UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:
INGENIERÍA DE SISTEMAS

TEMA:
"SEGURIDAD EN LA GESTIÓN DE LA INFORMACIÓN PARA LAS ORGANIZACIONES PÚBLICAS DESDE EL ENFOQUE ISO/IEC 2700: UN MAPEO SISTEMÁTICO"

AUTOR:
Yaritza Julieth Terán Terranova

TUTOR:
Ing. Joe Frand Llerena Izquierdo

Abril 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Yaritza Julieth Terán Terranova**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor

Firma del tutor

Seguridad en la Gestión de la Información para las Organizaciones Públicas desde el enfoque ISO/IEC 2700: un mapeo sistemático

Yaritza Terán Terranova[1] [0000-0002-3975-899X], Bertha Alice Naranjo Sánchez[1] [0000-0002-4386-2335] and Joe Llerena-Izquierdo [1] [0000-0001-9907-7048]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
yterant@est.ups.edu.ec, bnaranjo@ups.edu.ec, jllerena@ups.edu.ec

Resumen Los problemas son muy evidentes en las organizaciones públicas sin seguridad en la gestión de la información. Se han propuesto diversos análisis, entre ellos, los riesgos que enfrentan las organizaciones públicas, para resolver el robo en las bases de datos de la información ingresada, teniendo en cuenta el uso de la metodología para preservar la garantía de la seguridad de la información y al administrar los riesgos de forma más efectiva. El trabajo pretende identificar el uso de método deductivo y la investigación exploratoria. Para el desarrollo de este articulo académico se realizó un estudio a la metodología MAGERIT que protege la información en su confidencialidad y disponibilidad dando garantía a la seguridad del sistema, incluyendo a los procesos de las organizaciones públicas y un mapeo sistemático. Los resultados obtenidos en los artículos seleccionados, da un enfoque de interés y un control de factores de seguridad de la información, tomando en cuenta que MAGERIT sigue siendo una medida de seguridad que mitiga las amenazas y riesgos de sus procesos incluyendo el mapeo nos da como requerimiento una validación para ser considerados en la industria del desarrollo de software**.**

Abstract. The problems are very evident in public organizations without security in the management of information. Various analyzes have been proposed, among them, the risks faced by public organizations, to solve the theft of information in the database, taking into account the use of the methodology to preserve the guarantee of information security and when managing data. risks more effectively. The work aims to identify the use of the deductive method and exploratory research. For the development of this academic article, a study was carried out on the MAGERIT methodology that protects the information in its confidentiality and availability, guaranteeing the security of the system, including the processes of public organizations and a systematic mapping. The results obtained in the selected articles, give a focus of interest and a control of information security factors, taking into account that MAGERIT continues to be a security measure that mitigates the threats and risks of its processes, including the mapping that requires validation. to be adopted by the software development industry.

Palabras claves: mapeo sistemático, metodología, validación empírica.

1 Introduccion

1.1 Las organizaciones públicas y sus prioridades de seguridad de la información

Las entidades públicas con la seguridad de la información se ha visto con las nuevas generaciones en los estudios universitarios y demostrados siendo un gran desafío en todas las Organizaciones y se requiere que la información sea confidencial, de esta investigación se toma a las organizaciones púbicas que en la actualidad presenta problemas de riesgos en la información con los ataques informáticos y amenazas internas y externas, en las organizaciones públicas se ha permitido que información falsa y sin valor alguno tenga acceso y a su vez sean expuestas, dañe los lineamientos y no tenga protección sino que más bien ocasionen robos en la base de la información ingresada.

Dentro del estudio continuo los profesores demuestran que se debe dar mayor prioridad a la protección de los activos de la información porque este así genera confianza a los ciudadanos en el entorno y a su vez evita que tengan riesgos de vulnerabilidades informáticas dentro de las entidades [1] .

En las Organizaciones Públicas, hay muchas amenazas que pueden afectar a las mismas, se ha dicho que si las organizaciones conocieran y desarrollaran el proceso y considerara las metodologías no fueran cuestionadas, sino que más bien con esas protecciones en la seguridad cuidaran la información interna y de esa manera se alcanza los logros junto a una red de profesionales con gran conocimiento, a su vez teniendo en cuenta las recomendaciones ya que se lo considera una manera oportuna para ayudar ante los riesgos que sale a la luz en las organizaciones públicas y los recursos exploratorios permitan ser un complemento educativo y eficaz con el uso continuo de herramientas y metodologías tecnológicas [4].

En este artículo la metodología encuentra la inconsistencia que hay dentro del sistema ya que estas no han sido reflejadas y por mucho tiempo no sabían de la existencia, para llegar a este análisis reflejamos con las investigaciones por que para las organizaciones públicas los procesos que se realizaran e investigados ayuda a tener mayor control de las amenazas sin ser obligadas a ingresar a la base.

Se resulta que los investigadores realizan medidas de seguridad que las garantice y sus procesos sean factibles con fórmula de evaluación de riesgo y probabilidad de amenaza, prototipo de gestión de riesgos en organizaciones públicas y las técnicas necesarias para la creación de prototipos [13]- [14].

1.2 Normas ISO/IEC 2700

La serie 2700 se encuentran orientada con prácticas que ayudan a relacionarse junto a la implantación de seguridad en la gestión del sistema informático, y su mantenimiento dando a conocer que se tiene el objetivo establecido para manejar los aspectos que están

vinculados a la gestión realizada para mejorar la seguridad e incluso la mejora contigua y la mitigación de riesgos, se tiene muchas normas, pero las principales como:

- La ISO 27001 da una especificación para establecer requerimientos y gestionarlos por medio de un SGSI además realiza una adaptación de enfoques de los riesgos.
- La ISO 27002 define las prácticas para fundar el SGSI, por medio de los dominios, controles y sus objetivos.
- La ISO 27003 facilita en las implantaciones las guías de forma correcta, siendo centrados en realizar exitosos procesos.
- La ISO 27007 establece procedimientos para poder realizar de manera internas o externas auditorias siendo verificadas y certificadas incluyendo de la ISO/IEC 27001.
- La ISO 27009 junto a la norma 2701 se complementa en conjunto con requisitos y nuevos controles de aplicaciones para hacer más eficaz su implantación.
- La ISO 27011 establece principios para mantener y gestionar en las organizaciones un SGSI de telecomunicaciones indicando la implantación de controles eficaces.
- La ISO 27013 con un establecimiento de guía de las normas 27001 y el sistema de gestión de servicios en las organizaciones siendo ambas instauradas.
- La ISO 27017 nos facilita una guía de controles para los servicios cloud de manera específica incluso basadas en norma 27002.
- La ISO 27019 provee normas basadas al 27002 que aplicar las industrias vinculadas al sector de la energía.

Los SGSI o también llamados sistemas de gestión de seguridad de la información te permiten y te ayudan a que las organizaciones garanticen que todos los activos de la empresa sean adecuadamente manipulados que no se encuentren riesgos de fuga de la información.

2 Metodología

Con el estudio se pretende identificar y por medio de las investigaciones mostrar evidencias usando método deductivo incluyendo aplicaciones de criterio del SGSI, que corresponde a ISO/IEC 2700, análisis de riesgos y la investigación exploratoria para analizar los artículos encontrados en las referencias y en la información disponible en línea, la metodología que protege la información en su integridad, confidencialidad y disponibilidad garantiza la seguridad del sistema y los procesos de las organizaciones públicas y a su vez una medida de seguridad que mitiga la vulnerabilidad, amenaza y riesgos de sus procesos en las organizaciones para proteger la información.

Referente a las investigaciones se encuentra la inconsistencia que hay dentro del sistema en las organizaciones ya que estas no han sido reflejadas y por mucho tiempo no

sabían de la existencia teniendo medidas de seguridad que las garantice y sus procesos sean factibles con fórmula de evaluación de riesgo y probabilidad de amenaza, prototipo de gestión de riesgos en organizaciones públicas y fórmula de factor de privacidad y seguridad [8].

Table 1. Tabla de amenazas y Riesgos

Altos Riesgos	Medio Riesgos	Bajo Riesgos
(12-16)	(8-9)	(1-6)

Este proceso al analizar los riesgos es importante tener en cuenta las características que tienen estos, siendo este de manera dinámica o cambiante quiere decir que se realiza amenazas incluye vulnerabilidad, con caracteres diferentes y no siempre es percibido de manera similar entre las organizaciones públicas que nos suele da resultados inadecuados. Dependiendo los rangos sea altos, medio o bajo se señala en la tabla de probabilidades y magnitudes que reflejan cada amenaza.

Table 2. Tabla de probabilidades y magnitudes de amenazas

Magnitud de Daños				
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4
	Probabilidad de Amenazas			

Se aplicó en diferentes organizaciones públicas dado cuando más alta es la probabilidad y la magnitud el riesgo se hace más grande, lo que significa que es de total necesidad proporcionar la medida resguardando la seguridad y privacidad de la información. Gracias a esto se ha ido optado el estudio de mapeo sistemático que obtiene una visión amplia del campo académico, y viendo puntos educativos. Podemos observar los procesos de mapeo sistemático en Fig 1.

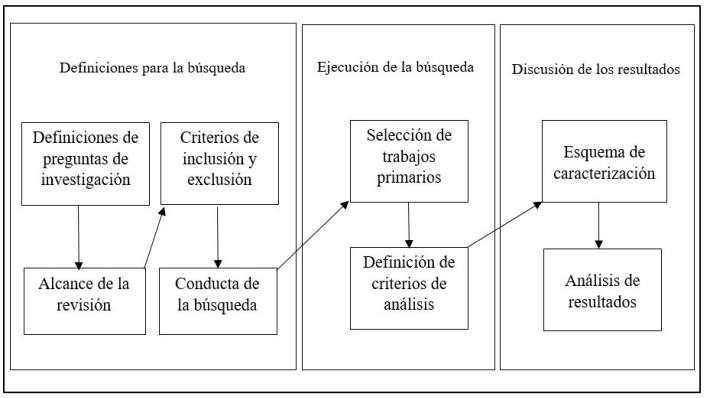

Fig 1. Procesos de mapeo sistemático

Por el análisis de este estudio se adquiere nuevos procesos siendo estos: definición de pregunta de investigación, ejecución de búsqueda y el análisis de resultados, todo como lo podemos ver en la Fig 1, considerando el mapeo sistemático y sus procesos.

Pregunta de investigación.

Ya que aún no se visualiza las guías para la tarea de requisitos con metodologías ágiles con control, se realiza la siguiente pregunta: ¿Que metodología o proceso ayuda a mejorar la seguridad en la gestión de la información dentro de las organizaciones públicas?

Table 3. Preguntas de Investigación

Preguntas de Investigación	Motivación
Q1. ¿Qué propuestas existen sobre los riesgos a los ataques informáticos?	Analizar los riesgos internos y externos de las organizaciones públicas con referencia a los ataques informáticos.
Q2. ¿Qué evidencia empírica existe de la aplicación en los ataques informáticos?	Implementar una metodología correcta para poder mitigar los riesgos en las entidades públicas
Q3. ¿Qué metodología se determina para la gestión de la información?	Determinar la metodología MAGERIT para resolución y análisis de problemas de privacidad y seguridad de la información.

Alcance de revisión.

En la actualidad se da a conocer el listado con la base de publicaciones en relación a la seguridad, nos hemos percatado en los principales riesgos y amenazas en las organizaciones realizando el análisis en el área informática. El desarrollo de esta investigación

se realizó con la mayor cantidad de publicaciones relacionadas. Además, se realizaron búsquedas analizadas, artículos relacionados, y otros.

Criterios de inclusión.
Para la investigación realizada con los estudios considerando los siguientes criterios de inclusión:

- Las publicaciones académicas se seleccionaron para su inclusión en el estudio con relación a la informática y proponiendo evaluar metodologías del desarrollo de la seguridad de manera ágil.
- También incluyendo estudios cualitativos, deductivos y realizados por estudiantes.

Estrategia de búsqueda.
Las identificaciones de los estudios primarios dieron los siguientes filtros:

1ero: Análisis y restructuración de Título.
2do: Investigación y revisión de Abstract.
3ero: Recopilación de publicaciones, artículos y análisis del mismo.

Estudios primarios.
En la búsqueda se dieron resultados que fueron analizados incluso se aumentó variables de los análisis de riesgos q fueron aplicadas se lo puede observar en table 4, luego que el filtro tres se aplicó siendo seleccionadas ciertas publicaciones de las cuales reflejan los estudios brindados, incluyendo la definición de los criterios de cada investigación que nos ayuda como esquema clasificando con el punto de vista a los estudios universitarios como en la parte educativa nuestro estudio de investigación se basa en los requisitos eductivos, siendo experimentados con casos controlados y analizados. La metodología teniendo la práctica encontrada no da una especificación del tipo de metodología ágil, con la posibilidad de ser aplicada en cualquier metodología.

Variables de análisis de riesgos en las organizaciones publicas.
En las investigaciones realizadas se tuvo en cuenta activos para la seguridad de la información por los incidentes, es por eso que urgentemente hemos analizado variables para el análisis de riesgos de la información [9].

Table 4. Variables aplicadas al análisis de riesgo

Activos	Amenazas	Vulnerabilidades
Base de datos	Pérdida de información	Backup no activa

Antivirus	Virus	Sin actualización de antivirus
Switch	Descargas eléctricas	Sin mantenimiento preventivo
Firewall	Carencia de actualización	Falta de actualizaciones
Equipos tecnológicos	Daño de Hardware	Sin mantenimiento preventivo

Esquema de Caracterización.
Se encontraron los trabajos usando metodologías y de las áreas de conocimiento y esto permite responder las preguntas planteadas en la investigación realizada para la seguridad en gestión de la información completa con el mapeo sistemático.

Table 5. Esquema de Clasificación

Preguntas	Respuesta
Q1. ¿Qué propuestas existen sobre los riesgos a los ataques informáticos?	**a.** Procesos **e.** Requisitos **b.** Métodos **f.** Otros **c.** SGSI **d.** Protocolo
Q2. ¿Qué evidencia empírica existe de la aplicación en los ataques informáticos?	**a.** Mapeo sistemático **e.** Otros **b.** Propuesta **c.** Evolución **d.** Requerimientos
Q3. ¿Qué metodología y normas se determina para la gestión de la información?	**a.** MAGERIT **b.** Familia ISO-IEC 2700(1,2,7 y 11) **c.** Otros

Análisis de resultados.

a. Pregunta Q1. Propuesta de los riesgos en los ataques informáticos

En la Fig 2 se muestra de manera gráfica los resultados de la pregunta Q1 de manera investigativa, podemos destacar que la mitad con un 52.14% proponen los metodos de las propuestas de riesgos por las cuales nos ayuda a mejorar la seguridad de la información para las entidades públicas, seguido este con SGSI 27.81% hablando de estos la gestión ayuda con sus procesos investigativos dándonos un 17.52% de investigaciones por las cuales nos dejan claro todo lo que nos beneficia para la gestión de la información.

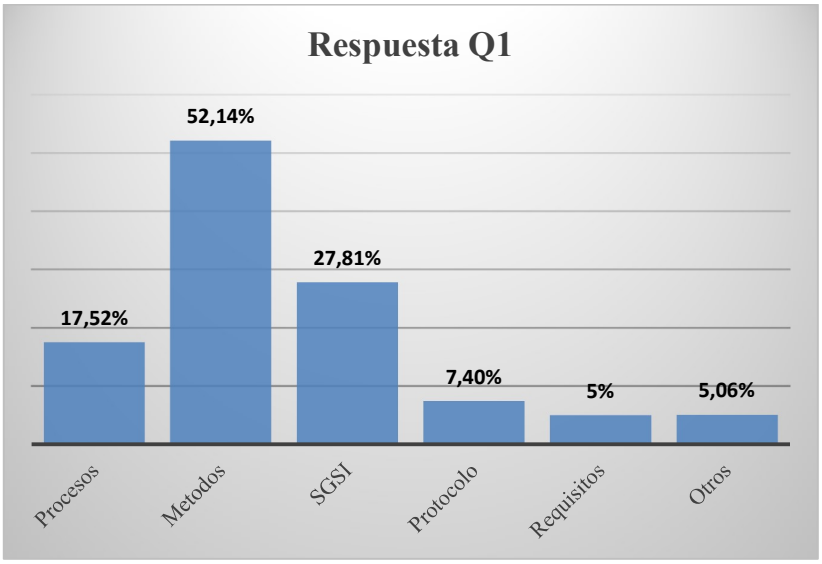

Fig 2. Resultado de esquema de clasificación Q1

b. Pregunta Q2. Evidencia empírica de la aplicación en los ataques informáticos

En la Fig 3. Se muestra de manera gráfica los resultados de la pregunta Q2 de manera investigativa, podemos darnos cuenta que tenemos un mapa sistemático con un 45.13%, con una propuesta de 21.10% y mostrando la evolución para poder así mejorar esos ataques que a las organizaciones les afecta y realizan muchas veces plagio de datos.

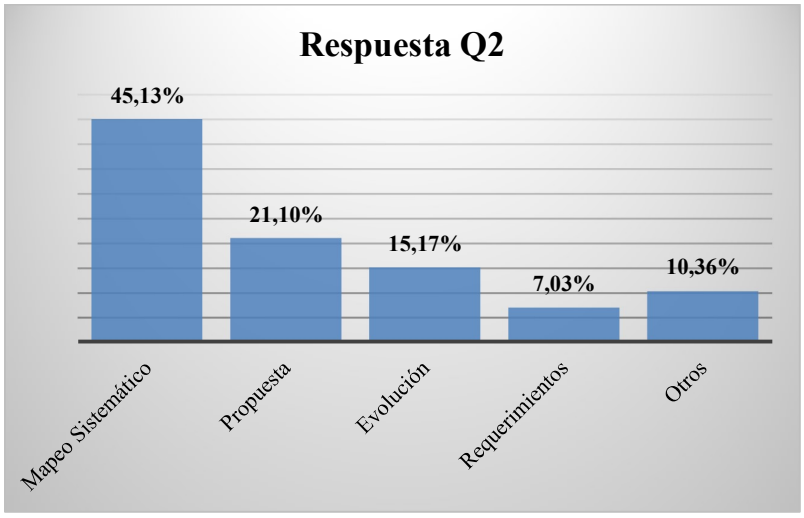

Fig. 3. Resultado de esquema de clasificación Q2

c. Pregunta Q3. Porcentaje del resultado de pregunta Q3 metodología y normas.

En la Fig 4. visualizamos con gráficos y los resultados de la pregunta Q3 de manera investigativa, podemos darnos cuenta que tenemos a MAGERIT como la metodología mas investigativa con un 56.90% porque es la que nos ayuda y nos demuestra la ayuda para la seguridad de la información, incluso las normas ISO-IEC 2700 con un 17.20%.

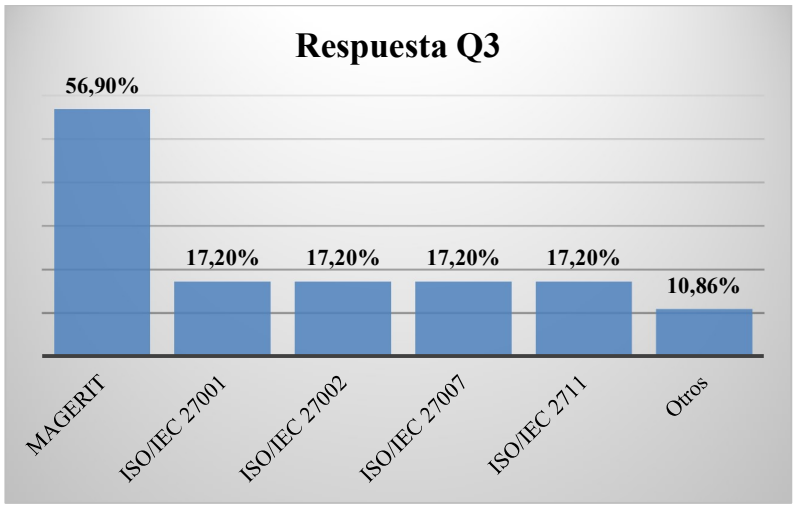

Fig 4. Resultado de esquema de clasificación Q3

3 Resultados

En las investigaciones se muestra un prototipo visualizándolo en el grafico a continuación este se da a conocer por medio de un diagrama de flujo los pasos para un proceso identificando los riesgos en las organizaciones públicas para las mejoras ya sea esta interna o externa, previniendo o reduciendo los riesgos que se conocen dentro de la organización, revisando la necesidad siendo esta una planificación antes analizada.

Dando una alternativa para así reducir los riesgos de seguridad en la gestión de la información y visualizar las mejoras, es por eso que las organizaciones públicas consideran la identificación de los riesgos para así tomar las medidas y ser abordadas, proporcionando los recursos necesarios en las organizaciones e implementando las acciones para que luego de las verificaciones para que la gestión de riesgos se mejore por las medidas tomadas para una mejor seguridad en la gestión de la información.

En el diagrama de flujo mostrado a continuación determina los riesgos, siendo cuestionado de manera interna y externa incluso teniendo requisitos que determinan los procesos y trata a los riesgos o amenazas para que no haya fallas, las organizaciones públicas muestran los riesgos tomando medidas sobre los análisis que se realiza para poderlos identificar y proporcionando recursos necesarios, los procesos operativos gestiona e implementan acciones, sean estas tomadas por riesgos ya que previene y reduce los mismos siendo actualizados durante su planificación sino fuera necesario regresara a identificar y luego termina el proceso.

La importancia es no perderle el sentido a la información organizacional en la privacidad y seguridad de la gestión dada junto con datos que se muestra el proceso y visualización que están representados, dando detalles y conocimientos técnicos que realizan la labor principal dentro del SGSI para así tomar las decisiones y realizar los ajustes necesarios junto a los objetivos antes mencionados.

También relacionado con MAGERIT que, con la generalización junto a las tecnologías de la información y su uso, refleja unos beneficios para las organizaciones, incluso da lugar a ciertos riesgos que de gran manera se minimiza con medidas de seguridad y refleja confianza para las organizaciones incluso conoce cuanto valor se está en juego y la ayuda para protegerlo.

Se descubre al planificar el tratamiento para que así los riesgos estén en bajo control, se prepara en si a las organizaciones para un gran proceso de evaluación, cada vez MAGERIT avanza con sus metodos, dando un proyecto de análisis, plan de seguridad y métodos, las organizaciones requieren gestionar procesos e implementar acciones, por las cuales se verifican y se previene o se reduce los riesgos siendo actualizados durante su planificación y se realiza un análisis para llevar un buen prototipo de gestión de riesgos.

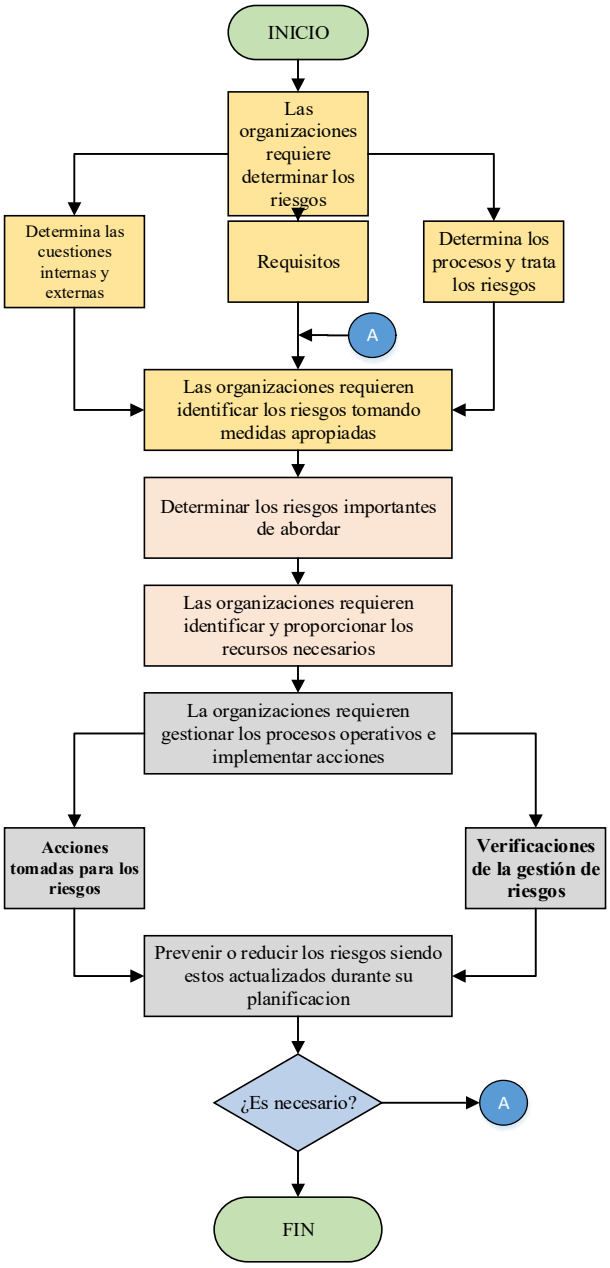

Fig 5. Prototipo de gestión de riesgos

El uso de recursos se recibió como una aceptación por parte de las nuevas generaciones y con las herramientas usadas que permite generar el objetivo exacto con un control de factores de ataques internos, los incidentes de seguridad de información siendo estas desde el 2007 en organización DPE (Defensoría pública del Ecuador) especificando el robo que fue más de 3 millones de registros en la cual incluyen los datos del banco y las tarjetas de créditos con datos personales el ministerio de telecomunicaciones realizó el análisis y se dieron cuenta de la filtración de da tos, el 6 de agosto del 2006 se produjo un ataque a AOL, 7 millones de usuarios afectados, en sus datos bancarios fueron llenos de compras en una página web y sin dejar atrás en el 2008 el ataque en la base en heartland payment systems se dio a exposición 134 millones de tarjetas de crédito y débitos, las cual hubieron robo de información, de identidad y de dinero [6]- [9], en 2010 se presentó ataques de 134 millones de usuarios que se afectó por los ataques en la base de datos, en el 2015 se dieron a conocer 165 millones de afectados no solo usuarios incluso hasta trabajadores por el mal uso de la base de datos que los riesgos llegaron hasta la perdida de dinero, 2018 se perdieron usuarios de 245 millones por las cuales produjo ataques en todas las páginas web dentro de la entidad.

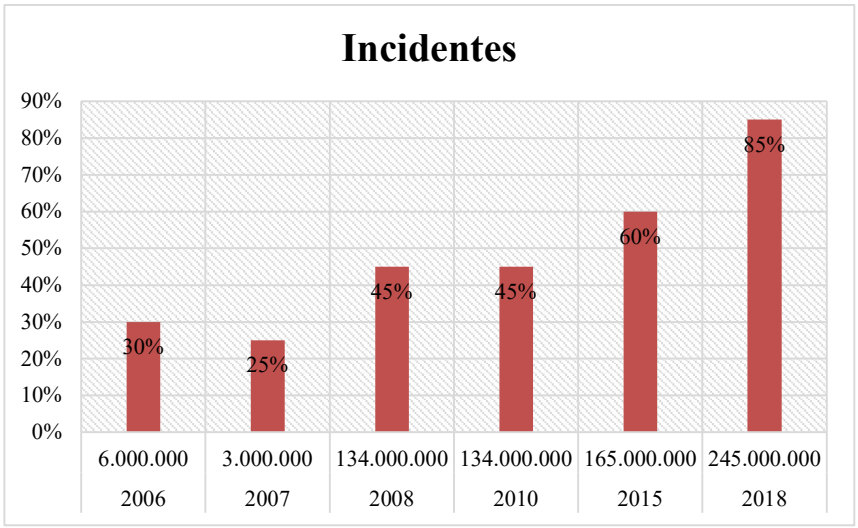

Fig 6. Gráfica de incidentes anuales con pérdida de millones de usuarios

Visualizando la figura, notamos la variedad de incidentes con su porcentaje y millones de pérdidas de usuarios anuales que tenía las entidades, se usaron técnicas y herramientas incluso metodologías para facilitar la comprensión y obtención de ayuda con la mejora de la información y realizar la seguridad, las técnicas son alineadas y demostradas en mapeo sistemático dando un buen objetivo para que gracias a la metodología se haga un desarrollo beneficioso dando presentación a los estudios primarios en el mapeo, validación y verificación de estrategias de búsqueda [28]- [30].

4 Discusión

El aprendizaje activo permite al estudiante involucrarse de forma más dinámica estimulando capacidades que permiten la observación detallada, analizando los riesgos que enfrentan las organizaciones públicas, para resolver el robo con el uso de la metodología con perseverancia a la garantía de la seguridad junto a los logros adquiridos en esta investigación es de suma importancia que las organizaciones públicas hayan recibido la información correcta para que puedan seguir la metodología y adaptarla. También ayudó a resolver que la información se encuentre segura y sin problemas. La metodología que se tenía en cuenta a pesar de que la metodología anterior no detuvo las amenazas o riesgos ocasionó daños, pero se eligió una metodología que ayudo a resolver el problema de manera eficaz.

Sin duda alguna, la metodología de MAGERIT analizó y ayudó de manera cualitativa y cuantitativa, basándose en elementos como la confidencialidad, la integridad y la disponibilidad siendo esta metodología es la alternativa correcta y efectiva para manejar la seguridad en las organizaciones públicas, sin olvidar el aporte del SGSI al mostrar los controles y beneficios de seguridad asociados, determinando los principales riesgos y enfoques para la gestión de riesgos, los cuales fueron ajustados a los requerimientos de privacidad y seguridad de las organizaciones públicas.

Se determina los riesgos en las organizaciones y se cuestiona de forma interna y externa teniendo requisitos por las que determina los procesos y trata a los riesgos o amenazas, las organizaciones públicas identifican los riesgos tomando medidas sobre el análisis que se realiza para poderlos abordar, identificando y proporcionando recursos necesarios, los procesos operativos lo gestiona e implementa acciones, sean estas tomadas por riesgos ya que previene y reduce los mismos siendo actualizados durante su planificación sino fuera necesario regresara a identificarlos procesos pero si lo es termina.

5 Conclusiones

Analizar, proponer y aplicar los riesgos con la metodología MAGERIT es una alternativa que permite mitigar las vulnerabilidades, amenazas y riesgos de sus procesos en las organizaciones públicas para proteger su información. MAGERIT es una medida de seguridad que permite mitigar las vulnerabilidades, amenazas y riesgos de sus procesos en las organizaciones públicas para proteger la información. El prototipo de Gestión de Riesgos mejora la seguridad e incluso la privacidad de la información en las organizaciones públicas.

Los resultados obtenidos están directamente vinculados a otras investigaciones junto al rol de seguridad informática incluyendo los estudios académico y los sistemas de información que se encuentran asociados [6] y un enfoque para optimizar la información de manera segura en las entidades públicas del Ecuador [15]- [18].

Cualquier prototipo basado en una metodología debe ser considerado como una alternativa para que organizaciones públicas se encuentren segura y resguardada la información.

Como trabajo futuro se plantea con respecto a los desarrollos de manera ágil, que a su vez facilita las prácticas necesarias identificando y obteniendo los productos de manera exitosa como beneficio para las organizaciones públicas [20].

Referencias

[1] M. A. Tejena-Macías, "Análisis de riesgos en seguridad de la información," Polo del Conoc., vol. 3, no. 4, p. 230, Apr. 2018. DOI:https://doi.org/10.23857/pc.v3i4.809.

[2] A. Singhal. "Development of Agile Security Framework using a Hybrid Technique for Requirements Elicitation". In Advances in Computing, Communication and Control, Springer, pp. 178-188. 2011

[3] S. M. T. Toapanta, F. G. M. Quimi, K. E. O. Pazmiño, R. M. Arrellano, and L. E. M. Gallegos, "Methodology to ensure information security in a distributed architecture for a public organization of Ecuador," in Frontiers in Artificial Intelligence and Applications, Oct. 2019, vol. 320, pp. 933–944. DOI:https://doi.org/10.3233/FAIA190267.

[4] M. Zhou, L. Han, H. Lu, C. Fu, and D. An, "Cooperative malicious network behavior recognition algorithm in E-commerce," Comput. Secur., vol. 95, Aug. 2020, DOI: 10.1016/j.cose.2020.101868.

[5] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," J. Netw. Comput. Appl., vol. 163, Aug. 2020, DOI: 10.1016/j.jnca.2020.102635.

[6] A. Singhal. "Development of Agile Security Framework using a Hybrid Technique for Requirements Elicitation". In Advances in Computing, Communication and Control, Springer, pp. 178-188. 2011.

[7] T. Srivatanakul, J.A. Clark and F. Polack. "Effective security requirements analysis: HAZOP and use cases". Information Security. Vol. 3225, pp. 416-427, 2004. DOI: https:// doi.org/10.1007/978-3-540-30144-8_35.

[8] S. M. Toapanta Toapanta, T. F. Prado Quintana, M. R. Maciel Arellano, and L. E. Mafla Gallegos, "Hyperledger technology in public organizations in Ecuador," in Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, Mar. 2020, pp. 294–301.DOI: https://doi.org/10.1109/ICICT50521.2020.00052.

[9] J. J. Cano M. and A. Almanza, “Study of the evolution of information security in Colombia: 2000-2018,” RISTI - Rev. Iber. Sist. e Tecnol. Inf., vol. 2020, no. E27, pp. 470–483, Mar. 2020. DOI:https://doi.org/10.1080/0144929X.2020.1771418

[10] C. Muyón and F. Montaluisa, “Information security methods to protect rest web services communication and data in http requests using json web token and keycloak red hat single sign on,” RISTI - Rev. Iber. Sist. e Tecnol. Inf., vol. 2020, no. E29, pp. 198–213, May 2020. DOI: https://doi.org/10.26599/TST.2018.9010031

[11] A. Bogantes, “El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados,” in CICIC 2020 - Decima Conferencia Iberoamericana de Complejidad, Informatica y Cibernetica, Memorias, 2020, vol. 1, pp. 57–62. DOI: https://doi.org/10.1007/978-981-13-8969-6_1

[12] D. Carrizo, O. Dieste and N. Juristo. “Systematizing requirements elicitation technique selection”. Information and Software Technology. Vol. 56, pp. 644-669, 2014. DOI: https://doi.org/10.1016/j. infsof.2014.01.009.

[13] M. Robles Carrillo, “Security of networks and information systems in the European Union: A comprehensive approach?,” Rev. Derecho Comunitario Eur., no. 60, pp. 563–600, May 2018. DOI:https://doi.org/10.18042/cepc/rdce.60.03

[14] L. Valencia, T. Guarda, G. P. L. Arias, and G. N. Quiña, “WSN security applied to smart metering systems based on cryptography techniques,” RISTI - Rev. Iber. Sist. e Tecnol. Inf., no. E17, pp. 393–406, Jan. 2019. DOI:https://doi.org/10.3233/JIFS-189167

[15] R. S. Cristóbal, “The reduction of number of parliamentary members and the modification of remuneration schemes for deputies in autonomous community,” Rev. Derecho Polit., vol. 92, pp. 73–118, 2015.

[16] D. Carrizo and J. Rojas. “Clasificación de prácticas de educción de requisitos en desarrollos ágiles: Un mapeo sistemático”. Ingeniare. Revista chilena de ingeniería. Vol. 24, p. 10. 2016. DOI: dx.doi.org/10.40.67/ S0718-33052016000400010.

[17] S. Moisés Toapanta Toapanta and L. Enrique Mafla Gallegos, “An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador,” in Fault Detection, Diagnosis and Prognosis, IntechOpen, 2020. DOI: https://doi.org/10.5772/intechopen.88931.

[18] M. Maguire. "Using human factors standards to support user experience and agile design". Lecture Notes Computer Science. Vol. 8009, pp. 185-194. 2013.

[19] A. Rallo Lombarte, “A new data protection law,” Rev. Esp. Derecho Const., vol. 2019, no. 116, pp. 45–74, 2019. DOI: https://doi.org/10.18042/cepc/redc.116.02

[20] A. R. Lombarte, “From «computing freedom» towards the constitutionalization of new digital rights (1978-2018),” Revista de Derecho Politico, no. 100. Universidad Nacional de Educacion a Distancia, pp. 639–669, Sep. 01, 2017. DOI: https://doi.org/10.5944/rdp.100.2017.20713

[21] M. Azhar et al., “Securing the human: Broadening diversity in cybersecurity,” in Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE, Jul. 2019, pp. 251–252. DOI: https://doi.org/10.1145/3304221.3325537

[22] C. Gralha, J. Araújo and M. Goulão. “Metrics for measuring complexity and completeness for social goal models”. Information Systems. Vol. 53, pp. 346-362, 2015. DOI: https://doi. org/10.1016/j.is.2015.03.006.

[23] VEBER, J., & KLÍMA, T. (2014). Influence of standards ISO 27000 family on digital evidence analysis. Paper presented at the IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, 103-111. Retrieved from www.scopus.com

[24] I. Hussain, S. Zahra, A. Hussain, H. D. Bedru, S. Haider, and D. Gumzhacheva, “Intruder attacks on wireless sensor networks: A soft decision and prevention mechanism,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 5, pp. 609–617, 2019. DOI: https://doi.org/10.14569/ijacsa.2019.0100578

[25] T. Katulic, “Transposition of EU network and information security directive into national law,” in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings, Jun. 2018, pp. 1143–1148. DOI: https://doi.org/10.23919/MIPRO.2018.8400208.

[26] M. T. Banday, “Applications of digital signature certificates for online information security,” in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018, pp. 756–804.

[27] SHRIVASTAVA, A., Kumar, A., Rai, A., Payal, N., & Tiwari, A. (2013). ISO 27001 compliance via Artificial Neutral Network. in computal intelligence and communication Network(CICN), (págs. 339-342).

[28] B. Damjanović, “ALGORITHM AES - STRUCTURE, TRANSFORMATIONS AND PERFORMANCE,” AKTUELNOSTI, vol. 3, no. 36, Dec. 2017. DOI: 10.7251/akt1636001d.

[29] S. M. Toapanta Toapanta, L. E. Mafla Gallegos, M. J. Chevez Moran, and J. G. Ortiz Rojas, "Analysis of models of security to mitigate the risks, vulnerabilities and threats in a company of services of telecommunications," in Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, Mar. 2020, pp. 445–450, DOI 10.1109/ICICT50521.2020.00077.

[30] L. Li, J. Pang, Y. Liu, J. Sun, and J. S. Dong, "Stateful Security Protocol Verification," Mar. 2014, Accessed: Jul. 02, 2020. [Online]. Available: http://arxiv.org/abs/1403.2237.

[31] K. Park, Y. Park, Y. Park, and A. K. Das, "E-Transactions Security Analysis," IEEE Access, vol. 6, pp. 30225–30241, 2018, DOI: 10.1109/ACCESS.2018.2844190.

[32] S. M. T. Toapanta, J. D. L. Cobeña, and L. E. M. Gallegos, "Analysis of cyberattacks in public organizations in Latin America," Adv. Sci. Technol. Eng. Syst., vol. 5, no. 2, pp. 116–125, 2020, DOI: 10.25046/aj050215.

[33] S. Delgado-Segura, C. Pérez-Solà, G. Navarro-Arribas, and J. Herrera-Joancomartí, "A fair protocol for data trading based on Bitcoin transactions," Futur. Gener. Comput. Syst., vol. 107, pp. 832–840, Jun. 2020, DOI: 10.1016/j.future.2017.08.021.

[34] J. M. B. Espalmado and E. R. Arboleda, "DARE Algorithm: A new security protocol by integration of different cryptographic techniques," Int. J. Electr. Comput. Eng., vol. 7, no. 2, pp. 1032–1041, 2017, DOI: 10.11591/ijece.v7i2.pp1032-1041

[35] M. Toapanta, Y. Terán, B. Naranjo and E. Mafla Security and Privacy in Information Management in a Distributed Environment for Public Organizations. DOI: 10.3233/FAIA200716

[36] N. Nesa and I. Banerjee, "A Lightweight Security Protocol for IoT Using Merkle Hash Tree and Chaotic Cryptography," in Advances in Intelligent Systems and Computing, 2020, vol. 996, pp. 3–16, DOI: 10.1007/978-981-13-8969-6_1.