ANÁLISIS DE LA SEGURIDAD DE INFORMACIÓN EN EL ÁREA DE SECRETARÍA DE LA UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ, EXTENSIÓN EL CARMEN

INFORMATION SECURITY ANALYSIS IN THE SECRETARIAT AREA OF THE UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ, EL CARMEN EXTENSION

Cedeño-Zambrano Irene Jacqueline
Universidad Laica Eloy Alfaro de Manabí. Manta – Ecuador
irenecedzam@gmail.com

RESUMEN

El presente trabajo fue enfocado en el análisis de la seguridad de la información lógica en el área de secretaría de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen. Se empleó los métodos analítico y sintético con el propósito de analizar por separado y manera global los datos. La técnica utilizada fue la encuesta a las secretarias para conocer su situación en su área de trabajo en cuanto al alojamiento de información en la nube. Se concluye que el cifrado de la información almacenada en OneDrive, provee de seguridad, evitando la incertidumbre de pérdida o violación de los datos que manejan en el área de secretaría.

Palabras clave: seguridad, información, OneDrive, Uleam, secretaría.

ABSTRACT

The present work was focused on the analysis of the security of logical information in the secretariat area of the Universidad Laica Eloy Alfaro de Manabí, El Carmen extension. Analytical and synthetic methods were used in order to analyze the data separately and globally. The technique used was the survey of secretaries to find out their situation in their work area in terms of hosting information in the cloud. It is concluded that the encryption of the information stored in OneDrive provides security, avoiding the uncertainty of loss or violation of the data handled in the secretariat area.

Keywords: security, information, OneDrive, Uleam, secretary.

Fecha de recepción: 19 de noviembre de 2018; **Fecha de aceptación:** 08 de enero de 2019; **Fecha de publicación:** 09 de enero de 2019.

1. INTRODUCCIÓN

La seguridad de la información lógica consiste en mantener intacta la integridad, disponibilidad y confidencialidad de los datos almacenados en sitios web, de manera que no se puedan efectuar ataques por parte de individuos maliciosos que buscan aprovecharse de un sistema vulnerable para causar un daño en beneficio propio, por ende, la protección de los datos en un tema a considerar para los usuarios por ser método de precaución.

El trabajo se desarrolló en el área de secretaria de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, está enfocado a la seguridad de la información en archivos alojados en la nube, para ello se toma en consideración los ataques a los que se encuentras expuestos los datos en almacenamientos, lo cuales se los detecta por medio de la auditoría de las vulnerabilidades y riesgos presente en OneDrive.

2. METODOLOGÍA

La metodología de este trabajo es cuanti-cualitativa basada en el análisis de los datos recolectados. Así, se trata de una investigación de campo y aplicada. Se emplea un análisis documental basado en la revisión de diversos tipos de artículos y textos provenientes que poseen fundamentos teóricos sólidos. Además, se realizó una encuesta a 4 secretarías de la Universidad Laica Eloy Alfaro de Manabí (Uleam).

2.1. Integridad

La integridad consiste en mantener la información intacta ante cualquier situación, es decir, sin modificaciones a los datos no autorizados. Es necesario tomar en cuenta que la integración ayuda a garantizar que la información sea verídica y exacta, por lo cual, esta propiedad permite que la información precedente se mantenga intacta de cualquier alteración aparente por individuos malintencionados que buscan beneficiarse con los datos privados (Gargallo, 2018).

2.2. Disponibilidad

La disponibilidad tiene como característica primordial tener todos los archivos y documentos encontrarse accesibles en cualquier momento que sea requerido por los individuos autorizados, por ende, la información de una organización u persona natural pueda obtener los datos de manera rápida y segura, evitando amenazas como la interacción y perdida del contenido en el sistema (Gargallo, 2018).

2.3. Confidencialidad

Mediante este proceso se puede declarar que una información es confidencial al ser entendida por el usuario, es decir, logra ser comprendida por una persona autorizada. Con el fin de evitar la intercepción se usan claves de cifrado asimétricas y simétricas para que la información envía no sufra ninguna de estas amenazas por individuos maliciosos en el traslado hasta su destino ya que al llegar el receptor podrá descifrarlo con ayuda de su clave privada de esta manera la información trasmitida llegará de manera intacta al receptor (Costas, 2015).

2.4. Amenazas y riesgos

En cuanto a los diversos de ataques informáticos que se presentan esta la interrupción que trata de la obstrucción de la información en un sistema informático. Por otra parte, se encuentra la intercesión siendo aquella que afecta de manera directa a la confidencialidad de la información en un sistema que consiste en interceptar los datos antes que lleguen a su destino final, otro de los tipos de amenazas se encuentra la modificación que afecta el entendimiento correcto de un mensaje que fue cambiado sin autorización (Posada Maya, 2017).

2.5. Sistema gestor de la seguridad de la información

La dependencia a la tecnología se ha hecho notar en los últimos tiempos en especial a programas de almacenamiento de información y lo que conlleva con esto las diversas amenazas, por ende, es primordial el sistema gestor de la seguridad de los archivos ya que evita interrupción de procesos, intercesión y aporta a descubrir fraudes disminuyendo el daño, ayudando a las empresas o

personas naturales a reaccionar cuando ocurra un error de seguridad en el sistema (César, 2015).

2.6. Medidas de seguridad

Existen diversas medidas de prevención entre las cuales está la preventiva que consiste en evitar que ocurran desastres en el sistema de información que pueda provocar un daño para, lo cual se usa herramientas de cifrado en el sistema de esta manera mantener segura la información, otra de las medidas es la detección como su nombre lo dice cumple la función de detectar y controlar los problemas en la seguridad, en cuanto a la medida de seguridad correctiva esta se pone en funcionamiento después que ocurra el incidente perjudicial en el software (Chicano, 2015).

2.7. Seguridad en la nube

El almacenamiento de información en la nube conlleva muchos riegos que afectar el desarrollo integro de los datos, por lo cual la seguridad en las plataformas tiene que ser una precaución principal por la existencia de los hackers y demás peligros que afectan la información ya que al encontrarse en el cloud son más vulnerables, por ende, la ciber seguridad le permite al usuario guardar sus documentos de una manera segura y evitar la incertidumbre de la pérdida de archivos importantes (Pistorious, 2017).

3. RESULTADOS

Una vez encuestadas a las cuatro secretarias de la Uleam, los resultados fueron los siguientes:

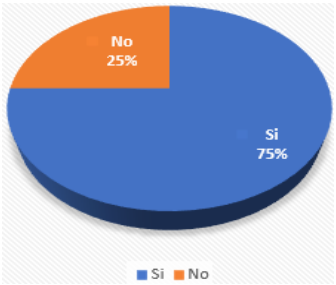

Figura 1. *Resultado de encuesta – Pregunta 1: ¿Considera primordial mantener datos seguros en la nube?*
Elaboración*: Autor.*

En base a los resultados, se puede notar que el 75% de la población considera primordial mantener los datos seguros en la nube.

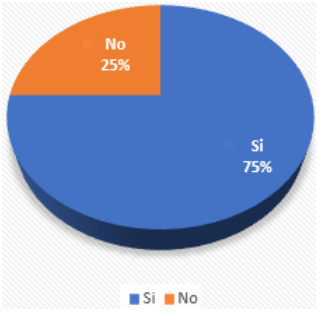

Figura 2. *Resultado de encuesta – Pregunta 2: ¿Utiliza claves de seguridad en su ordenador?*
Elaboración*: Autor.*

Existe una pequeña parte de las personas encuestadas que no usa clave en el ordenador como precaución, poniendo en riegos que los datos se filtren.

Figura 3. *Resultado de encuesta – Pregunta 3: ¿Posee un servicio de almacenamiento en la nube?*
Elaboración*: Autor.*

De acuerdo con los datos obtenidos, muestra que en su totalidad las secretarias poseen un servicio de almacenamiento en la nube.

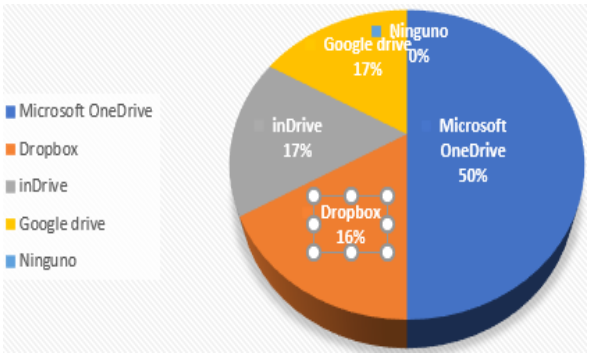

Figura 4. *Resultado de encuesta – Pregunta 4: ¿Qué tipo de servicio de nube utiliza?.*
Elaboración*: Autor.*

Las secretarias de la ULEAM extensión El Carmen, utilizan varios tipos de nubes, entre el más usado se encuentra Microsoft OneDrive, siendo un servicio pagado por la institución.

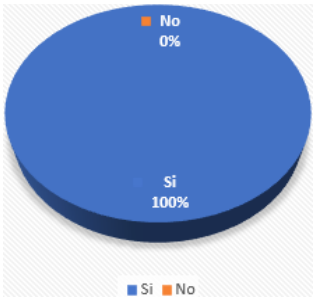

Figura 5. *Resultado de encuesta – Pregunta 5: ¿Considera importante cifrar sus datos para mantener segura su información?.*
Elaboración*: Autor.*

Los resultados de la encuesta indican que, en su totalidad, la población considera que al cifrar los datos se podrá mantener segura la información.

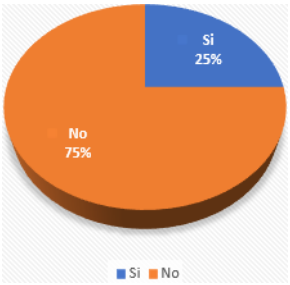

Figura 6. *Resultado de encuesta – Pregunta 6: ¿Ha presentado vulnerabilidades en su servicio de nube?.*
Elaboración*: Autor.*

Los datos obtenidos indican que los ataques han sido mínimos, del 25% en el área de secretaría, sin embargo, si se han presentado y demuestran la existencia de las vulnerabilidades en la nube.

Figura 7*. Resultado de encuesta – Pregunta 7: ¿Conoce herramientas de encriptación de datos en la nube?.*
Elaboración*: Autor.*

Se puede apreciar en los resultados, que el 50% de las secretarías desconocen sobre el uso de herramientas de encriptación para los datos en la nube y la otra mitad tiene poco conocimiento sobre el tema.

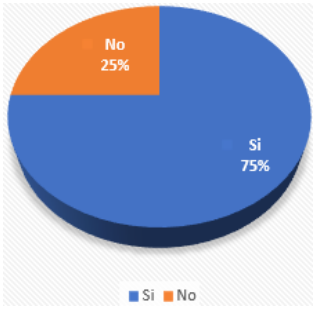

Figura 8. *Resultado de encuesta – Pregunta 8: ¿Accede a sus datos de la nube en dispositivos externos a su área laboral?*
Elaboración*: Autor.*

Como se observa en los resultados, un 75% de la población accede a la información en dispositivos externos al área laboral, por lo que corre riesgos de un ataque informático.

Figura 9. *Resultado de encuesta – Pregunta 9: ¿En que formato sube sus documentos a su nube?.*
Elaboración*: Autor.*

Se puede notar que los tres formatos son utilizados por las secretarias, por ende, la herramienta tiene que proteger todos los tipos de documentos encontrados.

Figura 10. *Resultado de encuesta – Pregunta 10: ¿Considera Ud que una herramienta de encriptación puede mantener segura su información en la nube?.*

***Elaboración**: Autor.*

La información obtenida por la encuesta afirma que el 100% de la población, consideran que poseer una herramienta de encriptación puede mantener los datos seguros.

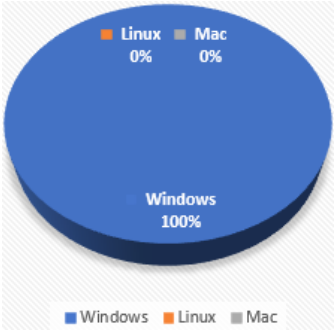

***Figura 11.** Resultado de encuesta – Pregunta 11: ¿Bajo que sistema operativo es recomendable contar con una herramienta de encriptación?.*
***Elaboración**: Autor.*

En base a la respuesta, la herramienta de encriptación tiene que ser compatible con el sistema operativo Windows.

***Figura 12.** Resultado de encuesta – Pregunta 12: ¿Está Ud de acuerdo con poseer una herramienta de encriptacion para la seguridad de la información en la nube?.*
***Elaboración**: Autor.*

Se percató que, en su totalidad de la población, se encuentran de acuerdo en poseer una herramienta de encriptación para la seguridad de la información en la nube.

4. DISCUSIÓN

El conocimiento sobre la seguridad de la información en los servicios de almacenamiento en la nube es muy importante para informar de los riesgos y protocolos a seguir para mantener segura la información, también evitar la

incertidumbre de los datos ante ataques por terceros. Esto se puede evidenciar en la pregunta 1 de la encuesta a las secretarias.

Microsoft OneDrive es considerado un almacenamiento de archivos en la nube, confiable y factible para el uso institucional, por ende, la ULEAM extensión El Carmen hace uso de este servicio en la nube para sus respectivas actividades, se puede ver reflejado en la pregunta 4 de la encuesta a las secretarias.

El uso de herramientas de encriptación de archivos en la nube es apropiado para mantener segura la información, gracias al cifrado de documentos por medio de una clave única para el usuario, con la finalidad de evitar ataques por terceros, siendo bien aceptada para su manejo institucional por las secretarias en la pregunta 10 de la encuesta.

5. CONCLUSIONES

El cifrado de la información almacenada en OneDrive, provee de seguridad, evitando la incertidumbre de pérdida o violación de los datos que manejan en el área de secretaría.

Por ende, se sugiere realizar capacitaciones para concientizar a la población de la universidad, los riegos que puede sufrir la información almacenada en la nube y los beneficios de cifrarla.

REFERENCIAS

César, J. P. (2015). Protección de datos y seguridad de la información. RA-MA.

Chicano, E. (2015). Gestión de incidentes de seguridad informática. IC.

Costas Santos, J. (2015). Seguridad y alta disponibilidad. RA-MA.

Fernández, J. A. (2017). Sistemas seguros de acceso y transmisión de datos. RA-MA.

Giménez Albacete, J. F. (2015). Seguridad en equipos informáticos. IFCT0510. IC Editorial.

González, E. S. (2015). Salvaguarda y seguridad de los datos. IFCT0310. IC Editorial.

Heredero, C., López, J. J., & Romo, S. M. (2019). Organización y transformación de los sistemas de información en la empresa. ESIC.

Maillo Fernández, J. A. (2017). Sistemas seguros de acceso y transmisión de datos. RA-MA.

Mattson, F. (2019). Ciberseguridad: los riesgos de la información en la nube. FELABAN.

Posada Maya, R. (2017). Los cibercrímenes: un nuevo paradigma de criminalidad. Universidad de los Andes.