Entre Ciencia e Ingeniería, vol.13, no. 25, enero-junio de 2019, páginas 68-76. DOI: http://dx.doi.org/10.31908/19098367.4016.
ISSN 1909-8367 (Impreso), ISSN 2539-4169 (En línea)

Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana[1]

A proposal for the management of the information security applied to a Colombian public entity.

D. L. Carvajal, A. Cardona, F. J. Valencia

Recibido: agosto 23 de 2018 - Aceptado: mayo 30 de 2019

***Resumen*— La información es considerada actualmente uno de los recursos más importantes en las organizaciones, no solo como insumo fundamental de los procesos, sino como recurso que adecuadamente gestionado permite delimitar estrategias organizacionales, lo que no ha sido ajeno en el sector público, en especial en lo que tiene que ver con su protección. El presente artículo tiene como objetivo presentar un caso de aplicación de la gestión de seguridad de la información en una entidad pública, utilizando para ello, previa revisión de la literatura, cuatro de los estándares internacionales de seguridad de la información (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27003:2010 e ISO/IEC 27005:2008) y su contextualización en Colombia, a partir de las directrices establecidas por el Ministerio de Tecnologías de Información. Se obtuvo como resultado el desarrollo de una metodología ajustada a las necesidades de la entidad pública con parámetros e indicadores de gestión del riesgo y controles pertinentes para disminuir la incertidumbre en la gestión de la información. El aporte realizado por el presente trabajo está relacionado con la integración de estándares internacionales de seguridad de la información y su contextualización en un ámbito gubernamental, dando respuesta a requerimientos regulatorios y permitiendo una vez finalizada la implementación, contar con un desarrollo metodológico pertinente que le permite a la organización pública desarrollar de forma continuada los procesos de gestión de seguridad de la información.**

***Palabras clave*— Seguridad de la Información, ISO/IEC 27000; SGSI, Riesgos de TI.**

***Abstract*— Information is considered today one of the most important resources in organizations, not only as fundamental input of processes, but as a resource to properly run allows to define organizational strategies, what has not been outside in the public sector, especially in what it has to do with its protection. This article aims to present a case for the application of the management of information security in a public entity, using, prior review of the literature, four international information security standards) ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27003:2010 and ISO/IEC 27005:2008) and their contextualization in Colombia, from the guidelines laid down by the Ministry of information technologies. Resulted in the development of a methodology adjusted to the needs of the public entity with management of risk and controls relevant indicators and parameters to reduce the uncertainty in the management of information. The contributions made by this work is related to the integration of international standards of security of the information and their contextualization in a Government area, responding to regulatory requirements and allowing once After implementation, having a relevant methodological development that allows the public organization develop information security management processes continuously.**

***Keywords*— Information Security, ISO/IEC 27000, ISMS, IT Risks.**

I. INTRODUCCIÓN

La información es considerada actualmente uno de los activos más valiosos para las organizaciones y como tal debe ser adecuadamente protegida de manera conjunta con los activos tecnológicos que permiten su generación, procesamiento, almacenamiento, uso y comunicación para garantizar que esté disponible cuando se requiere, que solo sea accesible por las personas y los dispositivos autorizados y que no exista ningún tipo de modificación no autorizada.

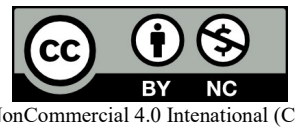
[1] Producto derivado del proyecto de investigación "Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie iso/iec 27000 para una entidad pública colombiana" Universidad Autónoma de Manizales.

D. L. Carvajal, Universidad Autónoma de Manizales, Manizales, Colombia, email: diana.carvajal.portilla@gmail.com

A. Cardona, Universidad Autónoma de Manizales, Manizales, Colombia, email: arturo.23.cardona@gmail.com

F. J. Valencia, Universidad Nacional de Colombia sede Manizales, Manizales, Colombia email: fjvalenciad@unal.edu.co

Como Citar este artículo: Carvajal, D. L; Cardona, A. y Valencia, F. J. Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana, Entre Ciencia e Ingeniería, vol. 13, no. 25, pp. 68-76, enero-junio 2019.
DOI: http://dx.doi.org/10.31908/19098367.4016.



Attribution-NonCommercial 4.0 Intenational (CC By-NC 4.0)

Particularmente las entidades del sector público requieren garantizar niveles aceptables de seguridad de la información, si se tiene en cuenta que en su mayoría es información de la ciudadanía que por lo general es sensible y debe ser adecuadamente protegida en términos de confidencialidad, integridad y disponibilidad.

Por lo anterior y teniendo en cuenta que es deber del estado y sus entidades salvaguardar la información de sus ciudadanos, el gobierno colombiano ha hecho esfuerzos por reglamentar y estandarizar los procesos asociados a la seguridad de la información a través de la estrategia de gobierno en línea (GEL) liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el cual contempla entre otros aspectos, normas y metodologías para cumplir con la obligatoriedad de las entidades públicas de implementar modelos de seguridad de la información acorde a las mejores prácticas a nivel internacional.

Es importante destacar algunos trabajos ya realizados, relacionados con factores críticos de éxito para implementar un sistema de gestión de seguridad de la información e implementación de este tipo de sistemas de gestión en entidades públicas.

En lo relacionado con factores críticos de éxito, algunos autores establecen como uno de los factores críticos un adecuado clima organizacional donde participen todos los niveles gerenciales [1], por su parte [2] establece premisas alrededor la evaluación periódica con marcos de referencia conocidos, el uso de enfoques creativos que mejoren la participación de los empleados, un lenguaje común y vocabulario amigable, la personalización de programas para grupos de usuarios y áreas; en [3] se proponen metodologías para tomar decisiones en inversiones de seguridad de la información sin sesgos personales a través de listas de verificación; por último se establecen prácticas de gestión del conocimiento como parte de las implementaciones de sistemas de gestión de seguridad de la información [4].

Con respecto a experiencias de implementaciones de sistemas de gestión de seguridad en entidades públicas, se encontraron trabajos como los desarrollados por [5] en Taiwan; [7] en Turquía, [8] en Sudáfrica, en Ecuador [9] y diversos trabajos académicos desarrollados en Colombia por parte de tesistas de diferentes universidades del país (e.g..[10]).

Este artículo es producto de la implementación de un proceso metodológico para el diseño de un sistema de gestión de seguridad de la información de una entidad pública colombiana, tomando como referencia algunas de las experiencias propuestas por la comunidad académica y profesional, además de los lineamientos establecidos por el gobierno nacional para tal fin, y fundamentalmente los referentes establecidos en las principales normas de la familia ISO/IEC 27000 a partir de la propuesta metodológica establecida en [6], por lo que se parte de una descripción de los lineamientos de la seguridad de la información en las entidades públicas para posterior a la presentación metodológica, dar a conocer los resultados propuestos en el presente artículo.

II. SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS

En el año 2016 el 46.7 % de las empresas en Colombia sufrieron algún tipo de incidente relacionado con la seguridad de la información [11], en diferentes modalidades como phishing, ransomware, ataques de denegación de servicios, fraudes internos y externos, infección de malware y explotación de diferentes vulnerabilidades. Las víctimas de estos ataques para el año 2016 en su mayoría son los ciudadanos con un 52%, seguido del sector financiero en un 14%, la industria tecnológica con el 8% y el sector gobierno con un 4%. Para este último, en los servicios de gobierno electrónico el malware se ha convertido en la principal amenaza, los atacantes utilizan correos falsos de entidades públicas para difundir y capturar la información de sus víctimas [12].

La seguridad de la información es un principio transversal en la protección de los derechos de los ciudadanos, la integridad del estado y la industria, es por ello que el estado colombiano desarrollo la estrategia gobierno en línea (GE) que tiene como objetivo tener un estado más eficiente, transparente y participativo, reglamentado de forma unificada a través del decreto 1078 de 2015 - *Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones*- de obligatorio cumplimiento para las entidades que conforman la administración pública colombiana [13], y en donde se establece su ámbito de aplicación, definiciones, principios y propósitos fundamentales.

Para cumplir con este objetivo, se establecieron plazos tanto para las entidades nacionales como territoriales, tal como se puede apreciar en las tablas I y II.

TABLA I
PLAZOS ENTES NACIONALES. [13]

Componente / Año	2015	2016	2017	2018	2019	2020
TIC para servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y privacidad para la información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

Como se puede apreciar entre el 2017 y el 2019 se espera una implementación cercana al 100 % por lo cual es importante hacer lo esfuerzos necesarios para cumplirlo.

Como apoyo al cumplimiento de la estrategia de gobierno en línea - en lo relacionado con el componente de seguridad y privacidad de la información- se estableció por parte de MinTIC el modelo de seguridad y privacidad de la información (MSPI) basado en familia de normas ISO/IEC 27000 [14], el cual proporciona un marco para su implementación en cualquier entidad pública.

TABLA II
PLAZOS ENTES TERRITORIALES. [13]

Componente/ año	Entidades A (%)				Entidades B (%)				Entidades C (%)			
	2017	2018	2019	2020	2017	2018	2019	2020	2017	2018	2019	2020
TIC para servicios	100	100	100	100	100	100	100	100	70	100	100	100
TIC para gobierno abierto	100	100	100	100	100	100	100	100	85	100	100	100
TIC para gestión	80	100	100	100	50	65	80	100	50	65	80	100
Seguridad y privacidad de la información	80	100	100	100	50	85	80	100	50	65	80	100

Cabe destacar algunas otras disposiciones del estado en materia de información y su manejo, una de ellas es la ley 1712 del 2014 catalogada como gobierno abierto, a través de la cual se reglamenta la transparencia y el derecho de acceso a la información [15], define principios como transparencia, buena fe, facilitación, gratuidad, eficiencia, calidad de la información y principio de divulgación proactiva de la información: Obligación de respuesta a las solicitudes de la sociedad y la publicación de información correspondiente a la actividad estatal de forma rutinaria y proactiva.

Asimismo la ley 1581 del 2012 de habeas data y los decretos 1377 del 2013 y 886 del 2014 que desarrollan el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política [16].

Las estrategias del gobierno, las diferentes reglamentaciones y la necesidad de asegurar la información dan pie al desarrollo de diferentes estrategias para cumplirlo.

III. METODOLOGÍA

Como punto de partida se llevó a cabo una revisión sistemática de literatura, con el fin de conocer aspectos metodológicos y experiencias en la implementación de sistemas de gestión de seguridad de la información tanto en entidades públicas como privadas, para lo cual se usó el método de revisión propuesto en [17], obteniendo referentes de autores y documentos tanto científicos como del sector productivo que sentaron las bases para su desarrollo.

De forma complementaria, se tomó como referencia la metodología propuesta en [6], donde se interrelacionan, tal como se puede observar en la Fig.1, cuatro de las principales normas de la familia de normas ISO/IEC 27000 para llevar a cabo la implementación de un sistema de gestión de seguridad de la información, la cual contempla los requisitos establecidos en la ISO/IEC 27001:2013 - *Sistema de gestión de seguridad de la información. Requerimientos*-; la ISO/IEC 27002:2013 -*Código de prácticas para controles de seguridad de la información*-; la ISO/IEC 27003:2010 - *Guía de implementación de un sistema de gestión de seguridad de la información*- y la ISO/IEC 27005:2008 - *Gestión del riesgo en la seguridad de la información*-.

Fig. 1. Principales normas de la familia ISO/IEC 27000 para implementar un Sistema de Gestión de Seguridad de la Información [6].

A partir de la combinación de ambos modelos y siguiendo algunas de las prácticas propuestas, se estableció como marco metodológico general las siguientes cinco fases:

1. Definición de alcance, límites y política del Sistema de Gestión de Seguridad de la Información (SGSI).
2. Análisis de los requisitos de seguridad de la información
3. Validación de riesgos y planificación del tratamiento de los riesgos
4. Valoración de riesgo
5. Diseño del SGSI

IV. DEFINICIÓN DEL ALCANCE Y DIAGNÓSTICO

Uno de los elementos más importantes en la implementación de un SGSI es el establecimiento del alcance del sistema, su importancia radica en que permite delimitar el proceso de gestión de riesgos y por ende pone foco a todo el proceso de implementación del SGSI. En tal sentido se realizó una revisión preliminar de los procesos de la entidad y la documentación existente, para posteriormente poder dar respuesta a las siguiente pregunta: ¿Cuál es la información más crítica que maneja la entidad, en función de su quehacer misional ?, para lo cual y con el apoyo del director de sistemas (funcionario responsable de la información en general y de la seguridad de la información en particular), se llegó a la conclusión de que la información financiera es la consideraba más crítica, por lo que a partir de allí se delimitó el alcance del SGSI. Sin embargo, cabe aclarar que las actividades llevadas a cabo para definir el SGSI en el alcance definido es aplicable de forma repetible y sistemática al resto de los procesos de la entidad.

Para llevar a cabo el diagnostico se tomó como referencia la plantilla denominada “Evaluación del MSPI” [14] proporcionada por MinTIC en el marco del proyecto

de máxima velocidad, el cual busca evaluar el nivel de madurez de las entidades a nivel nacional en lo relacionado con la implementación de GEL y particularmente la seguridad de la información. Este ejercicio fue desarrollado de forma conjunta con cada uno de los líderes de los procesos por medio de entrevistas y encuestas.

Como resultado de este proceso, y tal como se puede observar en la tabla III, los dominios de la ISO/IEC 27002:2013 mejor calificados fueron las políticas de seguridad de la información; la gestión de activos y el control de acceso. Mientras que aquellos dominios que obtuvieron menor calificación fueron: relaciones con los proveedores; gestión de incidentes de seguridad de la información y adquisición, desarrollo y mantenimiento de sistemas.

TABLA III
RESULTADOS DIAGNÓSTICO DE CONTROLES

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	60	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	60	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	27	60	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	60	60	EFECTIVO
A.9	CONTROL DE ACCESO	54	60	EFECTIVO
A.10	CRIPTOGRAFÍA	30	60	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	50	60	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	39	60	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	35	60	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19	60	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	60	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6	60	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	47	60	EFECTIVO
A.18	CUMPLIMIENTO	56	60	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		36	60	REPETIBLE

El promedio total de la evaluación de los controles de seguridad de la información establecidos en la ISO/IEC 27002:2013 arrojó como resultado un nivel de avance del 36%, muy por debajo de la meta prevista para el 2017 que era del 60%.

V. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La primera fase en un proceso de identificación de riesgos, es la identificación de los activos de información que hacen parte del alcance previsto, para lo cual se llevó a cabo un inventario de los activos de información que poseía la entidad y sus niveles de criticidad en función de los 3 pilares de la seguridad de la información: Confidencialidad, Integridad y, Disponibilidad, partiendo para ello de las recomendaciones propuestas en la guía 5 MPSI [18], - *Guía para la gestión y clasificación de activos de información*"-, la cual contempla la siguiente información para cada activo: nombre, nivel de clasificación de la información, información relacionada con su ubicación, tanto física como electrónica, propietario, custodio y usuarios y derechos de acceso.

En lo relacionado con la clasificación de la información, la guía establece criterios en función de la triada Confidencialidad, Integridad y Disponibilidad tal como se puede observar en la Fig.2, y cuyos criterios se describen a continuación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fig. 2. Valoración de activos por confidencialidad, integridad y disponibilidad [18].

Confidencialidad: definida por la norma ISO/IEC 27000 como la propiedad de que la información no esté disponible o revelada a personas, entidades o procesos no autorizados, y cuenta con las siguientes categorías de acuerdo a [18]:

Información pública reservada: Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

Información pública clasificada: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. No puede ser conocida por terceros sin autorización

Información pública: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Integridad: definida por la norma ISO/IEC 27000 como la propiedad de exactitud y completitud y cuenta con las siguientes categorías de acuerdo a [18]:

A (Alta): Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.

M (Media): Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.

B (Baja): Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

Disponibilidad: definida por la norma ISO/IEC 27000 como la propiedad de ser accesible y utilizable bajo la demanda de una entidad autorizada y cuenta con las siguientes categorías de acuerdo a [18] :

1 (Alta): La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

2 (Media): La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.

3 (Baja): La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

A partir de la aplicación de los criterios a cada uno de los activos y teniendo en cuenta los resultados obtenidos, se realiza la clasificación del nivel de criticidad de los activos, tomando como referencia la Fig. 3.

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fig. 3. Criticidad activos de información [18].

Fig. 4. Resultados criticidad activos de información.

Como resultado de este ejercicio se encontró la siguiente distribución de los activos de información como se muestra en la Fig.4

VI. ESTABLECIMIENTO DEL CONTEXTO DEL ANÁLISIS DE RIESGOS.

Los estándares de gestión de riesgos van desde enfoques clásicos hasta metodologías que incorporan la lógica difusa como parte de su evaluación, tal como se establece en [19]. En particular la norma ISO/IEC 27005:2008, establece como parte del contexto, la definición de parámetros, antes de llevar a cabo una valoración de riesgos. En tal sentido, se han definido como parte del proceso de gestión de riesgos, parámetros de probabilidad, impacto y criterios de aceptabilidad del riesgo por parte de la entidad pública.

A. Parámetros de probabilidad

Los parámetros de probabilidad establecen la frecuencia de ocurrencia de una amenaza, y por lo general se define en escalas que representan un descriptor y una frecuencia de ocurrencia, tal como se puede observar en la tabla IV, la cual ya estaba definida previamente por la entidad en ejercicios previos de gestión de riesgos.

TABLA IV
EJEMPLO DE PARÁMETRO DE PROBABILIDAD

Nivel	Descriptor	Descripción	Frecuencia
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años.

B. Parámetros de impacto

El impacto representa las consecuencias que podría tener la materialización de cualquier amenaza sobre la información o los activos de información, y por lo general, de acuerdo a la ISO/IEC 27001:2013, se miden en función de la confidencialidad, integridad y disponibilidad [20].

Los parámetros de impacto se deben definir para cada uno de los criterios de impacto, y para el caso de la entidad se definieron en compañía de los integrantes de la organización con una escala de 5 niveles. Una muestra de ellas se puede observar en la tabla V.

TABLA V
EJEMPLO DE PARÁMETROS DE IMPACTO DEFINIDOS EN LA ENTIDAD

Nivel	Descriptor	Criterio que se debe aplicar
	Confidencialidad	
2	Menor	La divulgación no autorizada de información podría tener un efecto adverso menor sobre las operaciones de la organización, los activos relacionados o sus individuos
	Integridad	
3	Moderado	La modificación o destrucción no autorizada de información podrían tener un efecto adverso moderado sobre las operaciones de la organización, los activos relacionados o sus individuos
	Disponibilidad	
5	Catastrófico	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso catastrófico sobre las operaciones de la organización, los activos relacionados o sus individuos

C. Parámetros de aceptabilidad del riesgo

Los criterios de aceptabilidad del riesgo permiten determinar a partir del cálculo del riesgo - resultante de la multiplicación de la probabilidad por el impacto -, el nivel de riesgo al cual está expuesta la organización y el apetito de riesgo o nivel de aceptabilidad del riesgo que tiene definida la organización. En este sentido se aplicaron los criterios de aceptabilidad del riesgo ya definidos previamente por la entidad, tal como se puede observar en la Fig. 5.

Es de resaltar el compromiso de la alta dirección en la definición y aprobación de los criterios de aceptabilidad teniendo en cuenta que a partir de allí se establecerán los niveles de riesgo inherente y residual y los compromisos

financieros futuros para seguir gestionando adecuadamente el riesgo a través de la implementación de nuevos controles de tecnologías de información.

Identificación	Criterio	Calificación
	B: Zona de riesgo baja, asumir el riesgo	<=3
	M: Zona de riesgo moderada, asumir/ reducir el riesgo	>3 y <=6
	A: Zona de riesgo alta, reducir, evitar, compartir o transferir el riesgo	>6 y <=10
	E: Zona de riesgo extrema, , reducir, evitar, compartir o transferir el riesgo	>10 y <=25

Fig. 5. Criterios de aceptabilidad del riesgo de la entidad.

D. valoración y tratamiento de riesgos.

De acuerdo con la norma ISO/IEC 27005:2008, la valoración de riesgos cuenta con tres fases: Identificación de riesgos, estimación del riesgo y evaluación del riesgo.

E. Identificación de escenarios de riesgo

Para la identificación de amenazas de los activos de información de la entidad (riesgos), se tomó como referencia el catálogo de amenazas Magerit - Metodología de análisis y gestión de riesgos de los sistemas de información - del Ministerio de Hacienda y Administraciones públicas de España[21], la cual contempla 43 amenazas dependiendo del tipo de activo.

Cada una de las amenazas fueron estudiadas en compañía de los responsables de la seguridad de la información de la entidad quienes seleccionaron las que a su juicio podrían llegar a materializarse, obteniendo un total de 34 posibles amenazas, entre las que se destacan los ataques intencionados con un 47%, tal como se puede apreciar en la Fig.6.

F. Estimación del riesgo

Para este punto y compañía de cada uno de los funcionarios de la entidad relacionados con los activos, se les solicita estimar la probabilidad de ocurrencia y su posible impacto, previa capacitación al respecto. Una vez determinados los valores, se realizar el cálculo del riesgo inherente (Probabilidad * Impacto) y a partir de allí se estima la vulnerabilidad inherente, entendida como el nivel de riesgo al que está expuesta la organización en cada uno de los riesgos, sin tener en cuenta los controles existentes. Los resultados arrojan un 50% de los riesgos con vulnerabilidad baja, seguido del 27% con vulnerabilidad media, 13% alta y 10% extrema, tal como se puede observar en la Fig. 8.

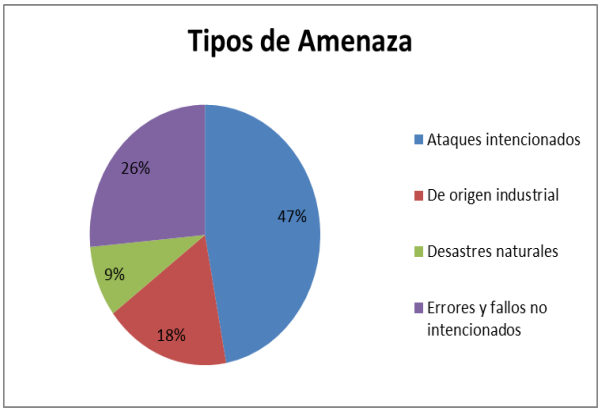


Fig. 6. Tipos de amenazas seleccionadas en la entidad.

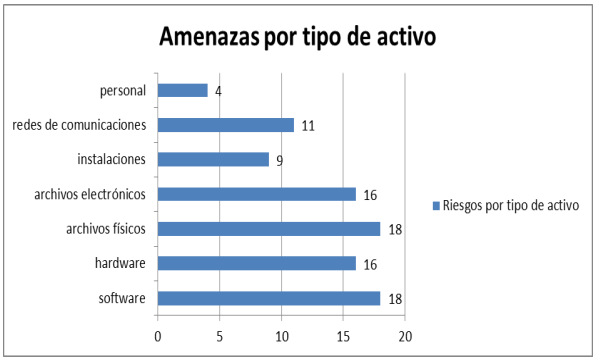


Fig. 7. Amenazas por tipo de activo

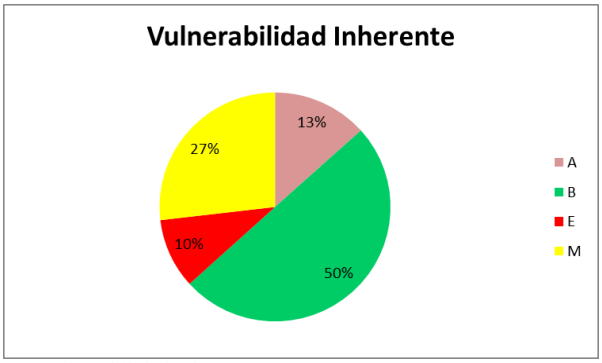


Fig. 8. Vulnerabilidad Inherente

También se puede analizar los riesgos por tipo de activo como se muestra en la Fig. 9, siendo el más representativo el software seguido por la información física y virtual (documentos).

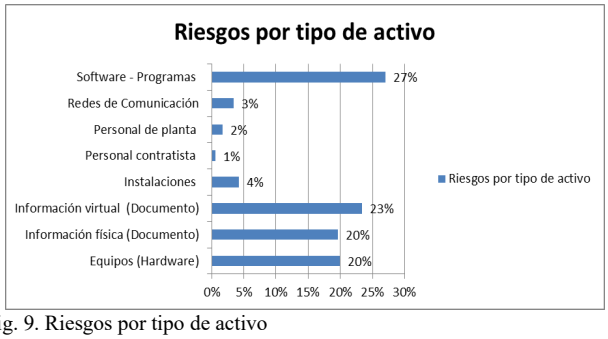


Fig. 9. Riesgos por tipo de activo

Por último podemos observar en la Fig.10 la vulnerabilidad de los riesgos por dimensión de seguridad siendo la disponibilidad de la información la dimensión que más afectación puede llegar a tener en la entidad pública.

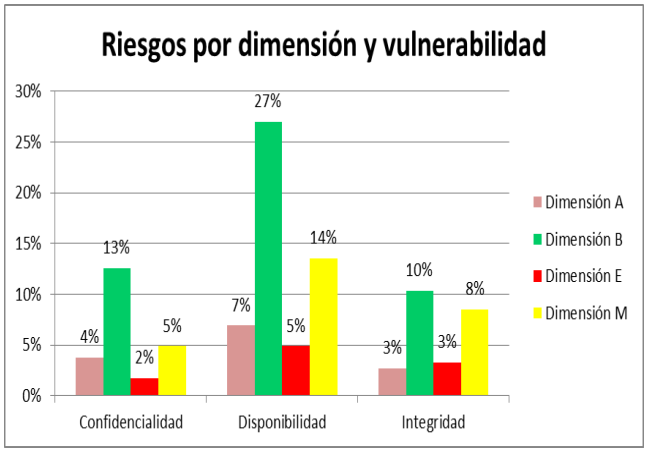


Fig. 10. Riesgos por dimensión y vulnerabilidad.

G. *Evaluación del riesgo*

La evaluación del riesgo permite determinar el riesgo residual, para lo cual de deben identificar inicialmente los controles que se encuentran actualmente implementados en la entidad y relacionarlos con los riesgos identificados, para posteriormente determinar el efecto que puede llegar a tener el control en la disminución de la probabilidad o el impacto, cuyos resultados en la entidad, se pueden observar en la Fig. 11, tomando como referencia la propuesta realizada por [6].

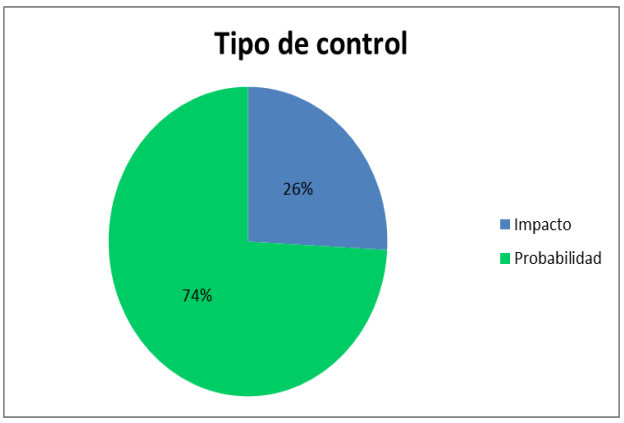


Fig. 11. Efecto de los controles existentes en la disminución del riesgo en la entidad.

Al aplicar la disminución de la probabilidad o el impacto con los controles existentes en la vulnerabilidad inherente, se obtiene la vulnerabilidad residual, cuyos resultados se puede observar en la Fig. 12.

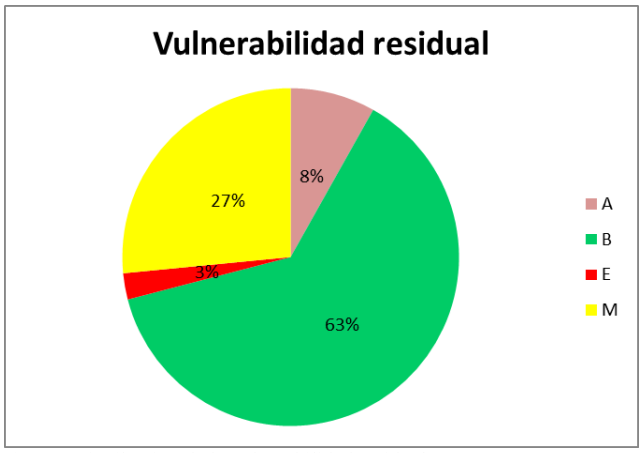


Fig. 12. Distribución de la vulnerabilidad residual.

TABLA VI
INFORMACIÓN DOCUMENTADA QUE DEBE TENER UN SGSI BASADO EN LA ISO/IEC 27001:2013 [6]

Numeral ISO/IEC 27001:2013	
4.3	*Determinación del alcance del SGSI*
5.2	*Política de seguridad*
6.1.2.	*Valoración de riesgos de seguridad de la información*
6.1.3	*Tratamiento de riesgos de seguridad de la información*
6.1.3	*Declaración de aplicabilidad*
6.2.	*Objetivos de seguridad de la información y planes para lograrlos*
7.2	*Competencia*
7.5.	*Información documentada*
7.5.3	*Control de la información documentada*
8.1	*Planificación y control operacional*
8.2.	*Valoración de la seguridad de la información*
8.3	*Tratamiento de riesgos de seguridad de la información*
9.1	*Seguimiento, medición, análisis y evaluación*
9.2	*Auditoría interna*
9.3	*Revisión por la dirección*
10.1	*No conformidades y acciones correctivas*
10.1	*No conformidades y acciones correctivas*

VII. DISEÑO DEL SGSI.

El diseño del sistema de gestión de seguridad de la información contempla las siguientes fases:

- Documentación del sistema, a partir de los requerimientos establecidos en la ISO/IEC 27001:2013 tal como se pueden observar en la tabla VI.
- Plan de tratamiento de riesgos, en el cual se documentan los controles propuestos para disminuir la vulnerabilidad residual y lograr llevar los riesgos identificados en la entidad a un nivel aceptable.
- Declaración de aplicabilidad, en la cual se muestran los controles de la norma ISO/IEC 27002:2013 contra los controles actuales y propuestos en la entidad

VIII. CONCLUSIONES

La revisión sistémica de literatura llevada a cabo, previa implementación del SGSI en la entidad, permitió establecer que para poder implementar exitosamente un sistema de gestión de seguridad de la información se deben tener en cuenta factores legales, sociales, culturales y organizacionales, siendo en el caso de la entidad pública objeto de implementación, el factor legal uno de los componentes indispensables y obligatorios para emprender un proyecto de esta magnitud.

De igual forma, dentro de los aspectos a tener en cuenta para lograr una exitosa implementación de un SGSI se deben tener en cuenta tres elementos indispensables: la concientización de los colaboradores, el compromiso de la alta dirección y la cultura organizacional, aspectos que fueron considerados como parte de la implementación.

Los resultados del diagnóstico de seguridad de la información de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 muestran un grado de avance en la entidad, por debajo de la meta planteada por MinTIC para el año 2017, con lo cual se evidencia la importancia del diseño e implementación del sistema de gestión de seguridad de la información y el cual una vez desarrollado permitió disminuir la vulnerabilidad existente, pasando en aquellos riesgos considerados de vulnerabilidad extrema de un 10% a un 3%; riesgos con vulnerabilidad alta de un 13% a un 8%; riesgos con vulnerabilidad media se mantiene en el 27% y los riesgos con vulnerabilidad baja aumentaron de 50% a 63%. Estos valores seguramente podrán disminuir mucho más si se implementan los controles propuestos en el plan de mitigación de riesgos.

Entre las dimensiones de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), los resultados muestran que la disponibilidad es la que representa las vulnerabilidades más altas, debido a que tiene la mayor cantidad de escenarios de riesgo y se fundamenta por la disponibilidad del software, de la información física y virtual que debe tener la entidad.

No obstante, los resultados arrojados, es necesario comprender que la seguridad de la información inicia como un proyecto, pero termina como un proceso más de la organización, que debe seguir siendo gestionado de forma permanente.

REFERENCIAS

[1] Bauer, S., Bernroider, E. W., y Chudzikowski, K. «Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks.,» Computers and Security, nº 68, pp. 145-159, 2017.

[2] Chan, M., Woon, I., y Kankanhalli, A. «Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing ,National University of Singapore Atreyi Kankanhalli School of Com.,» Journal of Information Privacy and Security, vol. 1, nº 3, pp. 18-41, 2005.

[3] Dor, D., y Elovici, Y. «A model of the information security investment decision-making process.,» Computers & Security, nº 63, p. 1–13, 2016.

[4] Said, A. R., Abdullah, H., Uli, J., y Mohamed, Z. A. «Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation.,» Procedia - Social and Behavioral Sciences, vol. 123, pp. 433-443, 2014.

[5] Ku, C. Y., Chang, Y. W., y Yen, D. C. «National information security policy and its implementation: A case study in Taiwan.,» Telecommunications Policy, vol. 33, nº 7, pp. 371-384, 2009.

[6] Valencia, F. J., y Orozco, M. «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO / IEC 27000.,» RISTI, nº 22, p. 73–88, 2015.

[7] Ozkan, S., y Karabacak, B. «Collaborative risk method for information security management practices: A case context within Turkey,» International Journal of Information Management,, vol. 30, nº 6, pp. 567-572, 2010.

[8] Patrick, H., Van Niekerk, B., y Fields, Z. «Information Security Management: A South African Public Sector Perspective,» de Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution. IGI Global., IGI Global, 2018, pp. 382-405.

[9] Patiño, S., y Yoo, S. G. «Study of the Maturity of Information Security in Public Organizations of Ecuador,» de International Conference on Technologies and Innovation, 2018.

[10] Campos, J. F. «Seguridad de la información en el sector público colombiano,» 2015.

[11] ESET, «ESET Security Report Latinoamérica 2017,» 19 03 2018. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf.

[12] Centro cibernético Policial, «Amenazas del Cibercrimen en Colombia 2016-2017,» Bogotá, 2017.

[13] MINTIC, «Decreto Numero 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones,» Bogotá, 2015.

[14] MINTIC, «Modelo de Seguridad y Privacidad de la Información.,» Bogotá, 2016.

[15] Congreso de la República de Colombia, «Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional [Ley 1712 de 2014],» Bogotá, 2014.

[16] Congreso de la República de Colombia, «Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.,» Bogotá, 2012.

[17] Kitchenham, B. «Procedures for Performing Systematic Literature Reviews,» 2004. [En línea]. Available: http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf. [Último acceso: 15 1 2019].

[18] MINTIC, «Guía para la Gestión y Clasificación de Activos de Información,» Bogotá, 2016.

[19] A. A. Angarita, C. A. Tabares y J. I. Rios, «Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento,» Entre Ciencia e Ingeniería, vol. 9, nº 17, pp. 71-80, 2015.

[20] Valencia, F. J., Marulanda, C. E., y López, M. «Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional,» Gerencia Tecnológica Informática, vol. 15, nº 41, pp. 65-77, 2015.

[21] Direcciòn General de Modernizaciòn Administrativa Procedimientos e Impulso de la Administraciòn Electrònica., «MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Mètodo,» 2012.

Diana Lizeth Carvajal Portilla. Ingeniera de sistemas y telecomunicaciones en la Universidad Católica de Pereira. Culminó la Maestría en gestión y desarrollo de proyectos de software de la Universidad Autónoma de Manizales.

ORCID: https://orcid.org/0000-0001-5581-9054

Arturo Cardona Londoño Ingeniero de sistemas y computación en la Universidad Tecnológica de Pereira. Culminó la Maestría en gestión y desarrollo de proyectos de software de la Universidad Autónoma de Manizales.
ORCID: https://orcid.org/0000-0002-3173-9962

Francisco Javier Valencia Duque. PhD en Ingeniería, Industria y Organizaciones. Máster en Administración de Tecnologías de información del ITESM, Especialista en diseño de sistemas de auditoría. Ingeniero de Sistemas y Administrador de Empresas. Profesor Asociado Universidad Nacional de Colombia. Certificaciones internacionales CISA, CRISC, COBIT Foundations y Auditor líder ISO/IEC 27001. ORCID: https://orcid.org/0000-0002-0617-2386