UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

ARTICULO ACADÉMICO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

"ANALYSIS FOR THE ADOPTION OF SECURITY STANDARDS TO IMPROVE THE MANAGEMENT OF SECURITIES IN PUBLIC ORGANIZATIONS"

AUTORA

ALVARADO RONQUILLO MADELEINE LILIBETH

TUTOR:

ING. JOE LLERENA IZQUIERDO MSC

GUAYAQUIL – ECUADOR

2021

DECLARATORIA DE RESPONSABILIDAD

Yo, **MADELEINE LILIBETH ALVARADO RONQUILLO**, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro. Además, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de la autora.

Madeleine Alvarado R.

Nombre: **Madeleine Lilibeth Alvarado Ronquillo**

CESIÓN DE DERECHOS DE AUTOR

Yo MADELEINE LILIBETH ALVARADO RONQUILLO con documento de identificación N^{O} 0932034622 manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado intitulado: "...ANALYSIS FOR THE ADOPTION OF SECURITY STANDARDS TO IMPROVE THE MANAGEMENT OF SECURITIES IN PUBLIC ORGANIZATIONS..." mismo que ha sido desarrollado para optar por el título de: .INGENIERIA DE SISTEMAS.. en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a Io determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

(Firma)

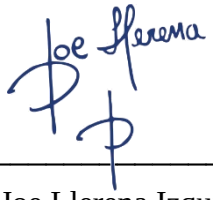
Nombre: Madeleine Lilibeth Alvarado Ronquillo

Cédula: 0932034622

Fecha: 16/11/2020

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Certifico que el presente artículo académico fue desarrollado por la señorita Madeleine Lilibeth Alvarado Ronquillo bajo mi supervisión.



Mg. Joe Llerena Izquierdo
Universidad Politécnica Salesiana,
Sede Guayaquil

Analysis for the Adoption of Security Standards to Improve the Management of Securities in Public Organizations

Segundo Moisés ToapantaToapanta*[1],Madeleine Lilibeth Alvarado Ronquillo[1], Luis Enrique Mafla Gallegos[2],Alberto Ochoa Zezzatti[3]

[1]Department Computer Science, Salesian Polytechnic University of Ecuador (UPS), Chambers 227 and June 5, Ecuador
[2]Faculty of Systems Engineering, National Polytechnic School (EPN), Ladrón the Guevara E11·253, Ecuador
[3]Industrial and Manufacturing Department, Autonomous University of Ciudad Juarez (UACJ), Av. Plutarco Elías Calles #1210, México

**Corresponding Author: Segundo Moisés ToapantaToapanta, Email:stoapanta@ups.edu.ec*

Abstract: Las organizaciones públicas tienen la tarea permanente de administrar adecuadamente la seguridad de la información que manejan. El objetivo de esta investigación es analizar los estándares de seguridad adoptados por las organizaciones públicas en Ecuador para mejorar su gestión de la seguridad de la información. Se aplicó el método deductivo para la revisión y análisis de estándares adecuados para las instituciones públicas. Como resultado, se obtuvo información sobre las diferentes políticas, estándares y lineamientos de seguridad que aplican, organismos públicos nacionales e internacionales. Resultó un Diagrama de actividades para la adopción de estándares para organismos públicos; un prototipo de modelo de gestión de la seguridad de la información basado en estándares; y una Matriz de Gestión de Seguridad de la Información, a partir de la cual se calculó el Porcentaje de Mitigación de Riesgos. Se concluyó que mantener altos niveles de seguridad en las organizaciones públicas requiere la adopción de estándares de control en diferentes áreas y la colaboración de los diferentes niveles organizativos y jerárquicos de las organizaciones públicas.

Keywords:*Security standards, Security management, Public organization, Information security*

Introducción

Las organizaciones públicas tienen la tarea permanente de administrar adecuadamente la seguridad de la información que manejan. Por ello, han tenido que considerar seriamente proteger su información a través de estándares normalmente aceptados que buscan evitar que la institución sea víctima de ciberdelincuentes [1]. En referencia a lo anterior, una figura de la Unión Internacional de Telecomunicaciones (UIT) menciona que Ecuador es el sexto país más ciberseguro de América Latina de un total de 19 países. A nivel latinoamericano, los países más ciberseguros son Uruguay y Brasil. Mientras que en todo el mundo dominan Singapur y Estados Unidos [2].

Las normas son normas escritas que están contenidas en un documento disponible al público, establecidas por consenso y adoptadas por un organismo reconocido;

establece las reglas, requisitos, características, lineamientos o recomendaciones generales que se deben seguir para lograr un nivel óptimo de regulación en un área en particular en relación a problemas actuales o problemas que puedan surgir en el futuro [3].

La falta de implementación de estándares de seguridad puede traer consigo una serie de problemas para las instituciones públicas ecuatorianas, como robo o filtración de información, ya sea por técnicas digitales como incrustación de software malicioso, virus que afectan el sistema, keyloggers para revelar códigos de acceso, spyware para recopilar información de los sistemas de forma maliciosa y utilizarla; Ataques de inyección SQL, ataques de denegación de servicio [4]. Luego está la ingeniería social a través de la cual ciertas personas ajenas o relacionadas con la organización, acceden a la información interna de la empresa y la utilizan para dañarla [5]. Y no debemos olvidar desastres naturales como incendios, deslizamientos de tierra, inundaciones o errores humanos [6].

Las instituciones públicas del Ecuador son un colectivo de organismos destinados a brindar y facilitar servicios a la comunidad. Actualmente existen 3251 instituciones públicas que forman parte directamente de la administración pública central u otras que pertenecen a gobiernos autónomos descentralizados. Las instituciones públicas del Ecuador, han implementado una serie de Sistemas Integrales de Información, lo cual ha facilitado los procesos o trámites ciudadanos. También están obligadas a integrar su información al Sistema Nacional de Información y su Gestión de Seguridad de la Información es evaluadada por el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL).

Sin embargo asegurar la confidencialidad, integridad y disponibilidad de la información sigue siendo un tema del cual la ciudadanía desconfía debido a diferentes hechos que han sido de conocimiento público en los últimos años:

- Filtración de datos de 20 millones de datos de ecuatorianos entre personas vivas y muertas, que incluían información personal, bancaria y hasta tributaria.
- Alteración de datos de ciudadanos en bases de datos del Registro Civil y elConsejo Nacional para la Igualdad de Discapacidades (CONADIS) para la obtención de beneficios o el cometimiento de actos delictivos.

Ataques de denegación de servicios a sitios web de entidades públicas.

A nivel internacional, organizaciones como The International Standard Organisation (ISO), han elaborado la familia de la norma ISO / IEC 27000, que contiene las mejores prácticas para el desarrollo, implementación y mejora continua de Sistemas de Gestión de Seguridad de la Información (SGSI) en organizaciones [7]. La implementación de este estándar permite a las organizaciones de cualquier tipo administrar adecuadamente la seguridad de sus activos, su información financiera, propiedad intelectual, datos de empleados e información confiada por terceros relacionados de alguna manera con la institución en Ecuador, el Servicio Ecuatoriano de Normalización (INEN) es la entidad encargada de velar por el cumplimiento de los requisitos de calidad de las instituciones públicas y privadas, en este sentido tiene facultades para regular y cumplir los requisitos para garantizar la seguridad de los usuarios y la prestación de un servicio de calidad. El Servicio Ecuatoriano de Normalización ha adoptado normas técnicas ISO y bajo el Esquema Gubernamental de Seguridad de la Información (EGSI) junto con el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), evalúan periódicamente la Gestión de la Seguridad de la Información de los organismos públicos ecuatorianos.

El objetivo de esta investigación es analizar los estándares de seguridad adoptados por las organizaciones públicas en Ecuador para mejorar su gestión de la seguridad de la información.

¿La implementación de estándares de seguridad en una organización pública ayuda a mejorar la gestión de la seguridad de la información?

La adopción de estándares de seguridad basados en normativas internacionales permite a las organizaciones establecer políticas, procedimientos y controles con el objetivo de reducir los riesgos a los que está expuesta la información. Debido a los controles de seguridad instalados, se puede lograr una mejora en la gestión de la seguridad, en términos de eficiencia y mejora continua.

La evaluación de los niveles de seguridad de la información en cada una de sus dimensiones garantizará la continuidad del negocio, así como la identificación temprana de los riesgos de seguridad y los posibles daños a la información. La evaluación de los controles y métricas de seguridad es necesaria ya que brindan información para la toma de decisiones en los tres niveles de decisión de las organizaciones: operacional, táctico y estratégico [8].

Se revisaron las siguientes referencias: An approach of National and International Cybersecurity Laws and Standards to Mitigate Information Risks in Public Organizations of Ecuador [9], An Empirical Study of Information Security Management Success Factors [10], Critical Success Factors Analysis on Effective Information Security Management: A Literature Review [11], Cyber-security Policy Framework and Procedural Compliance in Public Organisations [12], Identifying factors of "organizational information security management" [13], Organizational factors to the effectiveness of implementing information security management [14], Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study [15], Analysis of Appropriate Standards to solve Cybersecurity problems in Public Organizations [16], Adapting ISO 27001 to a Public Institution [17], Ecuadorian Standardization Service [18].

Se aplicó el método deductivo para la revisión y análisis de estándares adecuados para las instituciones públicas que permitan mejorar la gestión de la seguridad de la información.

Los resultados obtenidos fueron: un diagrama de actividades para la adopción de estándares para organismos públicos; un prototipo de modelo de gestión de la seguridad de la información basado en estándares; y una Matriz de Gestión de Seguridad de la Información, a partir de la cual se calculó el Porcentaje de Mitigación de Riesgos.

Mantener altos niveles de seguridad en las organizaciones públicas requiere la adopción de estándares de control en las diferentes áreas y la colaboración de los diferentes niveles organizativos y jerárquicos de las organizaciones públicas.

1. Materiales yMétodos

En primera instancia en Materiales se realizó una búsqueda de información de diferentes fuentes que permitió definir los estándares utilizados en los organismos públicos de gobierno y el proceso de adopción. En segundo lugar, en Métodos se definieron los pasos para lograr los resultados.

1.1 Materiales

1.1.1Esquema de seguridad de la información gubernamental - EGSI

Los organismos públicos ecuatorianos tienen la obligación y responsabilidad de proteger la información que manejan, gran parte de esta información tiene que ver con los ciudadanos y otra parte estrictamente con la gestión interna de la empresa. En cualquier caso, con el avance de las Tecnologías de la Información y las Comunicaciones (TIC), los organismos estatales han prestado mayor atención a la protección de sus activos de información y así generar confianza en la ciudadanía de que sus datos están seguros [16].

En Ecuador se han emitido Acuerdos Ministeriales con el fin de gestionar de manera eficiente y efectiva la seguridad de la información en las entidades públicas. A su vez, mantiene la Comisión de Seguridad Informática y Tecnologías de la Información y las Comunicaciones a cargo de las cuestiones de seguridad informática de las entidades gubernamentales [16]. Esta comisión fue creada con el propósito de analizar la situación de la seguridad de la información en las instituciones públicas del Estado ecuatoriano y ha llegado a determinar la necesidad de aplicar normas y procedimientos de seguridad de la información, e incorporar la cultura y los procesos institucionales, su gestión permanente, con este fin se elaboró el Esquema de Seguridad de la Información del Gobierno (EGSI).

El objetivo de EGSI es incrementar la seguridad de la información en las entidades públicas. La implementación del EGSI se realiza a través del Ciclo de Mejora Continua (PDCA), que consta de cuatro pasos: Planificar, Hacer, Actuar y Verificar.

Table 1: Clasificación de cumplimiento de EGSI

% de hitos cumplidos	Ponderación del nivel de cumplimiento de EGSI
90% a 100%	Alto
75% a 89%	Medio
50% a 74%	Regular
<50%	Bajo

El EGSI está dividido en 11 secciones y tiene 126 lineamientos o hitos prioritarios que deben ser evaluados y cumplidos por los organismos públicos en Ecuador [16]. La calificación final de cumplimiento de la EGSI se realiza de acuerdo con la Tabla 1.

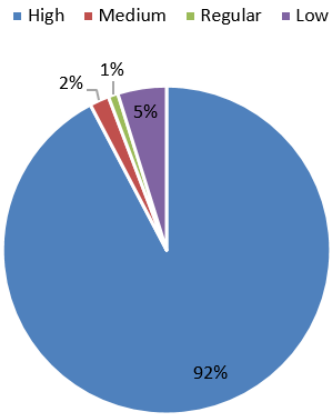


Figure 1.EGSI compliant entities

La Figura 1 muestra el nivel de cumplimiento de las organizaciones públicas en Ecuador, según los hitos que deben cumplir las organizaciones.

1.1.2ISO/IEC 27001: 2013

ISO / IEC 27001: 2013 es el estándar internacional que rige la gestión de la seguridad de la información. Especifica los requisitos que deben seguir las organizaciones con respecto a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) [17]. ISO / IEC 27001: 2013 define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información, dimensiones esenciales que deben ser cubiertas en mayor o menor medida, controles, estándares establecidos en una organización [11].

1.1.3ISO/IEC 27002: 2013

Describe el Código de prácticas para la implementación de controles de seguridad de la información. ISO / IEC 27002: 2013 proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización [13]. A través de ISO / IEC 27002: 2013, las instituciones podrán seleccionar los controles estandarizados adecuados que formarán parte del Sistema de Gestión de Seguridad de la Información de la organización. A través de este estándar, las empresas también pueden desarrollar sus propias pautas de gestión de seguridad de la información. El estándar cuenta con 114 controles, agrupados en 14 dominios y 35 objetivos de control que las organizaciones pueden adaptar según su naturaleza [6].

1.1.4INEN ISO/IEC 27002

INEN ISO / IEC 27002 es la norma técnica ecuatoriana, dirigida a instituciones derivadas de la Administración Pública Central, cuyo objetivo es la adecuada Gestión de la Seguridad de la Información. Este estándar es una traducción del estándar ISO / IEC

27002, por lo que su estructura es la misma que la del estándar internacional. La implementación del estándar establecido por el INEN sirve como referencia para que las instituciones públicas seleccionen y adopten controles comúnmente aceptados como parte del proceso de implementación del Esquema de Seguridad de la Información del Gobierno (EGSI) [18]. Según este estándar, los activos de una organización están en constante amenaza de verse afectados, en los que se involucran procesos, sistemas, redes y personas. Los cambios en los procesos, los sistemas comerciales y otros cambios externos pueden ser causas de riesgos para la seguridad de la información, por lo que es necesario implementar un conjunto de controles adecuados: políticas, procesos, procedimientos, estructuras organizacionales que utilizan software y hardware de recursos para garantizar que una organización cumpla con sus objetivos de seguridad y objetivos estratégicos.

1.2 Metodos

El objetivo de este estudio fue analizar los estándares de seguridad que pueden adoptar las organizaciones públicas ecuatorianas para mejorar su gestión de la seguridad de la información. Para ello, se aplicó el método deductivo para revisar y analizar los estándares adecuados para las instituciones públicas.

Con el objetivo de evaluar el impacto en la Gestión de la seguridad de la información producido por la adopción de controles estándar de seguridad, se desarrollaron y utilizaron escalas de valoración de Confidencialidad, Integridad y Disponibilidad de la información.

La creación del prototipo del modelo de Gestión de Seguridad de la Información se llevó a cabo en base al análisis de la norma ISO IEC 27001 y 27002. A partir de la norma 27001, se consideraron las dimensiones de seguridad de la información: confidencialidad, integridad y disponibilidad. De igual forma, se consideraron los 14 dominios del estándar 27002, resultado del análisis de 4 dimensiones propuestas que forman parte de las organizaciones públicas.

Para la evaluación del impacto producido por la adopción de controles en la Gestión de Seguridad de la Información, se tomó como referencia una agencia del Registro Civil del Ecuador, la cual forma parte de las instituciones que han culminado la primera fase del EGSI.

Table 2: Escala para valoración de Confidencialidad de la información

Escala	Valor	Criterio
Alto	3	El control es esencialmente importante y tiene un efecto crucial para asegurar la confidencialidad de la información
Medio	2	El control instaurado es medianamente importante para asegurar la confidencialidad de la información
Bajo	1	El control instaurado es importante asegurar la confidencialidad de la información

La Tabla 2 muestra la escala de calificación de la Confidencialidad de la información. La integridad y disponibilidad de la información se evaluaron con base en la misma escala. El objetivo de esta evaluación fue brindar valores cualitativos a cada valor

cuantitativo, en función de la importancia de establecer un control para asegurar la información de la empresa. La valoración cuantitativa de las dimensiones de la seguridad de la información, luego permitió calcular la valoración del impacto de los controles, la cual se llevó a cabo aplicando la siguiente fórmula:

$$VIC = \frac{C + I + D}{n} \qquad (1)$$

Donde C es Confidencialidad, I es Integridad, D es Disponibilidad, VIC es Evaluación de Impacto de Control yn es el Número de dimensiones de seguridad evaluadas, que para el caso es 3.

Table 3: Escala para valoración del Impacto del Control

Escala	Ponderación	Acción
Alto	3 - 2	Debe ser instaurado inmediatamente
Medio	1,99 - 1,01	Debe ser instaurado en el menor tiempo posible
Bajo	1	Debe ser instaurado cuando se cuente con los recursos

Los resultados de la Evaluación de Impacto de Control se ponderaron utilizando la escala de la Tabla 3. Luego se calcula el Porcentaje de Mitigación del Riesgo. Para hacer esto, primero calcule el VIC promedio usando la fórmula:

$$\bar{X} = \frac{\sum x}{n} \qquad (2)$$

Finalmente, con la media de X se calculó el Porcentaje de Mitigación de Riesgo, dividiendo la media de X por la puntuación máxima que puede obtener cada control, en este caso 3 y multiplicando por 100%.

$$PRM = \frac{\bar{X}}{3} * 100\% \qquad (3)$$

2 Resultados

2.1 Diagrama para la adopción de estándares en organismos públicos

La mejora de la Gestión de la Seguridad de la Información en las organizaciones públicas se puede lograr mediante la adopción de estándares, esto requiere que se sigan una serie de pasos básicos:

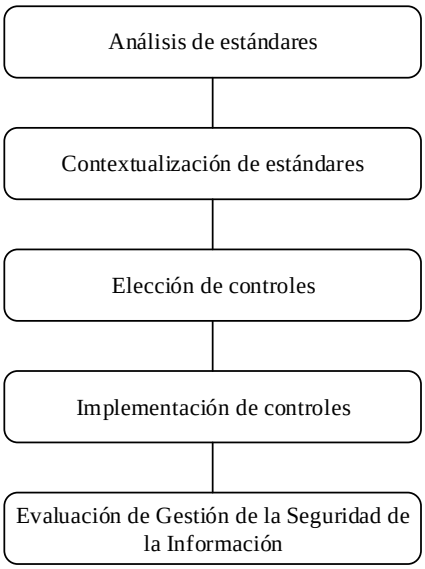


Figure 2. Adopción de estándares para mejora de la Gestión de la seguridad de la información

La Figura 2 muestra las actividades que se deben seguir para mejorar la Gestión de la Seguridad de la Información en las Organizaciones Públicas. El primer paso es la revisión y análisis de los estándares nacionales e internacionales, el segundo paso es contextualizar los estándares de acuerdo a la naturaleza de la organización para saber si los controles pertenecientes a ese estándar son aplicables a la organización pública, el tercer paso es la elección de los controles de seguridad de la información más adecuados a la naturaleza de la organización, el cuarto paso es la implementación de dichos controles, el último paso es la evaluación de la Gestión de Seguridad de la Información lograda con la implementación de los controles.

2.2Prototipo de un modelo de gestión de seguridad de la información basado en estándares

El análisis de las normas y estándares nacionales e internacionales que deben acatar las instituciones públicas del Ecuador, permitió la creación del siguiente prototipo del Modelo de Gestión de Seguridad de la Información basado en estándares.

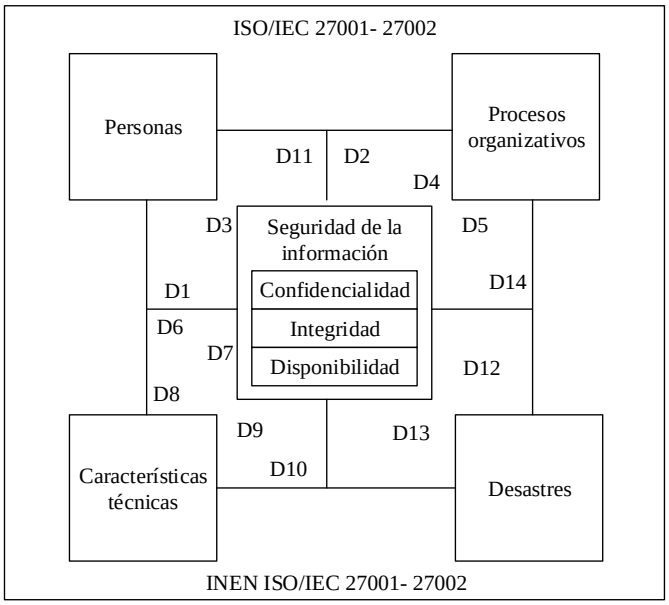


Figure 3. Gestión de seguridad de la información basada en estándares

Este prototipo integra los dominios de la norma ISO / IEC 27002 los cuales se clasificaron en 4 dimensiones: Personas, Procesos Organizacionales, Características Técnicas y Desastres. La gestión de la seguridad de la información se realiza en estas 4 dimensiones para lograr niveles satisfactorios de seguridad de la información en sus 3 dimensiones: Confidencialidad, Integridad y Disponibilidad.

Los diferentes controles de ISO / IEC 27002 que forman parte de las 4 dimensiones representadas en el modelo de la Figura 3, se pueden evaluar con el Método de Distancia Mínima. El método Distancia mínima a un punto ideal es un método que permite evaluar diferentes parámetros de objeto en un espacio matemático unitario de n dimensiones. El método de distancia mínima es una metodología que se puede utilizar para evaluar la seguridad informática en las organizaciones [6]. Con este método, las organizaciones públicas pueden evaluar los controles a partir de estándares adaptados, utilizando la siguiente ecuación:

$$d = \sqrt{(X_i - X_1)^2 + (X_i + X_2)^2 + \cdots (X_n - X_m)^2} \quad (4)$$

Ec. 4 calcula la distancia euclidiana, distancia desde cualquier punto en el espacio n-dimensional al punto perfecto (1, 1, 1, ...) o el punto que el usuario define como punto ideal teniendo en cuenta sus requerimientos y recursos disponibles, a partir de ahí puedes decidir cómo gastar los recursos para administrar la seguridad informática, esto es muy útil a la hora de optimizar recursos y se requiere dar mayor prioridad a unos controles que a otros. Dependiendo de si (1, 1, 1, ...), o cualquier otro punto se estableció como punto ideal, los valores de los parámetros pueden tomar valores muy cercanos a uno o al

punto ideal, lo que significa que son más importantes que el punto ideal. otros; y por tanto, la organización dedicará más recursos a controlar dichos parámetros.

2.3 Matriz de gestión de seguridad de la información

Se realizó una matriz de gestión de la seguridad en la que se ponderaron los diferentes controles que implementan los organismos públicos, según el impacto que dicho control produce en el mantenimiento de la seguridad de la información evaluada en sus 3 dimensiones.

Table 4: Matriz de Gestión de la seguridad de la información

Controles	**Impacto en la seguridad de la información**				**Escala**
	C	**I**	**D**	**VIC**	
Biométricos	3	1	1	1,67	Medio
Cámaras de seguridad	3	1	1	1,67	Medio
Firewalls	2	2	2	2	Alto
Antivirus	2	2	1	1,67	Medio
Controladora wireless, puntos de acceso	2	1	1	1,33	Medio
Respaldos de información	1	3	3	2,33	Alto

La matriz generada se muestra en la Tabla 4, donde el respaldo de discos duros obtuvo el mayor valor de impacto en la Gestión de Seguridad de la Información, seguido de la implementación de firewalls. El controlador inalámbrico para puntos de acceso es el control que obtuvo la calificación más baja.

Se determinó que el respaldo de discos duros y la implementación de firewalls, son controles que causan un alto impacto en la mejora de la Gestión de la Seguridad de la Información, por lo que estos controles deben ser implementados de manera inmediata con el fin de resguardar la información y los activos de la organización. La instalación de biometría, cámaras de seguridad, antivirus y configuración de controlador inalámbrico de puntos de acceso, son controles que provocan un impacto medio por lo que deben ser implementados en la organización en el menor tiempo posible.

2.4 Cálculo del porcentaje de mitigación de riesgos

Los resultados obtenidos en la Evaluación de Impacto de Control se utilizaron para calcular el Porcentaje de Mitigación de Riesgos.

$$\bar{X} = \frac{1,67 + 1,67 + 2 + 1,67 + 1,33 + 2,33}{6} = 1,78 \quad (5)$$

Ec. 5 calculó el promedio de las evaluaciones de impacto de los controles.

$$PRM = \frac{1,78}{3} * 100\% = 59,3\% \quad (6)$$

El cálculo del Porcentaje de Mitigación de Riesgo se realizó aplicando la Ec. 3 y permitió determinar áreas en las que se deben mejorar los controles para reducir los riesgos relacionados con la información.

3 Discussion

Este trabajo presenta un análisis para la adopción de Estándares de Seguridad con el fin de mejorar la Gestión de la Seguridad en Organizaciones Públicas. Cualquier organismo público que pretenda adoptar estándares nacionales e internacionales podrá aplicar la metodología propuesta en este trabajo.

El modelo de Gestión de la Seguridad de la Información desarrollado consideró las dimensiones descritas en ISO / IEC 27002, en otro estudio [17], y la ISO / IEC 27001.

En este estudio se desarrolló una Matriz de Gestión de la Seguridad de la Información con base en el impacto producido por los controles seleccionados de la norma ISO / IEC 27002 de acuerdo con la naturaleza de la organización; contrario a lo realizado en otros estudios donde analizan el impacto de un riesgo que se convierte en amenaza, lo que ayuda a determinar el nivel de riesgo según su impacto y probabilidad de ocurrencia; sin embargo, la propuesta desarrollada en este estudio es una alternativa más simplificada que se enfoca en la Gestión de la Seguridad para la mitigación de riesgos.

El porcentaje de mitigación de riesgo encontrado para una organización pública fue del 59,3%. En una investigación similar [9], este porcentaje fue del 58,6%..

4 Future Wordand Conclusion

En el futuro, se deben investigar los factores que influyen positiva o negativamente en la adopción de estándares en las organizaciones públicas.

Mantener altos niveles de seguridad en las organizaciones públicas requiere la adopción de estándares de control en diferentes áreas y la colaboración de los diferentes niveles organizativos y jerárquicos de las organizaciones públicas.

La mejora de la Gestión de la Seguridad de la Información requiere su evaluación en sus tres dimensiones: Confidencialidad, Integridad y Disponibilidad y se logra con una adecuada gestión de personas, procesos organizacionales, características técnicas y desastres en torno a los controles descritos en la norma. ISO / IEC 27002.

El respaldo de los discos duros y la implementación de firewalls son controles que producen un mayor impacto para garantizar la seguridad de la información, por lo que deben ser implementados de manera inmediata en todas las instituciones públicas con el fin de sobreproteger la información de la organización. La instalación de biometría, cámaras de seguridad, antivirus y configuración de controlador de punto de acceso inalámbrico son controles que causan un impacto medio, por lo que deben ser implementados en organismos públicos en el menor tiempo posible.

La mayoría de las organizaciones públicas de Ecuador han implementado el Esquema Gubernamental de Seguridad de la Información (EGSI) en conjunto con la norma INEN ISO / IEC 27002, que demuestra el avance de las organizaciones públicas ecuatorianas en el área de protección y gestión de la seguridad de la información.

5 Acknowledgments

The authors thank to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

[1] Cannon G, Statham P, Yamada A. Biometric Security, Standardization. Encycl Biometrics. 2009;122–9.

[2] Ministerio de las Telecomunicaciones y de la sociedad de la información. Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad. [Internet]. [Consulted 10 Jul 2012] Available in https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/

[3] Olifer D. Evaluation metrics for ontology-based security standards mapping. 2015 Open Conf Electr Electron Inf Sci eStream 2015 - Proc. 2015;17–20.

[4] Heimes R. Global InfoSec and Breach Standards. IEEE Secur Priv. 2016;14(5):68–72.

[5] Sedinić I, Perušić T. Security Risk Management in complex organization. 2015 38th Int Conv Inf Commun Technol Electron Microelectron MIPRO 2015 - Proc. 2015;(May):1331–7.

[6] Felipe FD, Acevedo EM, Sanchez MM. Evaluating informatics security in an organization: The minimal distance method. Proc 2017 IEEE 24th Int Congr Electron Electr Eng Comput INTERCON 2017. 2017;17–9.

[7] Lontsikh PA, Karaseva VA, Kunakov EP, Livshitz II, Nikiforova KA. Implementation of information security and data processing center protection standards. In: 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. 2016. p. 138–43.

[8] Doynikova E, Fedorchenko A, Kotenko I. Ontology of metrics for cyber security assessment. ACM Int Conf Proceeding Ser. 2019.

[9] Toapanta SMT, Gurumendi AJ, Gallegos LEM. An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of ecuador. ACM Int Conf Proceeding Ser. 2019;(December):61–6.

[10] Zammani M, Razali R. An empirical study of information security management success factors. Int J Adv Sci Eng Inf Technol. 2016;6(6):904–13.

[11] Tu Z, Yuan Y. Critical success factors analysis on effective information security management: A literature review. 20th Am Conf Inf Syst AMCIS 2014. 2014;1–13.

[12] Lubua EW, Pretorius PD. Cyber-security policy framework and procedural compliance in public organisations. Proc Int Conf Ind Eng Oper Manag. 2019;(July):1847–56.

[13] Singh AN, Gupta MP, Ojha A. Identifying factors of "organizational information security management." J Enterp Inf Manag. 2014;27(5):644–67.

[14] Chang SE, Ho CB. Organizational factors to the effectiveness of implementing information security management. Ind Manag Data Syst. 2006;106(3):345–61.

[15] Almubayedh D, Khalis M Al, Alazman G, Alabdali M, Al-Refai R, Nagy N. Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study. 21st Saudi Comput Soc Natl Comput Conf NCC 2018. 2018;1–6.

[16] T SMT, E GSG, Enrique L, Gallegos M. Analysis of Appropriate Standards to solve Cybersecurity problems in Public Analysis of Appropriate Standards to solve Cybersecurity problems in Public Organizations. In 2020.

[17] Carvalho C, Marques E. Adapting ISO 27001 to a Public Institution. Iber Conf Inf Syst Technol Cist. 2019;2019-June(June):19–22.

[18] Servicio Ecuatoriano de Normalización. NTE INEN-ISO/IEC 27002. 2017.