Fecha de presentación: abril, 2024, **Fecha de Aceptación**: mayo, 2024, **Fecha de publicación**: julio, 2024

55

HABILIDADES EN CIBERSEGURIDAD: PROTEGIENDO LA INTEGRIDAD DE LAS CAMPAÑAS DIGITALES Y LA REPUTACIÓN DE LA MARCA

CYBERSECURITY SKILLS: PROTECTING THE INTEGRITY OF DIGITAL CAMPAIGNS AND BRAND REPUTATION

Geordy Tomas Pesantez Salinas[1*]
E-mail: geordy.pesantez.71@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0001-5010-6810
Diego Marcelo Cordero Guzmán[1]
E-mail: dcordero@ucacue.edu.ec
ORCID: https://orcid.org/0000-0003-2138-2522
Edwin Joselito Vásquez Erazo[1]
E-mail: evasqueze@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-9817-6773
*Autor para correspondencia
[1]Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Pesantez Salinas, G. T., Cordero Guzmán, D. M., y Vásquez Erazo, E. J., (2024). Habilidades en ciberseguridad: protegiendo la integridad de las campañas digitales y la reputación de la marca. *Revista Conrado, 20*(99), 538-548.

RESUMEN

En Ecuador, la ciberseguridad en el marketing de campañas digitales y la reputación de la marca se erigen como aspectos críticos en la era digital. La investigación tiene como objetivo desarrollar habilidades de ciberseguridad en el marketing para empresas de publicidad en Macas, Ecuador. Se empleó una metodología mixta para obtener una comprensión detallada del tema, combinando técnicas cuantitativas y cualitativas. Se resalta la importancia de contar con habilidades especializadas en ciberseguridad y gestión de la reputación digital. Los resultados muestran una diversidad en la transparencia de las prácticas de protección de datos en agencias de publicidad, destacando la necesidad de estándares claros en seguridad de la información. La falta de claridad en la comunicación sobre protección de datos entre empresas y agencias subraya la necesidad de mejorarla. Se destaca la necesidad de mejorar prácticas de seguridad y comunicación en la industria del marketing y la publicidad, lo que implica el desarrollo continuo de habilidades en ciberseguridad y gestión de la reputación digital.

Palabras clave:

Habilidades digitales, consumidor, marketing, protección de datos, gestión de riesgos.

ABSTRACT

In Ecuador, cybersecurity in digital marketing campaigns and brand reputation are critical aspects in the digital era. The research aims to develop cybersecurity marketing strategies for advertising companies in Macas, Ecuador. A mixed methodology is employed to obtain a detailed understanding of the topic, combining quantitative and qualitative techniques. The results show a diversity in the transparency of data protection practices in advertising agencies, highlighting the need for clear standards in information security. The lack of clarity in data protection communication between companies and agencies underlines the need for improvement. The importance of safeguarding, understanding and applying data security measures in business relationships. Emphasizes the need to improve security and communication practices in the marketing and advertising industry.

Keywords:

Digital skills, consumer, marketing, data protection, risk management.

INTRODUCCIÓN

En el contexto actual del marketing digital, el desarrollo de habilidades en ciberseguridad emerge como un pilar fundamental para salvaguardar la reputación global de las marcas. En un entorno donde las amenazas cibernéticas son omnipresentes, garantizar la protección de los datos y la información del cliente se convierte en una prioridad ineludible. La integración de medidas de ciberseguridad en las estrategias de marketing no solo resguarda a las empresas de potenciales ataques, sino que también fortalece la confianza con los consumidores al demostrar un compromiso con la salvaguarda de su privacidad.

El desarrollo de habilidades en ciberseguridad implica no solo comprender los conceptos básicos de protección de datos, sino también estar al tanto de las últimas tendencias y amenazas en el mundo digital. Esto incluye la capacitación en la identificación de posibles vulnerabilidades en los sistemas de información y la implementación de medidas preventivas y correctivas para mitigar los riesgos.

Además, las habilidades en ciberseguridad también abarcan la capacidad de diseñar y mantener sistemas de seguridad robustos, así como la habilidad para responder de manera efectiva ante incidentes de seguridad. Esto implica contar con conocimientos sólidos en la configuración de firewalls, el cifrado de datos, la detección de intrusiones y otras técnicas de protección cibernética.

Esto resalta la necesidad de contar con habilidades especializadas en ciberseguridad, incluyendo la capacidad para identificar vulnerabilidades, implementar soluciones de protección de datos, realizar análisis de riesgos y cumplir con regulaciones de privacidad. La competencia en la gestión proactiva de la seguridad cibernética se vuelve esencial para mitigar amenazas y proteger la integridad de las marcas en el panorama digital actual.

La aplicación de prácticas robustas de ciberseguridad en las campañas digitales permite prevenir vulnerabilidades que podrían comprometer la información confidencial de los clientes y dañar la reputación de la marca. Al priorizar la seguridad en todas las iniciativas de marketing, las empresas pueden destacarse como líderes responsables en el mercado, lo que a su vez consolida la confianza del consumidor y mejora la percepción de la marca a nivel mundial (Buffett, 2020).

En el contexto latinoamericano, la ciberseguridad en el marketing digital y la gestión de la reputación de marca han evolucionado de manera significativa en los últimos años. Las empresas han intensificado su conciencia sobre los riesgos cibernéticos y han adoptado medidas más avanzadas para proteger sus datos y reputación. Esto implica inversiones en tecnologías de seguridad, el cumplimiento de regulaciones de privacidad y la capacitación del personal (González, 2020). La relevancia de la ciberseguridad en el marketing en América Latina se acentúa debido al vertiginoso aumento del uso de tecnologías digitales en la región. Se ha observado un aumento sustancial en los ciberataques, con un incremento del 48% en los últimos dos años, lo que no solo amenaza la seguridad digital, sino que también impacta negativamente en la economía, con pérdidas estimadas en miles de millones de dólares anuales.

La región enfrenta desafíos únicos, como la falta de conciencia, infraestructura obsoleta y escasez de profesionales capacitados en la integridad de las compañas digitales. Para abordar estos problemas, es esencial que las compañías, empresas y la sociedad inviertan en medidas de ciberseguridad. Según estudios, el 70% de las empresas en marketing planean aumentar sus inversiones en ciberseguridad en los próximos dos años. Ejemplos como Hanwha Vision muestran la importancia de desarrollar tecnologías avanzadas para detectar y prevenir ciberataques, reconociendo la relevancia de la ciberseguridad en el desarrollo tecnológico de la región (Abscheidt et al., 2020).

Asimismo, se ha centrado en la concienciación, la implementación de tecnologías avanzadas, el cumplimiento normativo y la educación del personal para prevenir incidentes de seguridad y mantener la confianza del consumidor en un entorno digital cada vez más complejo (González, 2020).

En Ecuador, la ciberseguridad en el marketing de campañas digitales y la reputación de la marca se erigen como aspectos críticos en la era digital. La ejecución de estrategias de marketing digital implica el manejo de datos sensibles de los clientes, aumentando el riesgo de ciberataques y vulnerabilidades en la seguridad de la información. Proteger la integridad de los datos de los clientes, asegurar la privacidad de la información y mantener la reputación de la marca son elementos esenciales en el contexto digital ecuatoriano.

Las empresas deben estar al tanto de los riesgos cibernéticos asociados con las campañas de marketing digital y tomar medidas preventivas para mitigar las amenazas. Es crucial implementar prácticas de ciberseguridad sólidas, como el cifrado de datos, la autenticación de usuarios, la monitorización de la red y la capacitación del personal en seguridad informática. Además, es fundamental cumplir con las regulaciones locales e internacionales de protección de datos para garantizar la confianza de los clientes

y mantener la reputación de la marca intacta (Anchundia, 2017).

A partir de las evidencias previamente expuestas, surge el problema central de esta investigación: ¿Cómo proteger la información de los clientes de las empresas de publicidad en la ciudad de Macas?, se establece como objetivo desarrollar habilidades de ciberseguridad en el ámbito del marketing para las empresas de publicidad en Macas, que garantice la protección de los datos de sus clientes.

El impacto de la ciberseguridad en la experiencia del consumidor en el comercio electrónico es un tema de creciente relevancia en el panorama empresarial contemporáneo. En un entorno donde las transacciones en línea son cada vez más comunes, el resguardo de la información de los clientes se convierte en un imperativo para garantizar la confianza y la satisfacción del consumidor. La seguridad de los datos personales y financieros de los clientes es fundamental para el buen funcionamiento del comercio electrónico, ya que cualquier brecha en la seguridad puede tener repercusiones negativas tanto para los consumidores como para las empresas (Van, 2024).

La protección de la información del cliente se ha convertido en un pilar fundamental en el entorno del comercio electrónico, en un panorama donde la confianza es un activo invaluable, los consumidores están cada vez más conscientes de los riesgos asociados con la seguridad cibernética y valoran enormemente las garantías sólidas ofrecidas por las plataformas en las que realizan transacciones. La percepción de seguridad juega un papel crucial en la decisión de interactuar y comprometerse con una marca o un comercio en línea. Los consumidores se sienten más inclinados a compartir su información personal y financiera cuando confían en que está protegida de manera adecuada contra amenazas cibernéticas.

Por tanto, la implementación de medidas efectivas de ciberseguridad no solo resguarda la integridad de los datos, sino que también establecer como un factor determinante para fomentar la participación activa y la lealtad del cliente en el entorno del comercio electrónico. Las empresas que priorizan la seguridad no solo cumplen con las expectativas del consumidor moderno, sino que también se posicionan como líderes de confianza en un mercado altamente competitivo y digitalmente interconectado. En este sentido, la inversión en ciberseguridad no solo protege los activos digitales de una empresa, sino que también contribuye directamente a su crecimiento y sostenibilidad a largo plazo al fortalecer la relación con sus clientes y construir una reputación sólida en línea (Sánchez et al., 2017).

En el contexto del marketing digital, la importancia de la ciberseguridad se vuelve fundamental, las estrategias de marketing digital se basan principalmente en la recolección y utilización de los datos de los clientes, lo que los convierte en posibles blancos de ataques cibernéticos. La seguridad de estos datos resulta vital para resguardar la privacidad de los clientes y prevenir posibles infracciones que puedan afectar la confianza del consumidor y dañar la reputación de la marca. En un entorno digital cada vez más complejo y amenazante, proteger la información del cliente se convierte en una necesidad imperiosa no solo para garantizar la integridad de los datos, sino también para mantener la relación de confianza entre las marcas y sus clientes. Además, la ciberseguridad en el marketing digital puede influir en la efectividad de las estrategias de personalización y segmentación. Si los consumidores perciben que sus datos no están seguros, es menos probable que estén dispuestos a proporcionar información personal, lo que dificulta la capacidad de las empresas para ofrecer mensajes y ofertas personalizadas. Por lo tanto, la inversión en medidas de seguridad cibernética es crucial para mantener la efectividad y la relevancia del marketing personalizado en el comercio electrónico (Meraz, 2018).

El impacto económico de las vulnerabilidades de seguridad en el ámbito del comercio electrónico y el marketing digital es considerable. Las brechas en la seguridad de los datos pueden acarrear costos significativos para las empresas, incluyendo gastos de remediación, pérdida de clientes y sanciones regulatorias. Además, la reputación de la marca puede sufrir daños irreparables, lo que resulta en una disminución de la confianza del consumidor y una pérdida de ingresos a largo plazo. En este contexto, el desarrollo de habilidades en ciberseguridad se vuelve fundamental. Los profesionales del comercio electrónico y el marketing digital deben estar capacitados para identificar y mitigar riesgos de seguridad, implementar medidas de protección de datos efectivas y responder de manera rápida y eficiente ante posibles incidentes de seguridad.

Estas habilidades no solo se centran en aspectos técnicos, como la configuración de firewalls y la detección de intrusiones, sino también en aspectos estratégicos, como la elaboración de políticas de seguridad, la concienciación de los empleados y la gestión de crisis. Además, el desarrollo de competencias en ciberseguridad implica mantenerse al día con las últimas tendencias y amenazas en el campo de la seguridad cibernética.

Al adoptar un enfoque proactivo en la ciberseguridad, las empresas pueden proteger sus intereses financieros y garantizar su sostenibilidad a largo plazo en el mercado

digital. Más allá de salvaguardar la información del cliente, la ciberseguridad se convierte en un elemento crucial para preservar la reputación y la confianza del consumidor, así como para asegurar la viabilidad económica de las operaciones en línea Santiago y Sánchez, 2017.

Por lo tanto, es fundamental que las empresas inviertan en medidas de seguridad cibernética efectivas y mantengan una vigilancia constante para adaptarse a las amenazas en evolución en el panorama digital. Esto implica el desarrollo de habilidades en ciberseguridad entre los profesionales del comercio electrónico y el marketing digital.

Es esencial que estos profesionales estén capacitados para identificar y evaluar los riesgos de seguridad, implementar medidas de protección adecuadas y responder de manera efectiva ante posibles incidentes. Esto incluye no solo aspectos técnicos, como la configuración de firewalls y la detección de intrusiones, sino también aspectos estratégicos, como la elaboración de políticas de seguridad y la concienciación de los empleados.

Además, la vigilancia continua y la actualización constante de los sistemas de seguridad son fundamentales para garantizar una protección óptima contra los ataques cibernéticos. Esto implica estar al tanto de las últimas tendencias y amenazas en el campo de la seguridad cibernética, así como adaptarse rápidamente a los cambios en el panorama de riesgos.

Al desarrollar habilidades en ciberseguridad y mantener una postura proactiva frente a las amenazas cibernéticas, las empresas pueden no solo proteger la información del cliente, sino también fortalecer la confianza del consumidor en la marca. Esto contribuye a mejorar la satisfacción del cliente y a construir relaciones duraderas basadas en la confianza y la seguridad en el entorno digital del comercio electrónico y el marketing (Pstyga, 2022).

MATERIALES Y MÉTODOS

En la presente investigación se utilizó un enfoque de metodología mixta, que implica la integración de técnicas tanto cuantitativas como cualitativas dentro de un mismo estudio. Esta táctica se orienta a capitalizar las ventajas inherentes de ambas con el fin de lograr una comprensión más detallada del tema de investigación (Erazo, 2021). El enfoque mixto permite una exploración más amplia y diversa de los datos, así como la triangulación de resultados, lo que proporciona una visión holística del problema de investigación. Se emplean diversas estrategias, como la recolección simultánea o secuencial de datos y la combinación de resultados, para integrar los enfoques. Esto conduce a una comprensión más rica del fenómeno estudiado y enriquece la investigación al proporcionar una variedad de perspectivas (Hernández y Mendoza, 2018).

Tuvo un enfoque metodológico que compone métodos, inductivo-deductivo, analítico-sintético e histórico, que favorece para obtener una comprensión completa de la investigación. El método inductivo-deductivo en la investigación combina la observación de casos particulares con la formulación de teorías generales. En el enfoque inductivo, se parte de observaciones específicas para derivar conclusiones generales, mientras que, en el deductivo, se emplean teorías generales para hacer predicciones específicas verificables. Por otro lado, el método analítico-sintético implica descomponer un objeto de estudio en sus componentes individuales para analizarlos y luego integrarlos para obtener una visión global. El método histórico se basa en el estudio de eventos pasados para comprender el desarrollo de fenómenos, procesos o sociedades a lo largo del tiempo, utilizando fuentes históricas para identificar patrones y conexiones con el presente.

En el diseño de investigación de metodología no experimental se distingue por la ausencia de manipulación deliberada de variables independientes, permitiendo al investigador observar y recopilar datos sin intervenir en la situación estudiada. Se centran en la observación, descripción y correlación de fenómenos tal como se presentan en su entorno natural. Ejemplos de estos diseños incluyen estudios descriptivos, correlacionales, de caso, transversales y longitudinales, los cuales posibilitan la exploración de relaciones entre variables, la descripción de características de una población o fenómeno, y el análisis de tendencias a lo largo del tiempo sin intervención directa en la situación estudiada Morán y Alvarado, 2010.

Además, se usó los niveles o tipos de la investigación aplicada de campo, estas actividades son esenciales en esta investigación, ya que se enfocan en la implementación práctica de teorías a través de encuestas dirigidas a un grupo específico de personas. La investigación aplicada en encuestas abarca una variedad de enfoques metodológicos utilizados para recopilar datos de manera sistemática y obtener información relevante sobre opiniones. Estos tipos de investigación están diseñados para cumplir objetivos específicos, como analizar el mercado o comprender fenómenos sociales. La elección del tipo de encuesta se basa en los objetivos de investigación y en el público objetivo al que se dirige el estudio. Mientras que la de campo se centra en resolver problemas prácticos y crear soluciones concretas en contextos reales. Este enfoque implica intervenir directamente en el terreno de estudio, colaborando estrechamente entre investigadores,

profesionales y miembros de la comunidad. Su objetivo es aplicar los hallazgos de investigación para mejorar la calidad de vida y promover cambios positivos en la comunidad (Cordero et al., 2023).

Así mismo se usó la modalidad de campo implica la recopilación directa de datos en el entorno natural de los fenómenos estudiados, en contraposición a la investigación de laboratorio. Se observan y analizan los eventos tal como ocurren en la realidad, sin manipulación deliberada de variables. Se emplean técnicas como observación participante, entrevistas y cuestionarios para obtener una comprensión profunda y contextualizada de los fenómenos (Gandía et al., 2017).

RESULTADOS Y DISCUSIÓN

A continuación, se exponen los resultados obtenidos del cuestionario aplicado a través de un formulario digital de Google Forms, el cual fue distribuido entre 96 participantes que representan a clientes de empresas de publicidad en la ciudad de Macas, Ecuador. El método de muestreo utilizado fue el de conveniencia, seleccionando a los participantes según su disponibilidad y accesibilidad para garantizar una muestra representativa. Posteriormente, los datos recopilados fueron analizados y procesados utilizando el software Jeffreys´s Amazing Statistics Program (JASP), una herramienta confiable desarrollada por la universidad de Ámsterdam. La Tabla 1 muestra los resultados de la correlación entre las variables de investigación sobre las evaluaciones periódicas de riesgos de seguridad de la información por parte de las agencias de publicidad o proveedores de servicios de marketing, y la recepción de información detallada sobre cómo se protegen los datos de los clientes.

Tabla 1. Correlación de las variables de investigación.

Habilidades Ciberseguridad						
Protección de datos de sus clientes	A veces	No tiene servicio de proveedores de marketing	Nunca	Raramente	Sí, regularmente	Total
En cierta medida	20	0	2	11	9	42
No estoy seguro/a	6	1	4	12	2	25
No, no se ha proporcionado información al respecto	1	0	7	5	1	14
Sí, de manera exhaustiva	7	0	0	1	6	14
Total	34	1	13	29	18	95

Fuente: Elaboración de autores

La tabla muestra la correlación de las variables dependiente e independiente de la investigación.

Se observa que la mayoría de las empresas encuestadas indican que en cierta medida reciben información sobre la protección de datos, mientras que un porcentaje significativo se muestra indeciso al respecto. Por otro lado, un número considerable de empresas (14%) afirman no haber recibido información alguna sobre este tema. Es primordial notar que solo una minoría indica recibir información exhaustiva sobre la protección de datos. Estos resultados sugieren que existe una diversidad de experiencias en cuanto a la transparencia y la rigurosidad en la protección de datos por parte de las agencias de publicidad o proveedores de servicios de marketing, lo que subraya la necesidad de establecer estándares claros y prácticas sólidas en la gestión de la seguridad de la información en la industria.

A continuación, en la Tabla 2 presenta las proporciones contrastadas de la variable seguridad en relación con la experiencia de brechas de seguridad relacionadas con la información de los clientes durante la colaboración con agencias de publicidad o proveedores de servicios de marketing.

Tabla 2. Proporciones contrastadas de la variable seguridad.

Variable	Nivel	Recuentos	Total	Proporción	p
Seguridad relacionada con la información de sus clientes	En una ocasión	31	96	0.323	< .001
	No estoy seguro/a	33	96	0.344	0.003
	No, nunca hemos experimentado una brecha de seguridad	22	96	0.229	< .001
	Sí, en más de una ocasión	10	96	0.104	< .001
Nota. Proporciones contrastadas en relación al valor: 0.5.					

Fuente: Elaboración de autores

Un porcentaje significativo indica que nunca han experimentado una brecha de seguridad (22.9%), mientras que un número menor admite haber experimentado brechas de seguridad en más de una ocasión (10.4%). Estos resultados sugieren que, aunque hay una proporción considerable de empresas que no han experimentado brechas de seguridad, existe una preocupante cantidad que sí lo ha hecho, lo que resalta la importancia de mejorar las medidas de seguridad y la gestión de riesgos en las colaboraciones con agencias de publicidad y proveedores de servicios de marketing.

Los resultados revelan que la mayoría de las empresas encuestadas indican haber recibido información en cierta medida sobre cómo las empresas de publicidad protegen los datos de sus clientes y las estrategias de marketing, a continuación, se presenta la Tabla 3 donde se analiza y se indica la protección de datos de clientes en las empresas de publicidad.

Tabla 3. Porcentajes de Frecuencias.

Protección de los datos	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No estoy seguro/a	29	30.21	30.21	30.21
No, en absoluto	12	12.50	12.50	42.71
Sí, de manera exhaustiva	11	11.46	11.46	54.17
Sí, en cierta medida	44	45.83	45.83	100.00
Ausente	0	0.00		
Total	96	100.00		

Fuente: Elaboración de autores

Las empresas encuestadas indican haber recibido información en cierta medida sobre cómo las empresas de publicidad protegen los datos de sus clientes y las estrategias de marketing. Solo una pequeña fracción (11.46%) reporta haber recibido información de manera exhaustiva. Estos hallazgos sugieren una falta de claridad y transparencia en la comunicación entre las empresas contratantes y las empresas de publicidad. Es crucial que las empresas de publicidad mejoren sus esfuerzos de comunicación para proporcionar información clara y exhaustiva sobre cómo protegen los datos de los clientes y sus estrategias de marketing, lo que contribuirá a fortalecer la confianza y la colaboración entre ambas partes.

El análisis del chi-cuadrado para las variables habilidades en Ciberseguridad y protección de los datos de los usuarios arroja los siguientes resultados:

- Valor de chi-cuadrado **(X^2)**: 24.894
- Grados de libertad (gl): 9
- Valor p: 0.035

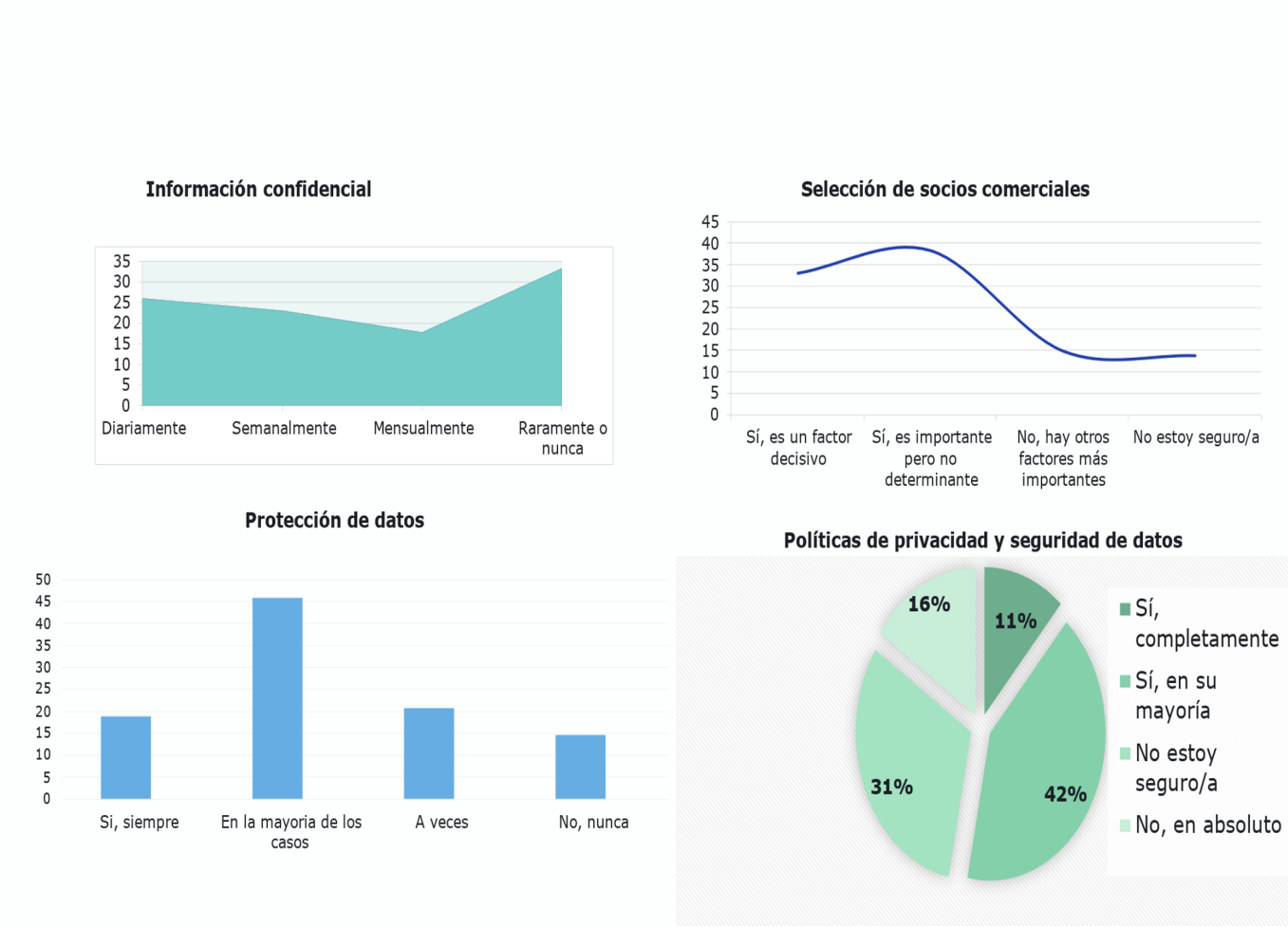
El valor de chi-cuadrado es una medida de la discrepancia que indica cuánto se desvían los datos observados de los datos esperados bajo la hipótesis nula de independencia entre las variables. Los grados de libertad (gl) en este caso son 9. Los grados de libertad se calculan restando 1 del producto del número de categorías menos 1 para cada variable. El valor p es la probabilidad de observar un valor de chi-cuadrado igual o más extremo que el valor observado, bajo la hipótesis nula de que no hay asociación entre las variables. En este caso, el valor p es 0.035, lo que indica que

la probabilidad de obtener un valor de chi-cuadrado tan extremo o más extremo es del 3.5%, asumiendo que no hay asociación entre las habilidades en ciberseguridad y la protección de los datos de los usuarios.

Dado que el valor p es menor que un nivel de significancia típicamente utilizado, como 0.05, se concluye que hay evidencia suficiente para rechazar la hipótesis nula y afirmar que hay una asociación significativa entre las habilidades en ciberseguridad y la protección de los datos de los usuarios.

A continuación, la Figura 1 proporciona una representación gráfica clara y concisa de los resultados obtenidos de un análisis exhaustivo sobre la ciberseguridad en el marketing y el resguardo de información de los clientes de publicidad en Macas, Ecuador.

Figura 1. Dashboard de los resultados obtenidos de la variable información, protección de datos, socios comerciales y políticas de privacidad de datos.



Fuente: Elaboración de autores

En la figura se evidencia los resultados del análisis a las variables de información confidencial, protección de datos de clientes y políticas de privacidad y seguridad de datos. Según la figura 1 se observa la frecuencia de compartir información confidencial de los clientes de las empresas de publicidad en Macas, Ecuador, es preocupante que un porcentaje significativo (26.0% diariamente, 22.9% semanalmente) comparta información confidencial de clientes con frecuencia. Esto podría plantear riesgos para la seguridad de los datos. En cuanto a la protección de datos, aunque la mayoría afirma que en la mayoría de los casos se protegen los datos (45.8%), aún existe una proporción considerable (14.6%) que dice que no se protegen en absoluto.

Esto indica una posible brecha en las prácticas de protección de datos. En cuanto a la importancia del resguardo de la información de los clientes en la selección de socios comerciales: La mayoría considera importante el resguardo de información de clientes al seleccionar socios comerciales, ya sea como factor decisivo (33.3%) o importante pero no determinante (38.3%). Esto sugiere una conciencia sobre la importancia de la seguridad de datos en las relaciones comerciales. Mientras que las políticas de privacidad y seguridad de datos de empresas de publicidad: Aunque una parte significativa está parcialmente de acuerdo con las políticas de privacidad y seguridad de datos de las empresas de publicidad, un 15.6% indica que no están de acuerdo en absoluto. Esto puede indicar preocupaciones sobre la eficacia de estas políticas.

El análisis de las variables de información confidencial, protección de datos de clientes y políticas de privacidad y seguridad de datos resalta la importancia del desarrollo de habilidades en ciberseguridad en el ámbito del marketing y la publicidad para garantizar la seguridad y confidencialidad de los datos en este contexto.

Los resultados de la investigación sobre la relación entre la transparencia, la ciberseguridad y la identidad digital en el entorno 5G elaborado por Rodríguez y Palomo (2023), proporcionan una visión integral de los desafíos y las oportunidades en este ámbito emergente y crítico. Ambos estudios destacan la importancia de la transparencia en la gestión de la seguridad de la información y en el despliegue de redes 5G. En el estudio de las agencias de publicidad, se observa una diversidad de experiencias en cuanto a la transparencia y la rigurosidad en la protección de datos, lo que subraya la necesidad de estándares claros y prácticas sólidas en la gestión de la seguridad de la información. Por otro lado, en el contexto de las redes, se señala que la implementación de estas redes requiere un entorno digital confiable, seguro y transparente, lo que sugiere que la transparencia es fundamental para garantizar la confianza en el uso de esta tecnología avanzada.

Además, ambas investigaciones señalan, la importancia de la ciberseguridad en el entorno digital. En el estudio de las agencias de publicidad, se evidencia la necesidad de mejorar las medidas de seguridad y la gestión de riesgos en las colaboraciones con estas entidades, especialmente considerando la preocupante cantidad de empresas que han experimentado brechas de seguridad relacionadas con la información de los clientes. Por otro lado, en el contexto de las redes 5G, se destaca que la determinación de la responsabilidad en este entorno involucra a diversas organizaciones que buscan establecer estándares para promover la seguridad y la automatización en los servicios conectados.

Así mismo subrayan la importancia de la identidad digital y su interrelación con la ciberseguridad y la configuración técnica del entorno digital. En el estudio de las agencias de publicidad, se señala que la falta de claridad y transparencia en la comunicación entre las empresas contratantes y las empresas de publicidad destaca la necesidad de mejorar los esfuerzos de comunicación para proporcionar información clara y exhaustiva sobre cómo se protegen los datos de los clientes y sus estrategias de marketing.

Los resultados de la investigación sobre la seguridad de la información en las PYMES de la ciudad de Milagro realizado por Zuña et al. (2019), revelan varios aspectos críticos que subrayan la importancia de la ciberseguridad en el entorno empresarial actual. En los dos estudios, se observan un gran número de pequeñas empresas son vulnerables a ciberataques, lo que pone de manifiesto la urgencia de implementar medidas sólidas de ciberseguridad. Esto se refleja en los resultados de la Tabla 1, donde se muestra que solo una minoría de las empresas encuestadas reciben información exhaustiva sobre cómo se protegen los datos de los clientes por parte de agencias de publicidad o proveedores de servicios de marketing. Esta falta de claridad y transparencia en la gestión de la seguridad de la información sugiere una vulnerabilidad generalizada que necesita ser abordada.

De igual manera ambas investigaciones, identifican que las empresas en constante cambio, como las de la industria y la agricultura en Milagro, son objeto de interés por parte de multinacionales debido a la oportunidad de promover productos tecnológicos y mejorar la seguridad de la información. Estos hallazgos, derivados de la Tabla 2, señalan la necesidad de que las PYMES en estas industrias sean especialmente proactivas en la implementación de medidas de seguridad cibernética, dada la naturaleza cambiante y globalizada de su entorno empresarial. También se evidencia que las PYMES enfrentan desafíos significativos en ciberseguridad, como ataques de phishing y malware. Esto es coherente con los resultados presentados en la Tabla 2, donde se muestra que un porcentaje considerable de empresas ha experimentado brechas de seguridad relacionadas con la información de los clientes durante su colaboración con agencias de publicidad o proveedores de servicios de marketing.

Se destaca que la ciberseguridad es un tema emergente y crucial para las empresas, tanto grandes como pequeñas, a nivel mundial. La Tabla 3 muestra que hay una falta de claridad y transparencia en la comunicación entre las

empresas contratantes y las empresas de publicidad en lo que respecta a la protección de datos de clientes y estrategias de marketing. Esto sugiere que muchas empresas, tanto grandes como pequeñas, podrían estar en riesgo de sufrir pérdidas económicas significativas debido a la falta de atención a la ciberseguridad.

El análisis de la presente investigación, ofrecen una perspectiva esclarecedora sobre la relación entre las prácticas de seguridad de la información en el ámbito del marketing y la experiencia de las empresas en cuanto a brechas de seguridad. En ambos estudios, se destaca la diversidad de experiencias reportadas por las empresas encuestadas en relación con la transparencia y la rigurosidad en la protección de datos por parte de las agencias de publicidad o proveedores de servicios de marketing. Aunque una proporción considerable indica recibir información en cierta medida sobre cómo se protegen los datos de los clientes, un porcentaje significativo se muestra indeciso al respecto, y otro grupo considerable afirma no haber recibido información alguna. Solo una minoría reporta recibir información de manera exhaustiva. Este panorama subraya la necesidad de establecer estándares claros y prácticas sólidas en la gestión de la seguridad de la información en la industria del marketing.

Por otro lado, los resultados también revelan la incidencia de brechas de seguridad relacionadas con la información de los clientes durante la colaboración con agencias de publicidad o proveedores de servicios de marketing. Aunque una proporción considerable de empresas indica nunca haber experimentado una brecha de seguridad, existe una preocupante cantidad que sí lo ha hecho. Estos hallazgos resaltan la importancia de mejorar las medidas de seguridad y la gestión de riesgos en las colaboraciones con agencias de publicidad y proveedores de servicios de marketing para garantizar la protección adecuada de los datos de los clientes.

Relacionando estos resultados con la noción de actividades de marketing socialmente responsables, se puede inferir que la transparencia y la eficacia en la protección de datos de los clientes pueden ser consideradas como prácticas socialmente responsables dentro del ámbito del marketing. La falta de claridad y transparencia en la comunicación entre las empresas contratantes y las empresas de publicidad, como se evidencia en los resultados, puede plantear un desafío para la legitimidad y la reputación de los departamentos de marketing. Sin embargo, la implementación de prácticas de seguridad de la información robustas y transparentes puede contribuir a mejorar la percepción de responsabilidad social de estos departamentos y, en última instancia, fortalecer la confianza y la colaboración entre las empresas contratantes y los proveedores de servicios de marketing.

Los hallazgos en ciberseguridad, donde se destaca la efectividad de las herramientas de detección y respuesta implementadas. Se observó que las tasas de detección y respuesta exitosas para diferentes tipos de amenazas fueron altas, lo que refleja la eficacia del sistema de ciberseguridad en identificar y mitigar amenazas de manera efectiva. Esto resalta la importancia de contar con medidas sólidas para proteger sistemas y datos contra diversas amenazas cibernéticas, especialmente en un entorno digital en constante evolución.

Los resultados de la investigación resaltan la importancia de los factores protectores para desarrollar habilidades cognitivas contra ciberataques, como se evidenció a través del uso del coeficiente de Pearson para validar la correlación entre ciberataques, teleeducación, teletrabajo y factores psicológicos elaborado por Zakiyah et al. (2023), se encontró una correlación positiva significativa entre el uso de Internet y los ciberataques, así como entre los factores psicológicos, los ciberataques y la vulnerabilidad del sistema. Estos hallazgos sugieren una influencia directa de los factores psicológicos en los ciberataques y la vulnerabilidad del sistema.

Sin embargo, en ambos casos se observa una correlación positiva entre el tiempo dedicado a Internet y el impacto en los factores psicológicos, lo que sugiere una relación directa entre estos elementos y el aumento de los ciberataques. Los cambios en el estilo de vida impulsados por la pandemia, como el teletrabajo y las compras en línea, han ampliado la propagación de los ciberataques. Estos hallazgos resaltan la importancia de considerar los factores humanos y psicológicos en la prevención y mitigación de ciberataques, así como la necesidad de fortalecer los procesos cognitivos de las personas para detectar y responder a las amenazas cibernéticas de manera más efectiva.

Así mismo, ambas investigaciones señalan los resultados de la investigación sobre las evaluaciones periódicas de riesgos de seguridad de la información por parte de las agencias de publicidad o proveedores de servicios de marketing, junto con la recepción de información detallada sobre cómo se protegen los datos de los clientes, subrayan la necesidad de establecer estándares claros y prácticas sólidas en la gestión de la seguridad de la información en la industria. La falta de transparencia y claridad en la comunicación entre las empresas contratantes y las empresas de publicidad destaca la importancia de mejorar los esfuerzos de comunicación para fortalecer la

confianza y la colaboración entre ambas partes en el ámbito de la seguridad de la información.

CONCLUSIONES

La variedad de respuestas en la encuesta refleja una diversidad de experiencias en cuanto a la transparencia y la rigurosidad en la protección de datos por parte de las agencias de publicidad o proveedores de servicios de marketing. Esta diversidad resalta la necesidad de establecer estándares claros y prácticas sólidas en la gestión de la seguridad de la información en la industria. El análisis del chi-cuadrado sugiere una asociación significativa entre las habilidades en ciberseguridad y la protección de datos, lo que respalda la importancia de establecer prácticas sólidas en este sentido.

La existencia de una proporción considerable de empresas que han experimentado brechas de seguridad destaca la importancia de mejorar las medidas de seguridad y la gestión de riesgos en las colaboraciones con agencias de publicidad y proveedores de servicios de marketing, mediante el desarrollo de habilidades en Ciberseguridad.

Los resultados revelan una falta de claridad y transparencia en la comunicación entre las empresas contratantes y las empresas de publicidad respecto a cómo protegen los datos de los clientes y ejecutan sus estrategias de marketing. La inclusión de habilidades en ciberseguridad en esta dinámica puede ser crucial para mejorar la transparencia y la confianza en estas comunicaciones. La falta de competencia en ciberseguridad puede obstaculizar la capacidad de las empresas de publicidad para comunicar eficazmente sus prácticas de protección de datos y estrategias de marketing, lo que destaca la necesidad de un enfoque más robusto en este aspecto para fortalecer la confianza y la colaboración entre ambas partes.

La conciencia generalizada sobre la importancia del resguardo de información de clientes al seleccionar socios comerciales se refleja en los resultados del análisis del chi-cuadrado, que indican una asociación significativa entre las habilidades en ciberseguridad y la protección de datos de los usuarios. Esto subraya la necesidad de mejorar las prácticas de seguridad de datos y la gestión de riesgos en la industria del marketing y la publicidad para garantizar la protección de la información confidencial de los clientes.

REFERENCIAS BIBLIOGRÁFICAS

Abscheidt, A., Melo, R., Lopéz, U., & Ortiz, F. (2020). ***La importancia de la ciberseguridad en latinoamérica***. Hanwha Vision.

Anchundia, C. (2017). Ciberseguridad en los sistemas informaticos de las universidades. ***Dominio de las ciencias, 3***(3), 200-217. https://dialnet.unirioja.es/descarga/articulo/6102849.pdf

Buffett, W. (2020). ***Reputación y ciberseguridad: del riesgo a la oportunidad, y el ciberorgullo***. Kaspersky. https://media.kaspersky.com/latam/KES_Cloud_Marketing_Whitepaper_Customer_0220_es_MX.pdf

Cordero, D., Erazo, J., & Bermeo, K. (2023). Calidad del servicio en organizaciones proveedoras de internet desde la perspectiva de estudiantes de los diferentes niveles educativos. ***Revista Conrado, 19***(90), 83-91. https://conrado.ucf.edu.cu/index.php/conrado/article/view/2870

Erazo, J. C. (2021). Capital intelectual y gestión de innovación: Pequeñas y medianas empresas de cuero y calzado en Tungurahua–Ecuador. ***Revista De Ciencias Sociales, 27***, 230-245. https://www.produccioncientificaluz.org/index.php/rcs/article/view

Gandía, C., Vegara, G., Lisdero, P., Quattrini , D., & Cena, R. (2017). ***Metodología de la investigación estrategias de indagación***. Buenos Aires: Estudios Sociológicos Editora.

González, J. (2020). ***Innovación en ciberseguridad estrategias y tendencias***. https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/JUAN%20GONZ%C3%81LEZ%20MART%C3%8DNEZ.pdf

Hernández, R., & Mendoza, C. (2018). ***Metodología de la investigación las rutas cuantitativas, cualitativa y mixta***. Mc Graw Hill Education,

Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. ***IUS. Ciencias Jurídicas de Puebla, 12***(41), 293-310. https://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf

Morán, G., & Alvarado, D. (2010). ***Métodos de investigación***. Pearson.

Pstyga, N. (2 2022). Latino. Ciberseguridad: todos podemos ser víctimas. https://iqlatino.org/ciberseguridad-todos-podemos-ser-victimas/?gad_source=1&gclid=CjwKCAjw48vBhBbEiwAzqrZVA7ml23U1PbBGdk3k0YvKf56NhqUt4p2MMfxJRd41MaiHvxe8NDqmhoC_ZIQAvD_BwE

Rodríguez, C. y Palomo, R. (2023). Trasparencia, ciberseguridad e identidad digital en el entorno 5G. ***Española de la Trasparencia, 18***, 359-380. https://doi.org/10.51915/ret.298

Sánchez, A., James, A., Montoya, R., y Luz, A. (2017). La confianza como elemento fundamental en las compras a través de canales de comercio electrónico. ***Innovar Journal, 27***(64), 11-22. https://www.redalyc.org/pdf/818/81850404002.pdf

Santiago, E. y Sánchez, J. (2017). Riesgos de ciberseguridad en las empresas. ***Ciencia, Tecnología y Medio Ambiente, 15***, 5-33. https://revistas.uax.es/index.php/tec_des/article/download/1174/964

Van, K. (2024). ***Beneficios del comercio electrónico***. https://www.statista.com/topics/871/online-shopping/#topicOverview

Zakiyah, Z., Ikhsan, I., y Farid. (2023). Entrepreneurial marketing and marketing performance through digital marketing capabilities of SMEs in post-pandemic recovery. ***Cogent Business & Management, 10***(2). https://www.tandfonline.com/doi/full/10.1080/23311975.2023.2204592

Zuña, E., Arce, Á., Romero, W., y Soledispa, C. (2019). Análisis de la seguridad de la información en las Pymes de la Cuidad de Milagro. ***Universidad y Sociedad***, ***11***(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202019000400487