Dom. Cien., ISSN: 2477-8818
Vol. 9, núm. 4. Octubre-Diciembre, 2023, pp. 388-402

DOI: https://doi.org/10.23857/dc.v9i4.3597

Ciencias Económicas y Empresariales
Artículo de Investigación

Ciberseguridad en pymes: caso de estudio en Cayambe

Cybersecurity in SMEs: case study in Cayambe

Cibersegurança nas PME: estudo de caso em Cayambe

Fabián Fernando Bautista-Chimarro [I]
fabian.bautista@intsuperior.edu.ec
https://orcid.org/0009-0008-4633-4328

Alba Elizabeth Flores-Ruiz [II]
alba.flores@intsuperior.edu.ec
https://orcid.org/0009-0008-4074-051X

Ramiro Gustavo Aguirre-Inga [III]
ramiro.aguirre@intsuperior.edu.ec
https://orcid.org/0000-0001-8538-4178

Correspondencia: alba.flores@intsuperior.edu.ec

*Recibido: 02 de agosto de 2023 *Aceptado: 15 de septiembre de 2023 * Publicado: 27 de septiembre de 2023

I. Instituto Superior Tecnológico Nelson Torres, Ecuador.
II. Instituto Superior Tecnológico Nelson Torres, Ecuador.
III. Instituto Superior Tecnológico Nelson Torres, Ecuador.

Resumen

La presente investigación tiene como objetivo general analizar el estado de la ciberseguridad en las Pymes del cantón Cayambe mediante una investigación primaria para el conocimiento del manejo de información privada. El proceso metodológico del estudio es cualitativo, de tipo bibliográfico, documental, experimental; se utilizó un enfoque cuantitativo y una encuesta para recopilar información sobre los riesgos de ciberseguridad y las metodologías de análisis de riesgo existentes aplicadas en las pymes. En el contexto de las pymes, se destaca que estas empresas dependen cada vez más de la tecnología y corren el riesgo de sufrir ciberataques que pueden causar grandes pérdidas financieras y de reputación. Los resultados del estudio revelaron que la mayoría de las pymes en Cayambe no tienen una buena protección cibernética. Se resalta la necesidad de implementar medidas de seguridad adecuadas y promover la conciencia sobre la importancia de la protección cibernética en las pymes.

Palabras Claves: Ciberseguridad; Ciberdelitos; Pymes.

Abstract

The general objective of this research is to analyze the state of cybersecurity in SMEs in the Cayambe canton through primary research to understand the management of private information. The methodological process of the study is qualitative, bibliographic, documentary, experimental; A quantitative approach and survey were used to collect information on cybersecurity risks and existing risk analysis methodologies applied in SMEs. In the context of SMEs, it is highlighted that these companies are increasingly dependent on technology and are at risk of cyberattacks that can cause large financial and reputational losses. The results of the study revealed that the majority of SMEs in Cayambe do not have good cyber protection. The need to implement adequate security measures and promote awareness about the importance of cyber protection in SMEs is highlighted..

Keywords: Cybersecurity; Cybercrimes; SMEs.

Resumo

O objetivo geral desta pesquisa é analisar o estado da segurança cibernética nas PME do cantão de Cayambe através de pesquisas primárias para compreender a gestão da informação privada. O processo metodológico do estudo é qualitativo, bibliográfico, documental, experimental; Foram

utilizadas uma abordagem quantitativa e um inquérito para recolher informações sobre os riscos de cibersegurança e as metodologias de análise de risco existentes aplicadas nas PME. No contexto das PME, destaca-se que estas empresas estão cada vez mais dependentes da tecnologia e correm o risco de ataques cibernéticos que podem causar grandes perdas financeiras e reputacionais. Os resultados do estudo revelaram que a maioria das PME em Cayambe não dispõe de uma boa protecção cibernética. É destacada a necessidade de implementar medidas de segurança adequadas e promover a sensibilização sobre a importância da ciberproteção nas PME.

Palavras-chave: Cíber segurança; Crimes cibernéticos; PME.

Introducción

A nivel global el desarrollo tecnológico ha sido el más grande en la historia, el internet es una herramienta poderosa como recurso y medio de comunicación, está presente en los hogares, instituciones públicas, privadas, centros educativos, influye en la vida cotidiana de las personas, brinda ventajas como es el acceso a información y recursos, permite una comunicación rápida y eficiente entre las personas, es un mercado global, el mismo que permite expandir el alcance de una empresa siendo esta grande o pequeña más allá de las fronteras geográficas, automatizar tareas, entre otros. Pero también existen aspectos negativos, es decir desventajas como la dependencia de la conectividad, sobrecarga de información, competencia, pero sobre todo el uso del internet implica riesgos de seguridad como ataques cibernéticos, robo de datos o virus informáticos (López, 2019).

Actualmente las amenazas cibernéticas y los riesgos derivados del ciberespacio plantean desafíos para garantizar la seguridad de cada país en el mundo. Sin embargo, América Latina y el Caribe no han progresado en el desarrollo de capacidades en ciberseguridad para hacer frente a esta situación. Los gobiernos de estos países deben comprender en primera instancia el nivel de riesgo y amenaza a la seguridad nacional que puede surgir de este ámbito y afectar al Estado-Nación; es por ello que se debe estructurar un marco jurídico para el combate de ciberdelitos, la creación de acuerdos multilaterales de cooperación y el desarrollo de programas de formación de profesionales en ciberseguridad, consolidando sus responsabilidades y obligaciones (Antonio, 2020).

Por otra parte, manifiesta García (2019), que la dependencia de los sistemas computarizados pone en riesgo la seguridad de los estados, organismos e individuos en el ciberespacio, ya que su fácil accesibilidad hace que las intromisiones clandestinas sean cada vez más comunes, potentes y

alarmantes, es por ello que existe un sistema de defensa efectivo llamado Ciberseguridad, el mismo que protege toda información sensible alojada en el ciberespacio.

En este contexto, Manuel (2021) señala que la ciberseguridad es el conjunto de medidas y prácticas diseñadas para proteger los activos digitales, sistemas informáticos, redes, dispositivos y datos de posibles amenazas, ataques o accesos no autorizados. Su objetivo principal es salvaguardar la confidencialidad, cuyo principio es que únicamente pueden acceder a los recursos de un sistema los usuarios autorizados; integridad, garantiza que los datos se mantienen intactos, no serán alterados ni modificados ya sea de forma accidental o intensional, por errores de hardware o software o por condiciones medioambientales, únicamente podrán ser modificados por usuarios autorizados; y, disponibilidad de la información digital, es decir, garantiza el acceso oportuno y confiable al uso de la información y los sistemas por los usuarios autorizados cuando estos lo requieran.

Entre las amenazas comunes que enfrenta la ciberseguridad se encuentran los virus informáticos, los ataques de phishing que es un tipo de ataque en el que los hackers intentan engañar a los usuarios para que revelen información confidencial, como contraseñas y datos bancarios, el robo de datos, el ransomware que es un tipo de malware que cifra los archivos de la empresa y solicita un rescate para su liberación, el hacking, el espionaje cibernético y el sabotaje de sistemas. Estas amenazas pueden tener consecuencias graves, como la pérdida de información confidencial, daños a la reputación, interrupción de servicios o incluso pérdidas económicas (Quintana, 2023). Esta es la realidad de las grandes empresas quienes se enfrentan a las amenazas de ciberataques, de igual manera las pequeñas y medianas empresas(pymes) quienes dependen cada vez más de la tecnología, específicamente de sistemas de información, por la necesidad de competitividad e innovación, corren el riesgo de sufrir ataques cibernéticos que logran causar grandes pérdidas financieras y de reputación. La preparación para la seguridad cibernética está brotando como una competencia crítica para la supervivencia y el crecimiento de las pymes (Ortega y Segura, 2022).

Por otra parte, Murillo y Gómez (2021) revelan que en el Ecuador a diario existen un gran número de ciberataques según la fiscalía general del Estado, encabezando la provincia de Pichincha con el 47,38% de denuncias por delitos informáticos, seguido la provincia del Guayas con un 27,57% y en tercer lugar la provincia del Oro con el 5,24%; los delitos informáticos más comunes incluyen la suplantación de identidad, la falsificación y uso de documentos falsos así como la apropiación fraudulenta por medios electrónicos. Aunque Ecuador todavía carece de una estrategia de seguridad cibernética, ha logrado avances significativos en cuanto a sus capacidades para enfrentar estas

amenazas, gracias al apoyo del equipo de respuestas ante incidentes cibernéticos del país, EcuCERT (Agencia de Regulación y Control de las Telecomunicaciones).

Como medio de protección contra estas amenazas, las Pymes deben implementar controles de seguridad adecuada, como la autenticación de dos factores, el cifrado de datos, la formación de los empleados en ciberseguridad y el uso de software antivirus y antimalware. También es importante realizar copias de seguridad regulares y mantener los sistemas y el software actualizados. Además, deben tener un plan de respuesta a incidentes en caso de que prevengan un ataque cibernético. El plan debe incluir procedimientos para la recuperación de datos, la notificación a las autoridades y la comunicación con los clientes y proveedores afectados (Carpentier, 2016).

El problema sobre los ciberataques en las Pymes del cantón Cayambe recurre a la necesidad de conocer la manera de proteger los datos y sistemas de información mediante la aplicación de diferentes técnicas de seguridad, por medio del uso de tecnologías de ciberseguridad. El problema es de relevancia para las Pymes, ya que puede afectar directamente su rentabilidad y sostenibilidad.

En base a lo establecido la presente investigación tiene como objetivo analizar el estado de la ciberseguridad en las Pymes del cantón Cayambe mediante una investigación primaria para el conocimiento del manejo de información privada.

Metodología

En el presente trabajo se empleó una investigación cuantitativa y de alcance exploratorio haciendo énfasis en las amenazas y vulnerabilidades de ciberseguridad, mediante el uso de una indagación para recopilar información sobre los riesgos y metodologías de análisis existentes aplicadas a las PYMES. El estudio se centró específicamente en la ciudad de Cayambe. Se realizó el análisis utilizando las metodologías que permiten evaluar el análisis de riesgos con el fin de identificar las amenazas existentes y riesgos asociados en términos de ciberseguridad, de igual manera se evaluó la importancia e impacto de las estrategias de seguridad debido a que no se han implementado de manera generalizada en todos los sectores empresariales.

Fue de tipo descriptivo, se caracterizó las condiciones de ciberseguridad de las empresas, induciendo cada uno de los elementos que hacen vulnerable a las organizaciones en el manejo de la información. Se empleó el método analítico – sintético, procediendo a analizar cada una de las variables e indicadores intervinientes en los procesos de ciberseguridad, se sintetizó la información develando los resultados más importantes.

La población objeto de estudio, estuvo conformada por 2774 pymes del cantón Cayambe (GADIP Cayambe, 2020, pg. 60), se aplicó una muestra con un margen de error de 9%, obteniendo 115 empresas a ser investigadas, aplicando la técnica de encuesta, mediante el instrumento del cuestionario estructurado que constó de 8 preguntas de opción múltiple, enfocadas a la ciberseguridad, vulnerabilidades, uso adecuado de los antivirus, ataques cibernéticos, medidas de seguridad, actualización de antivirus y capacitación en ciberseguridad.

Resultados

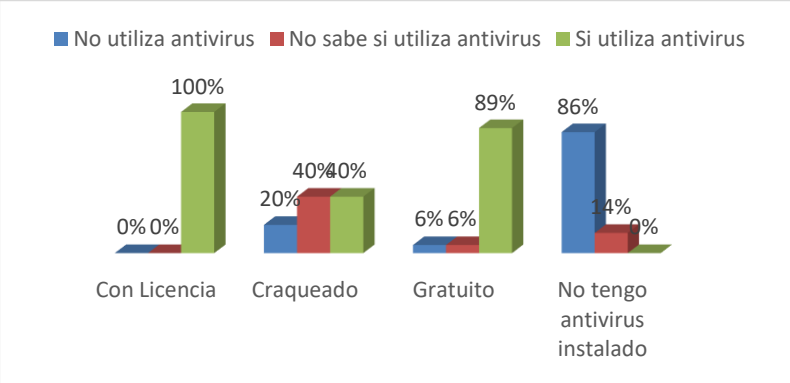
La ciberseguridad se ha convertido en un tema de vital importancia en el entorno empresarial actual, especialmente para las pequeñas y medianas empresas Pymes que enfrentan constantes desafíos para proteger sus activos digitales y salvaguardar la confidencialidad e integridad de su información.

En este contexto, se llevó a cabo un análisis exhaustivo de la ciberseguridad en las Pymes del cantón de Cayambe, donde se evaluaron diversos factores clave relacionados con la protección y prevención de ataques cibernéticos. Los siguientes aspectos fueron considerados para obtener una visión integral de la situación actual: Se examinó la adopción y utilización de software antivirus en las Pymes del cantón de Cayambe, analizando cómo esta medida contribuye a mitigar los riesgos asociados con posibles amenazas cibernéticas. Se evaluó la frecuencia y consistencia con la que las Pymes actualizan sus programas antivirus, ya que la actualización regular es crucial para mantenerse protegido contra las últimas amenazas y vulnerabilidades.

Se analizaron los diferentes tipos de ataques cibernéticos a los que las Pymes están expuestas, identificando las amenazas más comunes y las implicaciones que podrían tener para la seguridad de los sistemas y la información. Se examinaron las medidas preventivas implementadas, para protegerse contra posibles ciberataques, evaluando la efectividad de las estrategias y prácticas implementadas para reducir la exposición a riesgos. Se consideraron las medidas de seguridad implementadas, como la autenticación de usuarios, el cifrado de datos y el control de acceso, para evaluar la robustez de sus sistemas y la protección de su información sensible. Se analizó la adopción y el uso de las actualizaciones de Windows (Windows Update), ya que estas actualizaciones son cruciales para corregir vulnerabilidades conocidas y mantener el sistema operativo protegido. Se evaluó la capacitación y concienciación en ciberseguridad proporcionada a los empleados, reconociendo la importancia de contar con personal informado y preparado para enfrentar los desafíos de seguridad.

Por último, se consideró la frecuencia y el impacto de los ataques cibernéticos sufridos, con el objetivo de comprender la realidad y las consecuencias de estos incidentes.

Gráfico 1 Uso de Antivirus

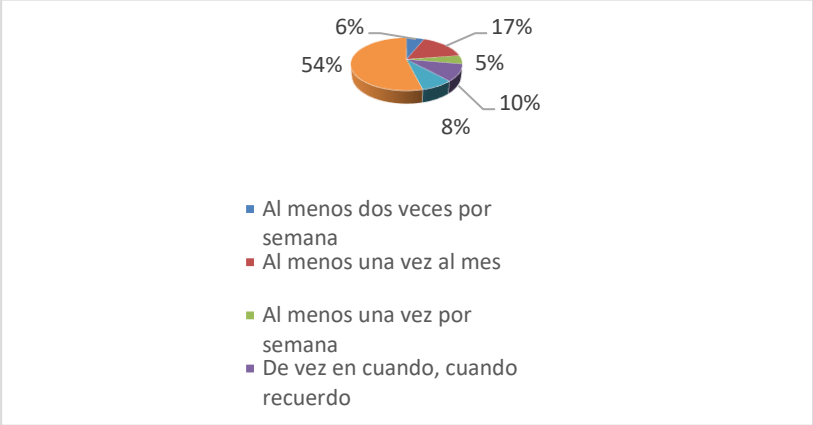


Los resultados mostraron que el 82% de los encuestados utiliza algún tipo de antivirus. Es importante observar que el 100% de aquellos que utilizan antivirus con licencia han optado por esta opción legal y confiable. Según menciona Carrillos y Elgueta (2022) los antivirus permiten atenuar el impacto de una amenaza, además permite reducir la exposición a riesgos.

Sin embargo, es preocupante que un porcentaje considerable de encuestados utilice antivirus craqueado (40%) y antivirus gratuito (89%). Los antivirus craqueados pueden violar los derechos de autor y no brindar la protección necesaria, mientras que los antivirus gratuitos pueden tener limitaciones en términos de características y actualizaciones de seguridad.

Existe una clara necesidad de promover la conciencia sobre la importancia de utilizar antivirus legales, actualizados y confiables en las PYMES de Cayambe. El hecho de que un porcentaje significativo de encuestados no utilice antivirus o utilice antivirus craqueado y gratuito indica una falta de comprensión de los riesgos asociados con la falta de protección cibernética adecuada.

Gráfico 2 Actualización de antivirus

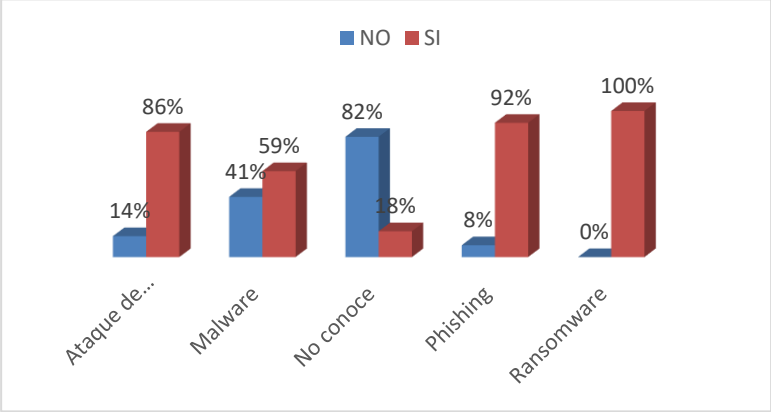


El análisis muestra que el 54% de los encuestados tiene configurado su antivirus para que se actualice de forma automáticamente. Esta es la opción más recomendada, ya que garantiza que el antivirus esté siempre actualizado sin depender de la intervención manual del usuario.

Aunque una parte considerable de los encuestados tiene configurado su antivirus para actualizarse automáticamente, hay un porcentaje notable de encuestados que no se actualiza con la frecuencia recomendada. Esto sugiere que se necesita una mayor conciencia sobre la importancia de las actualizaciones regulares del antivirus para mantener una protección efectiva contra las amenazas cibernéticas.

Los antivirus que incluyan actualización automática permiten la pronta detención, prevención y controles de recuperación para proteger contra código malicioso (Catuto, 2021)

Gráfico 3 Ataques cibernéticos



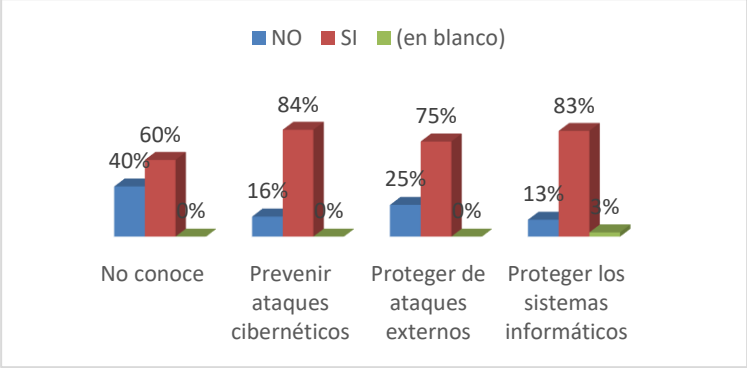
Es significativo observar que el 86% de los encuestados indica tener conocimiento sobre los ataques de inyección SQL, un tipo de ataque muy común en el ámbito cibernético. Sin embargo, es importante

destacar que el 14% de los encuestados aún no está familiarizado con este tipo de ataque, lo que puede dejar sus sistemas y datos vulnerables a posibles explotaciones de seguridad.

En relación con el conocimiento sobre los diferentes tipos de ataques cibernéticos, se observa que el 82% de los encuestados indica no conocer los ataques cibernéticos mencionados, mientras que solo el 18% afirma tener conocimiento sobre ellos. Este resultado refleja una preocupante falta de conocimiento en general sobre los tipos de ataques cibernéticos evaluados en la encuesta.

Es imperativo abordar esta brecha de conocimiento y promover la educación en ciberseguridad para proteger las estructuras informáticas y la información; debe ser importante para la estabilidad de las PYMES que se integran cada vez más a las redes de tecnología e información. Es necesario incorporar la ciberseguridad al proceso educativo como un tema de actualidad en la formación de especialistas en sistemas informáticos, así como otras profesiones de usuarios de sistemas informáticos(Valencia et al., 2020).

Gráfico 4 Principales tipos de ciberataques



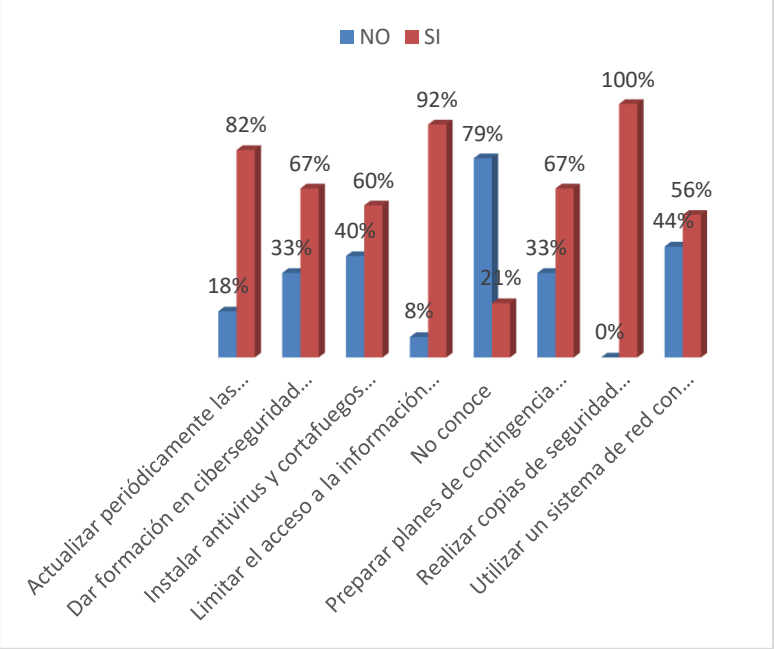
Los resultados revelaron que el 60% de las PYMES encuestadas indican no tener conocimiento sobre ciberseguridad, lo cual es alarmante. Esto señala una falta de conciencia y comprensión sobre los riesgos y las mejores prácticas de seguridad cibernética en el entorno empresarial.

El 84% de las PYMES indica estar preocupado por prevenir los ataques cibernéticos, esto es un indicio positivo, ya que muestra que una parte significativa de las empresas está consciente de la importancia de protegerse contra las amenazas cibernéticas. Sin embargo, es necesario enfocar esfuerzos adicionales en educar y concienciar al 16% restante sobre los riesgos y las medidas de prevención adecuadas. Los resultados revelan que hay un porcentaje significativo de PYMES en el cantón Cayambe que carecen de conocimientos básicos sobre ciberseguridad. Esto plantea una

preocupación importante, ya que las amenazas cibernéticas pueden tener un impacto negativo en la continuidad del negocio y la seguridad de la información.

La ciberseguridad requiere esfuerzos continuos para brindar soluciones y espacios ciberseguros. Los analistas e investigadores de seguridad informática se enfrentan a diario a la complejidad de investigar casos que pueden o no ser ciber amenazas, un desafío que incluye muchas variables: el desarrollo acelerado de la tecnología, la escasez de profesionales de seguridad digital, la guerra cibernética y las vulnerabilidades no descubiertas. puede ser importante en el proceso de investigación. Esto, a su vez, puede verse afectado por el tiempo y los recursos, lo que puede causar problemas no solo a nivel empresarial, sino también en la vida. Es por ello que se requiere de una actualización de conocimientos en el tema de ciberseguridad(Urcuqui et al., 2022).

Gráfico 5 Medidas de Seguridad



El análisis estadístico proporciona información sobre la situación de la formación en ciberseguridad y la preparación de planes de contingencia en un conjunto de empresas encuestadas, las mismas que son:

Formación en ciberseguridad: El 67% de las empresas encuestadas brindan formación en ciberseguridad a sus empleados, mientras que el 33% no lo hace. Se destaca que una parte significativa de las empresas está tomando medidas para capacitar a sus empleados en ciberseguridad,

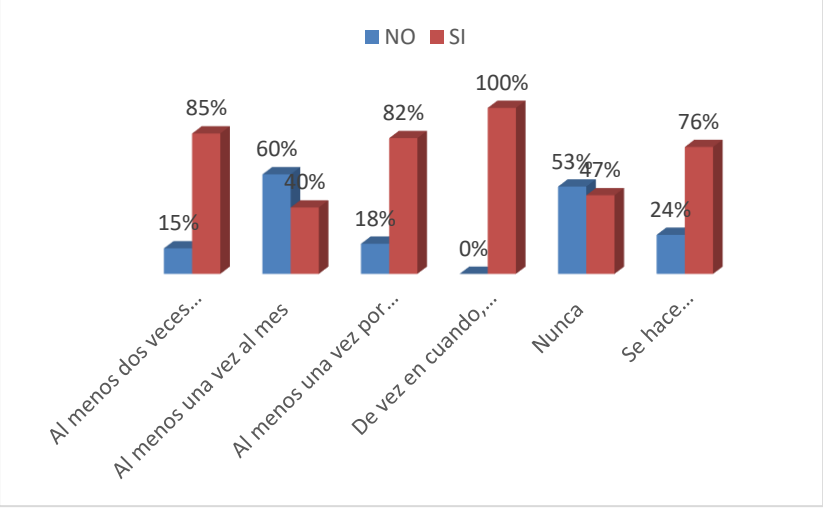
lo que es positivo. La capacitación es fundamental para aumentar la conciencia y el conocimiento sobre las amenazas y las mejores prácticas de seguridad en el entorno digital.

Conocimiento sobre medidas de ciberseguridad: El 79% de las empresas encuestadas indicaron que no conocen las medidas de ciberseguridad, mientras que el 21% sí tiene conocimiento sobre ellas. Es preocupante que la mayoría de las empresas carezcan de conocimiento sobre las medidas de ciberseguridad. Esto resalta la necesidad de promover la educación y la conciencia en ciberseguridad para garantizar una mejor protección contra los ataques cibernéticos. Las empresas que no conocen las medidas de seguridad pueden estar más expuestas a riesgos y vulnerabilidades.

Planes de contingencia ante ataques cibernéticos: El 67% de las empresas encuestadas preparan planes de contingencia ante ataques cibernéticos, mientras que el 33% no lo hace. Estos planes son esenciales para una respuesta rápida y eficiente en caso de un ciberataque y deben ser implementados por todas las empresas. Esto indica una conciencia creciente sobre la importancia de estar preparados para enfrentar posibles amenazas cibernéticas.

Promover la educación y la conciencia en ciberseguridad es esencial para mitigar riesgos y proteger los activos digitales de las empresas. La ciberseguridad se ocupa de garantizar la implementación y el mantenimiento de los atributos de seguridad de una organización y los activos de los usuarios frente a los riesgos de seguridad asociados en el entorno cibernético (Páez et al., 2019).

Gráfico 6 Uso del Windows Update

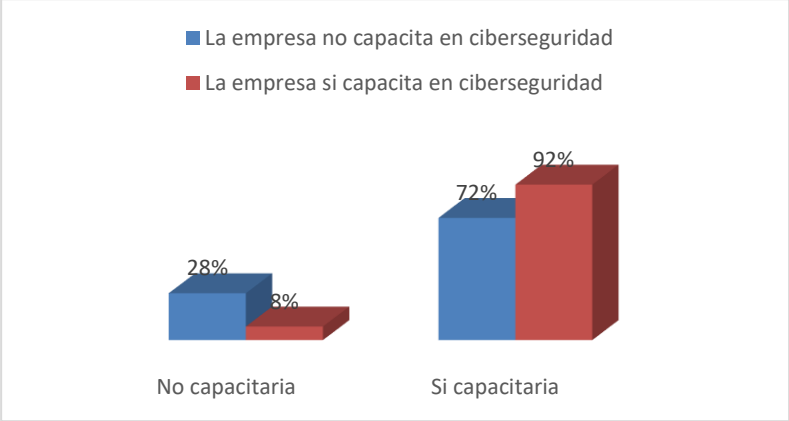


El análisis estadístico proporciona una visión detallada sobre la actitud de los encuestados hacia las actualizaciones periódicas de Windows. Frecuencia de actualizaciones: El 85% de los encuestados realiza actualizaciones de Windows al menos dos veces por semana, lo que indica que la mayoría de

las personas son conscientes de la importancia de mantener el sistema operativo actualizado. Sin embargo, el 40% de los encuestados realiza actualizaciones mensuales, lo que puede ser insuficiente para mantener el sistema al día con las últimas correcciones de seguridad y mejoras. Las actualizaciones periódicas son cruciales para garantizar que el sistema esté protegido contra vulnerabilidades conocidas.

Ausencia de actualizaciones: El 47% de los encuestados nunca realiza actualizaciones de Windows. Esta cifra es preocupante, ya que indica una falta de conciencia sobre los riesgos asociados con un sistema desactualizado y la importancia de instalar los últimos parches de seguridad. La falta de actualizaciones representa un riesgo para la seguridad de los sistemas. Se recalca la necesidad de educar a los usuarios sobre la importancia de las actualizaciones y promover una cultura de seguridad cibernética más proactiva, además es muy importante mantener los sistemas actualizados mediante actualizaciones periódicas de Windows (Villacián, 2018).

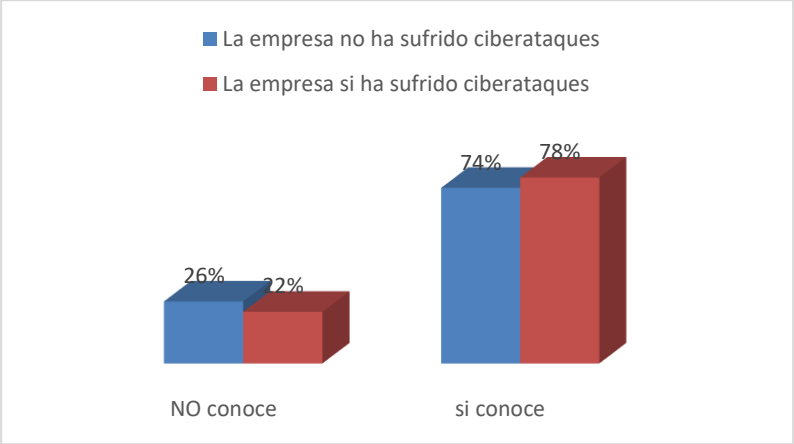
Gráfico 7 Capacitación en ciberseguridad



El análisis estadístico proporciona información valiosa sobre la situación de la capacitación en ciberseguridad en las empresas encuestadas. El 28% de las empresas encuestadas indicó que no brinda capacitación en ciberseguridad a sus empleados. Esta cifra es preocupante, ya que indica que casi una tercera parte de las empresas no está proporcionando la capacitación necesaria para que sus empleados estén preparados para reconocer y responder a posibles ataques cibernéticos. Mientras tanto el 92% de las empresas encuestadas indicó que sí brindaría capacitación en ciberseguridad a sus empleados, esto muestra que la gran mayoría de las empresas comprende la importancia de la capacitación en ciberseguridad y está dispuesta a invertir en perfeccionar el conocimiento sobre los posibles riesgos y medidas de seguridad en el entorno digital. Promover la capacitación en ciberseguridad es esencial

para mejorar la preparación de los empleados frente a las amenazas cibernéticas y fortalecer la seguridad general de las empresas en el entorno digital (Molina, 2021).

Gráfico 8 Ataques cibernéticos a Empresas



Los resultados mostraron información relevante sobre la incidencia de ciberataques en las empresas encuestadas, las mismas que se muestra un 74% de las empresas encuestadas dicen haber experimentado ciberataques en algún momento, esto destaca la realidad de que los ciberataques son una amenaza significativa y que muchas empresas están en riesgo de sufrirlos; mientras tanto el 26% de las empresas encuestadas indicó que no ha sufrido ciberataques, si bien esto puede parecer una cifra alentadora, es importante que estas empresas comprendan que el riesgo siempre está presente en el entorno digital y que ninguna organización está completamente inmune a los ciberataques. Es fundamental que estas empresas sean conscientes de la necesidad de tomar medidas proactivas para mejorar su postura de seguridad y proteger sus sistemas y datos. Las empresas que han sido atacadas deben aprender de sus experiencias pasadas y fortalecer sus defensas para minimizar el riesgo de futuros ataques. La ciberseguridad debe considerarse una prioridad estratégica para proteger la continuidad del negocio y la confianza del cliente.

Conclusiones

En este estudio se destaca la necesidad de mejorar la ciberseguridad en las PYMES del cantón Cayambe, especialmente en lo que respecta a la instalación y actualización de antivirus, ya que la mayoría de los encuestados no tienen instalado ningún antivirus en sus sistemas. Esto deja expuestos sus sistemas y datos a posibles ataques cibernéticos. Configurar el antivirus para que se actualice

automáticamente es la opción más recomendada, esto mitiga las posibles amenazas cibernéticas. Es fundamental educar a los usuarios sobre los beneficios de las actualizaciones y promover una cultura de seguridad cibernética que priorice la actualización regular del sistema operativo. Se debe fomentar el establecimiento de recordatorios o la configuración de actualizaciones automáticas para mejorar la consistencia en la implementación de las actualizaciones.

La conciencia y la educación sobre las mejores prácticas de ciberseguridad son fundamentales para proteger los sistemas y datos de las PYMES y garantizar su rentabilidad y sostenibilidad en un entorno cada vez más digitalizado y propenso a ciberataques, es por ello que es necesario implementar programas de capacitación y concienciación en ciberseguridad específicamente dirigidos a las PYMES. Promover la capacitación en ciberseguridad es esencial para mejorar la preparación de los empleados frente a las amenazas cibernéticas y fortalecer la seguridad general de las empresas en el entorno digital.

Estos programas deben enfocarse en aumentar la comprensión de los riesgos cibernéticos y las mejores prácticas de seguridad en el entorno empresarial.

Además, se deben promover iniciativas para que las PYMES adopten medidas efectivas para prevenir y protegerse contra los ataques cibernéticos. Esto puede incluir la implementación de políticas y procedimientos de seguridad, la actualización regular de software y sistemas, la capacitación del personal en seguridad cibernética y la adopción de soluciones de seguridad confiables. La ciberseguridad debe considerarse una parte esencial de la estrategia empresarial para garantizar la seguridad y la resiliencia en el entorno digital.

Referencias

Carrillos Vergara, G.O., Elgueta Carrillo, F.A., 2022. “Tu empresa digital.”

Catuto Pilay, R.M., 2021. Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución (bachelorThesis). La Libertad: Universidad Estatal Península de Santa Elena, 2021.

GADIP Cayambe, 2020.Plan de Desarrollo y Ordenamiento Territorial del Cantón Cayambe

Molina Castaño, S., 2021. Ciberseguridad de las empresas financieras.

Páez, L.A.G., Arenas, J.E.T., Moreno, A.N.B., 2019. CIBERSEGURIDAD Y ETHICAL HACKING: LA IMPORTANCIA DE PROTEGER LOS DATOS DEL USUARIO. EIEI ACOFI. https://doi.org/10.26507/ponencia.248

Urcuqui López, C., Navarro, A., Diaz, J., Villarreal, J., 2022. Cybersecurity: data holds the answer. https://doi.org/10.18046/EUI/ee.4.2022

Valencia-Arias, A., Giraldo, M.C.B., Acevedo-Correa, Y., Garcés-Giraldo, L.F., Quiroz-Fabra, J., Benjumea-Arias, M.L., Patiño-Vanegas, J., 2020. Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. Risti 225–239.

Villacián Leciñena, J., 2018. Comparativa entornos de trabajo para despliegue de actualizaciones Windows.

Antonio, J. M. A. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciber amenazas: DOI: http://dx.doi.org/10.18847/1.12.2. Revista de Estudios en Seguridad Internacional, 6(2), Article 2.

Carpentier, J.-F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Ediciones ENI.

García, A. A. (2019). Ciberseguridad: ¿Por qué es importante para todos? Siglo XXI Editores México. https://books.google.es/books?hl=es&lr=&id=ZqHDDwAAQBAJ&oi=fnd&pg=PT5&dq=ciberseguridad+que+es&ots=yhhc23Wsc5&sig=iWsPwJWNDMoBrbJnOinUsjmGbbk#v=onepage&q=ciberseguridad%20que%20es&f=false

López, E. V. (2019). Las ventajas y desventajas del internet en la sociedad. Conciencia Digital, 2(1), Article 1. https://doi.org/10.33262/concienciadigital.v2i1.928

Manuel, O. C., José. (2021). Ciberseguridad. Manual práctico. Ediciones Paraninfo, S.A.

Murillo, G. M., & Gómez, O. S. G. (2021). Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMEs: Caso de estudio en Riobamba. Revista Perspectivas, 3(2), Article 2. https://doi.org/10.47187/perspectivas.vol3iss2.pp45-53.2021

Ortega, O. B., & Segura, J. R. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, 016, Article 016. https://doi.org/10.26439/interfases2022.n016.6021

Quintana, Y. (2023). Ciberguerra. Los Libros De La Catarata.