-tendencias-ciberseguridad-2022

Díaz, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, *REDUR 8*, Diciembre 2010. https://www.boe.es/doue/2016/194/L00001-00030.pdf

Ferreras Fernández, T. (2016). *Visibilidad e impacto de la literatura gris científica en repositorios institucionales de acceso abierto. Estudio de caso bibliométrico del repositorio Gredos de la Universidad de Salamanca* [Tesis Doctoral Formación en Sociedad del Conocimiento, Universidad de Salamanca]. http://hdl.handle.net/10366/132444

García, G. & Vidal M. (2016). La informática y la seguridad. Un tema de importancia para el directivo. *Infodir, 12(22), 47-58*. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=63722.

Gómez, Ángel (2012). *El ciberespacio como escenario de conflicto. Identificación de las amenazas, en el ciberespacio*. Nuevo escenario de confrontación, Madrid, Ed. Ministerio de Defensa

Huichalaf, P. (2016). *Agenda digital con sentido ciudadano*. Editorial Universidad del Rosario. https://elibro.net/es/ereader/uta/219878?page=26

Martínez, A. & Marichal, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería, 6(2), 1-14*. http://www.redalyc.org/articulo.oa?id=193924743004.

Madeo, D. (2023). *La importancia del marketing estratégico en la industria de la seguridad electrónica*. https://revistainnovacion.com/nota/12022/la_importancia_del_marketing_estrategico_en_la_idustria_de_la_seguridad_electronica/

Matt, C., Hess, T., & Benlian, A. (2015). Digital Transformation Strategies. *Bus. Inf. Syst. Eng. 57*, 339-343. https://doi.org/10.1007/s12599-015-0401-5

Méndez, E., & Rivera, M. (2017). *Re-evolución digital: Lidera el futuro digital de tu empresa... antes de que desaparezca*. Penguin Random House Grupo Editorial México.

Montes, J. (2021). Logística 5.0: Transporta tu logística al mundo digital. *Revista de Comunicación, 19(1)*, 75-92. https://doi.org/10.26441/RC19.1-2020-A5

Páez, I., Sanabria, M., Gauthier, V., Méndez, R., & Rivera, L. (2022). *Transformación digital en las organizaciones*. Editorial Universidad del Rosario. https://elibro.net/es/ereader/uta/219878?page=26

Quiroz-Zambrano, S. & Macías-Valencia, D. (2017). Seguridad en Informática: consideraciones y Dominio de las ciencias, 3(5), 676-688. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Robinson, N. (2014). EU cyber-defence: a work in progress. *EU Institute for Security Studies*, vol.10, marzo 2014. http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf

Rodríguez, N. (2020). Innovando la educación en la tecnología: Actas del II Congreso Internacional de Ingeniería de Sistemas. Universidad de Lima.

Rogers, D. (2016). The Digital Transformation Playbook: Rethink Your Business for the Digital Age. Columbia University Press.

Sánchez, E. & Lettry, R. (2018). Los sistemas de información de costos en empresas vitivinícolas, *Revista de la Facultad de Ciencias Económicas 2008, 127, 79-103*. http://bdigital.uncu.edu.ar/8959

Saroka, R. (2002). Sistemas de información en la era digital, Buenos Aires, Argentina: Fundación OSDE. https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html.

Voutssas M. (2010). Preservación documental digital y seguridad informática. *Revista Investigación Bibliotecológica, 24(50), 127-155*. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&nrm=iso