# **Módulo:** Seguridad informática en la nube

# **Actividad:** Tarea
# Reto de aprendizaje 1. Ensayo de Seguridad Informática

**Nombre:** Roberto Mora Balderas

**Asesor:** José Abdón Espínola González

**Fecha:** 16 de abril de 2023

Seguridad informática

Con base en los avances tecnológicos de las últimas décadas, la humanidad contemporánea ha desarrollado una interconexión y una dependencia global, que abarca lo económico, lo político y lo social. La transferencia de información y de datos cada vez toma más peso e importancia para todos los ámbitos previamente mencionados, generando un impacto verdaderamente significativo para el desarrollo integral. Lo realmente importante es generar conciencia no solo de los beneficios que nos brinda esta transferencia de información si no de los riesgos que implica su mala utilización. A lo largo de este ensayo hablaremos acerca de que es la seguridad informática, sus niveles, su implementación y herramientas utilizadas para la misma.

Al hablar de seguridad informática debemos comenzar entendiendo su definición, y para esto podemos separarlo en 2 partes, ¿a qué nos referimos con información y a que llamamos seguridad? Comenzaremos definiendo que es la información, de acuerdo con el audio digital "El valor de la información" podemos definir como información a aquellos datos que por su contenido aportado puedan generar un beneficio a la persona que tiene acceso a ellos (Online, El valor de la información, 2019). Es decir, que la información es dependiente de la finalidad de la entidad que la necesita, y así mismo el valor que puede aportar la información está en función al análisis al cual se le someta. El valor relacionado con la información puede ir desde un valor económico (la información como activo), un valor al cual denominaremos como trascendental (el valor de la información como proceso de aprendizaje), un valor social y de posicionamiento (la información y capital social) todo de acuerdo con la finalidad con la cual será empleada (Musiño, 2010). Dicho esto, podemos observar que la información genera un impacto directo en muchos ámbitos en una entidad, ya sea una persona u organización, por lo que protegerla y cuidarla se vuelve de suma importancia, lo cual nos lleva al siguiente punto de nuestro cuestionamiento inicial.

Lo que se entiende actualmente como seguridad podría definirse como el acto de evaluar, estudiar y gestionar los riesgos a los que se encuentra sometida una entidad, en nuestro caso un sistema de información o sistema informático. De acuerdo con el libro

*Seguridad Informática* “La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditas y dentro de los límites de su autorización“ (Santos, 2015) por lo que podemos extraer de este fragmento las piezas claves que componen la seguridad informática, siendo estas: confidencialidad, integridad, disponibilidad, autenticación y no repudio, estas características son conocidas como CIDAN y al asegurar su cumplimiento podemos hablar de que la un sistema de información es seguro.

La seguridad informática, es un fenómeno que puede analizarse de acuerdo con el nivel del sistema de información que está protegiendo, para estos análisis podemos hablar de los modelos por capas, los cuales son protocolos que cooperan para gestionar las comunicaciones o transferencia de información de acuerdo con el libro *Seguridad por Niveles* (Estrada, 2011). Existen distintos tipos de modelos que se han ido empleando a lo largo de los años siendo el modelo OSI el modelo por excelencia, dividiendo el sistema en los siguientes niveles: Físico, enlace, red transporte, sesión, presentación y aplicación, cada nivel cuenta con protocolos específicos que componen su seguridad, sin embargo debido al aumento en la demanda de sistemas de comunicación el sistema OSI no ha podido proporcionar la velocidad necesaria por lo que se han realizado versiones más compactas, denominadas como RFC, el modelo RFC más famoso y utilizado es el modelo DARPA, el cual une los niveles de sesión, presentación y aplicación en uno solo, al cual denominaron como aplicación (Estrada, 2011).

Una vez que ya definimos que es la seguridad informática podemos hablar de su implementación, este fenómeno da origen a muchos métodos para llegar a dicho objetivo, uno de los métodos más utilizados es el COBIT 5. El COBIT 5 está compuesto de 5 principios para llevar a una política clara, que permita el control de las tecnologías de la información en una organización (Online, ¿Qué es COBIT 5?, 2019). Este método se basa en, satisfacer las necesidades del accionista, considerar la empresa de punta a punta, aplicar un único modelo de referencia integrado, posibilitar un enfoque holístico y separar el gobierno de la gestión (Online, Objetivos de la seguridad informática, 2019) generando un enfoque que permita el desarrollo de la empresa de manera segura. Las metodologías a pesar de poseer un enfoque distinto, entre ellas, en cómo llegar a la seguridad informática, todas tienen que basarse en los

mismos cimientos técnicos que se han ido desarrollando a lo largo de las últimas décadas lo cual nos lleva a nuestro último punto, las herramientas o técnicas para la seguridad informática.

Actualmente existen muchas técnicas para apoyar el cumplimiento de la seguridad informática, entre ellas de las más importantes se encuentran el cifrado simétrico y asimétrico, los cuales consisten en que los mensajes enviados utilicen claves para la encriptación de este. El cifrado simétrico usa una clave privada para cifrar y descifrar un correo electrónico cifrado. El cifrado asimétrico usa la clave pública del destinatario para cifrar el mensaje. Entonces, si el destinatario quiere descifrar el mensaje, tendrá que usar su clave privada para hacerlo. Otra técnica importante es una ubicación estratégica del centro de procesos de datos, este centro es el alma de la transferencia de información de una empresa, por lo que generando un espacio centralizado se logra ahorrar en costes de protección y mantenimiento, optimización de la comunicación entre servidores y mejorar el aprovechamiento de recursos humanos (Buendía, 2013).

Con todo lo previamente expuesto podemos observar como la seguridad informática, es un fenómeno complejo, es un estudio multidisciplinario que comprende áreas como la comunicación, la informática, sociología, economía, entre otras, dicho fenómeno no solo es importante debido a su complejidad sino también por su impacto global relacionado al valor que puede tener la información involucrada en la transferencia entre entidades. Es importante seguir indagando y profundizando en los métodos de protección de la información para encontrar las técnicas específicas que brinden respuestas a las emergentes situaciones de la vida contemporánea.

## Bibliografía


Buendía, J. F. (2013). *Seguridad Informática.* McGraw Hill.

Estrada, A. C. (2011). *Seguridad Por Niveles.* Madrid: RPI.

Kaspersky. (2019). *¿Qué es la ciberseguridad?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Musiño, C. M. (2010). El valor de la información, su administración y alcance en las organizaciones. Obtenido de https://acortar.link/VS4AnK

Online, A. (2019). ¿Qué es COBIT 5?

Online, A. (2019). El valor de la información [Grabado por A. Online].

Online, A. (2019). Objetivos de la seguridad informática.

Santos, J. C. (2015). *Seguridad Informática.* Madrid: RA-MA.