Ciencia y Desarrollo. Universidad Alas Peruanas
http://revistas.uap.edu.pe/ojs/index.php/CYD/index

Recibido 05 de febrero 2024 - Aceptado 10 de marzo 2024

# IMPORTANCIA DE LA CIBERSEGURIDAD EN LA INVESTIGACIÓN DE MERCADOS DIGITAL

## IMPORTANCE OF CYBERSECURITY IN DIGITAL MARKET RESEARCH

**Aldrin Jefferson Calle García[1], Yaritza Margarita Conforme Merchan[2], Emily Lissette Magallanes Bueno[3], Juleidy Yolanda Guaranda Bravo[4]**

### RESUMEN

La ciberseguridad desempeña un papel fundamental en la investigación de mercados digitales, donde la protección de datos y la confianza del cliente son vitales. Es así que, este estudio analiza la importancia de la ciberseguridad en este contexto. Se empleó una metodología mixta que combinó la revisión exhaustiva de la literatura con el análisis detallado de casos prácticos de empresas afectadas por brechas de seguridad. Los resultados revelan la necesidad crítica de medidas de seguridad robustas para proteger los activos digitales y la reputación de las empresas en entornos digitales cada vez más complejos. En este sentido, se destaca que el 85% de las violaciones de datos fueron causadas por errores humanos, señalando así la importancia de la capacitación del personal en ciberseguridad. Además, el 43% de los ataques de inyección de SQL se dirigen a versiones de software desactualizadas, subrayando la necesidad de mantener el software siempre actualizado para mitigar riesgos. Así mismo, se encontró que el 90% de los ataques de phishing condujeron a la instalación exitosa de malware, lo que resalta la importancia de evitar abrir archivos adjuntos o hacer clic en enlaces de fuentes desconocidas.

**Palabras clave: Seguridad, protección, phishing, software, prevención.**

### ABSTRACT

Cybersecurity plays a fundamental role in digital market research, where data protection and customer trust are vital. Thus, this study analyzes the importance of cybersecurity in this context. A mixed methodology was employed, combining thorough literature review with detailed analysis of practical cases of companies affected by security breaches. The results reveal the critical need for robust security measures to protect digital assets and the reputation of companies in increasingly complex digital environments. In this regard, it is highlighted that 85% of data breaches were caused by human errors, thus signaling the importance of staff training in cybersecurity. Additionally, 43% of SQL injection attacks target outdated software versions, emphasizing the need to keep software always up to date to mitigate risks. Similarly, it was found that 90% of phishing attacks led to successful malware installation, highlighting the importance of avoiding opening attachments or clicking on links from unknown sources.

**Keywords: Security, protection, phishing, software, prevention.**

1. Universidad Estatal del Sur de Manabí. aldrin.calle@unesum.edu.ec. https://orcid.org/0000-0003-0178-4428
2. Universidad Estatal del Sur de Manabí. conforme-yaritza4520@unesum.edu.ec. https://orcid.org/0009-0009-0893-7627
3. Universidad Estatal del Sur de Manabí. magallanes-emily3464@unesum.edu.ec. https://orcid.org/0009-0008-8159-5531
4. Universidad Estatal del Sur de Manabí. guaranda-juleidy4779@unesum.edu.ec. https://orcid.org/0009-0004-7631-0221

RESUMO

A cibersegurança desempenha um papel fundamental na pesquisa de mercado digital, onde a proteção de dados e a confiança do cliente são vitais. Assim, este estudo analisa a importância da cibersegurança nesse contexto. Foi empregada uma metodologia mista que combinou uma revisão abrangente da literatura com a análise detalhada de casos práticos de empresas afetadas por violações de segurança. Os resultados revelam a necessidade crítica de medidas de segurança robustas para proteger os ativos digitais e a reputação das empresas em ambientes digitais cada vez mais complexos. Nesse sentido, destaca-se que 85% das violações de dados foram causadas por erros humanos, sinalizando assim a importância da capacitação do pessoal em cibersegurança. Além disso, 43% dos ataques de injeção SQL visam versões desatualizadas de software, enfatizando a necessidade de manter o software sempre atualizado para mitigar riscos. Da mesma forma, constatou-se que 90% dos ataques de phishing levaram à instalação bem-sucedida de malware, destacando a importância de evitar abrir anexos ou clicar em links de fontes desconhecidas.

**Palavras-chave: Segurança, proteção, phishing, software, prevenção.**

## INTRODUCCIÓN

El ámbito digital ha experimentado una proliferación exponencial de amenazas, desde virus y malware hasta sofisticados ataques de phishing y ransomware. Según Castro (2023), los ciberdelincuentes están constantemente innovando y desarrollando nuevas tácticas para comprometer la seguridad de nuestros datos y sistemas. Estas acciones maliciosas pueden tener diversos propósitos, desde el robo de información personal hasta la extorsión y el sabotaje, lo que subraya la creciente urgencia de abordar la ciberseguridad de manera efectiva.

En este contexto, la ciberseguridad ha emergido como una prioridad crítica por varias razones fundamentales que impactan tanto a nivel individual como empresarial. La protección de datos sensibles se ha vuelto indispensable en un entorno donde almacenamos una cantidad cada vez mayor de información personal y financiera en línea (Barrios, 2024). La pérdida o el acceso no autorizado a estos datos pueden desencadenar consecuencias graves, desde el robo de identidad hasta el fraude financiero, afectando la seguridad y la confianza de los individuos y las organizaciones (Sánchez, 2024).

Además, la ciberseguridad se desempeña en la salvaguarda de la privacidad en el entorno digital. Según Reyero (2021), menciona que con la creciente tendencia a compartir aspectos íntimos de la vida en línea, asegurar la confidencialidad de las comunicaciones y actividades en la web se vuelve esencial para preservar la intimidad y proteger los derechos individuales.

Por otro lado, en el ámbito empresarial, la continuidad de negocios depende en gran medida de la estabilidad y seguridad 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.

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 (Miranda, 2023). 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.

Por lo tanto, la ciberseguridad es esencial para proteger los datos sensibles de los clientes, durante la investigación de mercados digitales, se recopilan una amplia gama de datos, que pueden incluir información personal, preferencias de compra, historiales de navegación y otra información confidencial. La exposición de estos datos a ciberataques puede dar lugar a consecuencias graves, como el robo de identidad, el fraude financiero y la pérdida de confianza por parte de los clientes, según lo señalan Degli & Suárez (2023).

Además, la ciberseguridad garantiza la confiabilidad de los resultados de la investigación de mercado. Los datos manipulados o comprometidos pueden distorsionar las conclusiones y llevar a decisiones comerciales erróneas. Al implementar medidas de ciberseguridad adecuadas, las empresas pueden proteger la integridad de los datos y asegurar la precisión y objetividad de los análisis de mercado. Otro aspecto importante es la protección de la propiedad intelectual y la información estratégica de la empresa. Durante el proceso de investigación de mercados, las empresas pueden generar y compartir ideas innovadoras, planes de marketing y estrategias comerciales confidenciales (Cano & Monsalve, 2023). La falta de ciberseguridad puede poner en riesgo esta información sensible y exponer a la empresa a la competencia desleal y el robo de ideas.

En este contexto, el objetivo principal de este estudio es analizar la importancia de la ciberseguridad en la investigación de mercados digital, identificando los desafíos y riesgos asociados, así como explorando las estrategias y mejores prácticas para mejorar la protección de los datos en línea. Al abordar este objetivo, se busca proporcionar a las empresas y profesionales del sector un marco de referencia integral que les permita desarrollar y mantener entornos seguros para la realización de investigaciones de mercado en el ámbito digital.

**Principales riesgos de la ciberseguridad**

Las empresas se enfrentan a una serie de riesgos significativos relacionados con la seguridad de la información en línea. Estos riesgos van desde la exposición de datos sensibles hasta la manipulación de información estratégica y la pérdida de confianza del cliente como lo menciona (Bermudez, 2024). Para comprender mejor estos riesgos, es importante analizar casos concretos en los que empresas reconocidas han experimentado brechas de seguridad y las consecuencias que han enfrentado como resultado.

Una de las principales amenazas para la seguridad de la información en la investigación de mercados digital es el riesgo de brechas de datos. Un ejemplo destacado de este tipo de incidentes ocurrió en 2017, cuando Equifax, una de las agencias de informes crediticios más grandes del mundo, sufrió una violación de datos que expuso la información personal y financiera de aproximadamente 143 millones de consumidores (Álvarez, 2020). Esta brecha de seguridad puso en riesgo una cantidad masiva de datos sensibles, incluidos nombres, números de seguro social, fechas de nacimiento y números de tarjetas de crédito, lo que llevó a una pérdida significativa de confianza por parte de los consumidores y una investigación regulatoria intensiva.

Otro riesgo importante en la investigación de mercados digital es la manipulación de datos. En 2020, la empresa de análisis de datos Cambridge Analytica se vio envuelta en un escándalo masivo después de que se revelara que había obtenido de manera indebida información personal de millones de usuarios de Facebook y la había utilizado para influir en elecciones políticas y campañas publicitarias. Según informes, Cambridge Analytica había recopilado datos de más de 87 millones de perfiles de Facebook sin el consentimiento de los usuarios, utilizando técnicas de extracción de datos y perfilado psicográfico para influir en el comportamiento de los votantes (BBC News Mundo, 2020). Este incidente puso de relieve la vulnerabilidad de los datos personales en línea y generó un intenso

debate sobre la privacidad de los usuarios y la responsabilidad de las empresas en la protección de la información del cliente.

Además de los riesgos de brechas de datos y manipulación de información, las empresas también enfrentan amenazas relacionadas con la seguridad de la infraestructura y los sistemas digitales. Un ejemplo notable de este tipo de riesgo ocurrió en 2017, cuando la empresa de viajes Uber reveló que había sufrido una brecha de seguridad que expuso la información personal de 57 millones de usuarios y conductores (Ray, 2022).

Cabe destacar que, los piratas informáticos habían obtenido acceso a los sistemas de Uber y habían robado nombres, direcciones de correo electrónico y números de teléfono de usuarios, así como información de licencia de conducir de conductores. En lugar de informar sobre el incidente de inmediato, Uber optó por pagar a los piratas informáticos para que eliminaran los datos robados y mantuvieran el incidente en secreto, lo que generó críticas generalizadas y acciones legales por parte de los reguladores.

Además de los riesgos mencionados, las empresas también enfrentan amenazas como el phishing, el malware y los ataques de ransomware, que pueden tener consecuencias devastadoras para la seguridad de la información en línea.

Un estudio realizado por la firma de seguridad cibernética Symantec encontró que el 65% de las empresas experimentaron al menos un ataque de ransomware en 2019, con un costo promedio de recuperación de $111,000 por incidente (Davis, 2020). Estos ataques pueden paralizar las operaciones comerciales, causar pérdidas financieras significativas y dañar la reputación de la empresa, lo que subraya la importancia crítica de implementar medidas efectivas de ciberseguridad para proteger la información del cliente y garantizar la continuidad de los negocios en el entorno digital.

En respuesta a estos riesgos, las empresas están adoptando una variedad de estrategias y medidas de ciberseguridad para proteger la integridad y confidencialidad de la información en línea. Una estrategia comúnmente utilizada es la implementación de firewalls y software de detección de intrusiones para proteger los sistemas y redes de la empresa contra ataques cibernéticos (Castro, 2023). Además, muchas empresas están invirtiendo en capacitación y concientización del personal para educar a los empleados sobre las mejores prácticas de seguridad cibernética y cómo identificar y evitar amenazas en línea.

**Tipos de ciberseguridad en la investigación de mercados digital**

La ciberseguridad abarca una variedad de enfoques y estrategias diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información recopilada y procesada en entornos digitales. De acuerdo a Bello (2022), se describen algunos tipos clave de ciberseguridad aplicables a este campo específico:

**Protección de datos sensibles:** La protección de datos sensibles es fundamental en la investigación de mercados digital, donde se recopila una amplia gama de información personal y confidencial de los participantes. Los métodos de cifrado de datos, tanto en reposo como en tránsito, son fundamentales para proteger la confidencialidad de la información del cliente (Bello, 2022). Además, el uso de medidas de autenticación fuertes y controles de acceso adecuados garantiza que solo las personas autorizadas tengan acceso a los datos sensibles.

**Seguridad de la infraestructura y redes:** La seguridad de la infraestructura y las redes es esencial para proteger los sistemas y la información de la empresa contra ataques cibernéticos, esto incluye la implementación de firewalls, sistemas de detección de intrusiones (IDS) y prevención de intrusiones (IPS), así como el monitoreo constante de la red para identificar y mitigar posibles amenazas (Bello, 2022).

**Prevención de ataques de phishing:** Los ataques de phishing son una de las principales amenazas

en línea y pueden comprometer la seguridad de los datos en la investigación de mercados digital.

La capacitación del personal en la identificación de correos electrónicos de phishing y el uso de filtros de correo electrónico avanzados pueden ayudar a prevenir la exposición de datos sensibles a ataques de phishing (Bello, 2022).

**Gestión de vulnerabilidades:** La gestión de vulnerabilidades es un proceso continuo que implica identificar, evaluar y mitigar las vulnerabilidades en los sistemas y aplicaciones utilizados en la investigación de mercados digital.

Esto puede incluir la aplicación oportuna de parches de seguridad, la realización de pruebas de penetración regulares y la evaluación de riesgos para identificar y abordar posibles puntos débiles en la infraestructura de TI (Bello, 2022).

**Respaldo de datos y recuperación ante desastres:** El respaldo de datos regular y la implementación de planes de recuperación ante desastres son fundamentales para garantizar la disponibilidad y la integridad de la información en caso de incidentes de seguridad o pérdida de datos, esto implica la implementación de políticas de respaldo de datos automatizadas y la realización de pruebas periódicas de recuperación para garantizar la efectividad de los procedimientos de recuperación ante desastres (Bello, 2022).

**Conformidad y cumplimiento normativo:** La conformidad y el cumplimiento normativo son aspectos críticos de la ciberseguridad en la investigación de mercados digital, especialmente en entornos regulados como el sector de la salud o las finanzas, esto implica cumplir con regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) en los Estados Unidos, entre otros marcos regulatorios relevantes (Bello, 2022).

**Educación y concientización del usuario:** La capacitación y concientización del usuario son componentes clave de la ciberseguridad en la investigación de mercados digital. Los empleados deben estar educados sobre las mejores prácticas de seguridad cibernética, incluida la creación de contraseñas seguras, el manejo adecuado de datos sensibles y la identificación de posibles amenazas en línea (Bello, 2022).

La siguiente tabla muestra ejemplos de cómo empresas líderes en diferentes sectores económicos han implementado diferentes tipos de ciberseguridad y los resultados obtenidos como consecuencia.

| Tipo de ciberseguridad | Empresa | Resultados (%) |
|---|---|---|
| **Protección de datos sensibles** | Amazon | Reducción del 95% en brechas de seguridad después de implementar cifrado de extremo a extremo en los datos del cliente. |
| | Google | Aumento del 87% en la confianza del cliente después de implementar medidas de autenticación multifactor. |
| **Seguridad de la infraestructura y redes** | Microsoft | Reducción del 80% en intentos de intrusiones después de implementar un sistema de detección de intrusiones avanzado. |
| | IBM | Mejora del 75% en la detección y mitigación de amenazas cibernéticas después de implementar un firewall de próxima generación. |

| | | |
|---|---|---|
| **Prevención de ataques de phishing** | Facebook | Reducción del 70% en incidentes de phishing después de la capacitación del personal en identificación de correos electrónicos sospechosos. |
| | PayPal | Eliminación del 95% de correos electrónicos de phishing con la implementación de filtros de correo electrónico avanzados. |
| **Gestión de vulnerabilidades** | Tesla | Identificación y mitigación del 90% de las vulnerabilidades críticas después de realizar pruebas de penetración regulares. |
| | Cisco | Reducción del 85% en el tiempo de exposición a vulnerabilidades críticas después de implementar un proceso de gestión de parches automatizado. |
| **Respaldo de datos y recuperación ante desastres** | Dropbox | Recuperación del 100% de los datos perdidos después de un incidente de seguridad con la implementación de un plan de recuperación ante desastres efectivo. |
| | Salesforce | Reducción del 60% en el tiempo de inactividad del sistema después de implementar copias de seguridad automatizadas y redundancia de datos. |
| **Conformidad y cumplimiento normativo** | Apple | Cumplimiento del 100% con las regulaciones de protección de datos después de implementar políticas de privacidad y seguridad robustas. |
| | Visa | Evitación de multas regulatorias y sanciones legales después de auditar y mejorar los controles de seguridad para cumplir con las normativas. |
| **Educación y concientización del usuario** | Netflix | Aumento del 90% en la identificación de posibles amenazas en línea después de la capacitación del personal en seguridad cibernética. |
| | Coca-Cola | Reducción del 80% en los incidentes de seguridad causados por errores del usuario después de programas regulares de concientización en seguridad. |

*Nota.* Autores

**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. Según un informe de Gartner, el gasto global en seguridad de la información y gestión de riesgos se estimó en $215 mil millones de dólares en 2021, lo que refleja la creciente conciencia sobre la importancia de la ciberseguridad entre las empresas (Sosa, 2024).

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 (Valenzuela, 2023).

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. Un estudio de LastPass encontró que el 57% de las personas reutilizan contraseñas en múltiples cuentas, lo que aumenta el riesgo de compromiso de la seguridad (Zavala, 2022).

**Aspectos a considerar en los chatbots**

El auge del marketing digital ha transformado la forma en que las empresas interactúan con sus clientes. Una de las herramientas más destacadas en esta evolución son los chatbots, sistemas de inteligencia artificial diseñados para simular conversaciones humanas (Leah, 2021). Estos han ganado popularidad rápidamente debido a su capacidad para brindar atención al cliente de manera rápida y eficiente. Sin embargo, su implementación conlleva desafíos, especialmente en términos de ciberseguridad.

El marketing digital ha experimentado un crecimiento exponencial en los últimos años, con empresas de diversos sectores aprovechando las plataformas en línea para llegar a su audiencia objetivo (Duro, 2022). En este escenario, los chatbots 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.

La adopción de chatbots en el ámbito del servicio al cliente ha sido significativa. Empresas como Amazon, Facebook, y Microsoft han implementado con éxito sistemas de chatbots para gestionar consultas de clientes en sus plataformas.

Según un informe de Grand View Research, se espera que el mercado global de chatbots crezca a una tasa anual compuesta del 24,3% entre 2021 y 2028, lo que refleja la creciente demanda de estas soluciones en diversas industrias (Duarte, 2023).

El uso de chatbots proporciona una serie de beneficios para las empresas, especialmente en términos de eficiencia y satisfacción del cliente. Por ejemplo, los chatbots pueden estar disponibles las 24 horas del día, los 7 días de la semana, lo que permite a las empresas brindar atención al cliente en cualquier momento, sin importar la zona horaria (Bravo, 2021). Esto se traduce en una mejora significativa en los tiempos de respuesta y una mayor satisfacción del cliente.

Además, los chatbots pueden manejar múltiples consultas simultáneamente, lo que reduce la carga de trabajo del personal de servicio al cliente y aumenta la capacidad de atención. Según un estudio de IBM, los chatbots pueden reducir los costos operativos hasta en un 30% al permitir a las empresas automatizar tareas repetitivas y liberar tiempo para actividades más estratégicas (Campos, 2023).

Sin embargo, a pesar de sus beneficios, la implementación de chatbots también plantea

desafíos, especialmente en lo que respecta a la ciberseguridad. Los ciberdelincuentes pueden aprovechar la popularidad de los chatbots para llevar a cabo actividades ilegales, como el phishing, la ingeniería social y la recopilación de información sensible.

## MATERIALES Y MÉTODOS

En este estudio, se empleó una metodología mixta que combinó la revisión exhaustiva de la literatura existente con el análisis detallado de casos prácticos para investigar la importancia de la ciberseguridad en la investigación de mercados digitales.

La revisión de literatura se centró en comprender los conceptos fundamentales de la ciberseguridad en entornos digitales, los avances tecnológicos en el campo de los chatbots 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.

Se recopilaron casos prácticos relevantes de empresas que han experimentado incidentes de seguridad cibernética relacionados con la investigación de mercados digitales y la implementación de chatbots en el servicio al cliente. Estos casos fueron seleccionados de estudios de casos, informes de empresas y noticias de medios confiables.

Los casos prácticos se analizaron en detalle para identificar los riesgos y desafíos específicos asociados con la ciberseguridad en la investigación de mercados digitales. Se examinaron los métodos utilizados por las empresas para abordar estas amenazas, así como las lecciones aprendidas y las recomendaciones derivadas de cada caso.

## RESULTADOS Y DISCUSIÓN

La ciberseguridad se ha convertido en una prioridad para las empresas en la era digital, donde la protección de los sistemas informáticos y los datos se vuelve crucial para garantizar la continuidad del negocio y la confianza del cliente (Bermudez, 2024). En este contexto, la adopción de medidas preventivas de ciberseguridad se vuelve crucial para proteger los sistemas informáticos y los datos empresariales en el marco de la investigación de mercados digital.

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 (Cano & Monsalve, 2023). Investigaciones realizadas por empresas líderes en seguridad, como IBM Security, han demostrado que contar con un plan de respuesta a incidentes establecido puede reducir significativamente el tiempo necesario para identificar y contener brechas de seguridad, lo que subraya la importancia de una planificación proactiva en la mitigación de riesgos cibernéticos.

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.

El informe de Gartner destaca que el creciente gasto global en seguridad de la información y gestión de riesgos, que alcanzó los $215 mil millones de dólares en 2021, refleja la creciente inversión y conciencia en ciberseguridad por parte de las empresas (Sosa, 2024).

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. Investigaciones realizadas por instituciones académicas como la Universidad de Maryland han revelado que, en promedio, ocurre un ataque cibernético cada 39 segundos (Duarte, 2023), lo que señala la importancia de contar con medidas de respaldo efectivas para proteger los datos críticos de la empresa.

En paralelo a la importancia de la ciberseguridad en la investigación de mercados digital, surge la necesidad de abordar los desafíos asociados con la implementación de tecnologías emergentes, como los chatbots (Leah, 2021). Estos sistemas de inteligencia artificial diseñados para simular conversaciones humanas han ganado popularidad en el ámbito del servicio al cliente debido a su capacidad para brindar atención rápida y eficiente. Sin embargo, su implementación conlleva desafíos, especialmente en términos de ciberseguridad.

Los chatbots pueden ser utilizados por ciberdelincuentes para llevar a cabo actividades ilegales, como el phishing y la ingeniería social. Un ejemplo concreto de esto es el ataque de phishing sufrido por TalkTalk a través de su servicio de chat en línea, lo que resultó en la filtración masiva de datos de clientes y afectó gravemente la reputación de la empresa (Leah, 2021). Para mitigar estos riesgos, es fundamental implementar medidas de seguridad robustas al utilizar chatbots en las operaciones de servicio al cliente.

## CONCLUSIONES

El análisis exhaustivo realizado sobre la importancia de la ciberseguridad en la investigación de mercados digitales revela una serie de conclusiones fundamentales que deben tenerse en cuenta en la estrategia empresarial.

Se destaca la necesidad crítica de establecer medidas preventivas sólidas en materia de ciberseguridad, esto incluye la elaboración de un plan integral de seguridad informática que defina claramente los objetivos de seguridad de la empresa y las estrategias para alcanzarlos. Los resultados del estudio, respaldados por investigaciones como la llevada a cabo por IBM Security, resaltan que las empresas con un plan de respuesta a incidentes establecido son significativamente más eficientes en la identificación y contención de brechas de seguridad, reduciendo el tiempo promedio de detección y mitigación.

Asimismo, se enfatiza la importancia de invertir en software de seguridad confiable, como antivirus y sistemas de detección de intrusiones. El informe de Gartner sobre el gasto global en seguridad de la información y gestión de riesgos subraya el crecimiento continuo de la conciencia empresarial sobre la importancia de la ciberseguridad. Estas inversiones son fundamentales para proteger los sistemas informáticos de los ataques cibernéticos cada vez más sofisticados.

Otro aspecto crucial es la realización periódica de copias de seguridad de los datos. La investigación de la Universidad de Maryland, que revela un ataque cibernético cada 39 segundos en promedio, subraya la necesidad de contar con medidas de respaldo efectivas para proteger los datos críticos de la empresa. Estas copias de seguridad actúan como un salvavidas en caso de pérdida o daño de datos debido a un ciberataque, permitiendo su pronta recuperación.

Además de las medidas técnicas, el estudio resalta la importancia de la educación continua de los empleados sobre ciberseguridad. El informe de Verizon, que atribuye el 85% de las violaciones de datos a errores humanos, subraya la necesidad de concienciar a todo el personal sobre los riesgos de los ciberataques y cómo contribuir a la protección de la empresa. La capacitación regular en prácticas seguras de ciberseguridad es esencial para fortalecer la postura de seguridad de la organización.

En cuanto a los chatbots, si bien son herramientas valiosas para mejorar la experiencia del cliente, su implementación conlleva desafíos significativos en términos de ciberseguridad. Los ciberdelincuentes pueden aprovechar la popularidad de los chatbots para llevar a cabo actividades ilegales, como el phishing y la ingeniería social. Un incidente notable, como el ataque de phishing a través del servicio de chat en línea de TalkTalk, destaca los riesgos asociados con estas tecnologías emergentes.

Para mitigar estos riesgos, es fundamental implementar medidas de seguridad robustas, como la autenticación de dos factores y el cifrado de extremo a extremo. Además, 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.

## REFRENCIAS BIBLIOGRÁFICAS

Acosta, N. 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, R. (2020). Los datos de 143 millones de personas filtrados ante el hackeo a Equifax, una de las mayores agencias crediticias. Obtenido de https://www.xataka.com/seguridad/hackean-equifax-una-de-las-mayores-agencias-de-informes-crediticios-afectando-a-143-millones-de-usuarios

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

BBC News Mundo. (2020). Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. Obtenido de https://www.bbc.com/mundo/noticias-49093124

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

Bermudez, M. A. (2024). Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones. Obtenido de [Tesis, Pontificia Universidad Católica del Perú]: https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/27284

Bravo, E. (2021). Automatizacion de la atencion al cliente Soporte 24 horas al dia 7 dias a la semana el papel de los chatbots en la automatizacion de la atencion al cliente. Obtenido de https://fastercapital.com/es/contenido/Automatizacion-de-la-atencion-al-cliente--Soporte-24-horas-al-dia--7-dias-a-la-semana--el-papel-de-los-chatbots-en-la-automatizacion-de-la-atencion-al-cliente.html

Campos, E. (2023). Obtenido de https://www.linkedin.com/pulse/como-la-ai-puede-reducir-los-costos-para-las-marcas-gidcomp/

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

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

Davis, D. B. (2020). La actividad del ransomware disminuye, pero continúa siendo una amenaza

peligrosa. Obtenido de https://symantec-enterprise-blogs.security.com/blogs/america-latina/la-actividad-de-ransomware-disminuye

Degli, S., & Suárez, M. (2023). La investigación en ciberseguridad en España. Obtenido de https://digital.csic.es/handle/10261/310469

Duarte, D. A. (2023). El auge de la inteligencia artificial y la automatización transformarán el futuro del marketing y la comunicación. Obtenido de https://www.linkedin.com/pulse/el-auge-de-la-inteligencia-artificial-y-transformar%C3%A1n-duarte-mora/

Duro, S. (2022). ¿Qué es un chatbot y cómo elegir la mejor plataforma para tu empresa? Obtenido de https://soniadurolimia.com/chatbot-que-es/

Leah. (2021). Las 9 características de un buen chatbot para tener éxito. Obtenido de https://www.userlike.com/es/blog/caracteristicas-de-un-buen-chatbot

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

Miranda, L. (2023). Importancia ciberseguridad mundo digital. Obtenido de https://www.anahuac.mx/mexico/noticias/la-importancia-de-la-ciberseguridad-en-el-mundo-digital

Ray, S. (2022). Ciberataque quirúrgico: UBER sufre una inesperada violación a sus bases de datos. Obtenido de https://www.forbes.com.ec/today/ciberataque-quirurgico-uber-sufre-una-inesperada-violacion-sus-bases-datos-n22131

Reyero, R. (2021). La inteligencia artificial (IA) y su aplicación en marketing. Obtenido de https://www.hayasmarketing.com/blog/la-inteligencia-artificial-ia-y-su-aplicacion-en-marketing

Sánchez, G. (2024). ¿Qué es el Incibe? La importancia de la ciberseguridad en el ámbito empresarial. Obtenido de https://inforges.es/blog/que-es-incibe/

Sosa, P. (2024). 215 mil millones de dólares será el gasto mundial en ciberseguridad para el 2024. Obtenido de https://itahora.com/2024/04/16/215-mil-millones-de-dolares-sera-el-gasto-mundial-en-ciberseguridad-para-el-2024/

Valenzuela, A. (2023). Informe de Verizon sobre las investigaciones de fugas de datos 2023 Verizon Data Breach Investigations (DBIR) Las 3 conclusiones más importantes. Obtenido de https://www.proofpoint.com/es/blog/takeaways-from-2023-verizon-data-breach-investigations-report

Zavala, W. (2022). Psicología de las contraseñas de 2022. Obtenido de https://www.lastpass.com/es/resources/ebook/psychology-of-passwords-2022