Ciencia & Desarrollo, Vol. 16, 21 (2) 100 - 112 (2017)
ISSN 2304 – 8891 Versión impresa
Depósito legal N° 2017-16148

GESTIÓN DE ACTIVOS BASADO EN ISO/IEC 27002 PARA GARANTIZAR SEGURIDAD DE LA INFORMACIÓN

ASSET MANAGEMENT BASED ON ISO / IEC 27002 TO GUARANTEE INFORMATION SECURITY

[1]Henry George Maquera Quispe, [2]Paola Nhataly Serpa Guillermo

RESUMEN

Muchas empresas carecen de controles de seguridad por lo que no pueden garantizar la seguridad de la información. El avance tecnológico y una gestión de la información, cada vez más compleja traen consigo la presencia de diversos tipos de amenaza que buscan reducir los niveles de servicio de los activos del área de proyectos digitales del Grupo de Periodismo Digital (GPD). Esta investigación se encaminó a la implementación y utilización de mecanismos de control para la gestión de activos basada en la norma internacional ISO/IEC 27002 bajo el objetivo de evaluar los niveles de seguridad en los activos de información mediante métricas formuladas a través de la guía de medición del desempeño para la seguridad de la información del NIST (National Institute of Standards and Technology). Un análisis de riesgos por cada tipo de activos permitió establecer que los mecanismos implementados basados en controles administrativos – técnicos – físicos han logrado reducir los niveles de riesgo. La gestión de activos de información ha permitido elevar las métricas de seguridad de la información y estrategias de seguridad con el fin de garantizar la continuidad de los procesos establecidos por el Grupo de Periodismo Digital mediante planes de continuidad de negocios y planes de recuperación ante desastres.

Palabras Clave: Activos de información, amenaza, control de riesgo, seguridad de la información, vulnerabilidad.

ABSTRACT

Many companies lack of security controls so they can not guarantee the security of information. Technological progress and information management, increasingly complex bring with them the presence of various types of threats that seek to reduce the service levels of the assets of the digital projects area of the Digital Journalism Group (GPD). This research was aimed at the implementation and use of control mechanisms for asset management based on the international standard ISO / IEC 27002 with the objective of evaluating security levels in information assets through metrics formulated through the guidance of performance measurement for information security of the NIST (National Institute of Standards and Technology). A risk analysis for each type of asset allowed to establish that the implemented mechanisms based on administrative - technical - physical controls have managed to reduce the levels of risk. The management of information assets has made possible to raise the information security metrics and security strategies in order to guarantee the continuity of the processes established by the Digital Journalism Group through business continuity plans and disaster recovery plans.

Keywords: Information assets, threat, risk control, information security, vulnerability.

INTRODUCCIÓN

Las empresas demandan la información y servicios de tecnologías de información como activos esenciales para la buena gestión de sus procesos. El aumento a la dependencia a estos dos tipos de activos genera la aparición de nuevos tipos de amenazas que aprovechan diversos puntos de vulnerabilidad que una empresa no atiende o desconoce. Esta situación se agrava cuando la gestión del conocimiento es una característica vital, por lo que una violación a los mecanismos de seguridad establecidos puede generar incidentes que afecten los niveles de productividad bajo el negativo impacto en la integridad, disponibilidad y confidencialidad de la información, y con el consiguiente aumento en los niveles de desconfianza en los clientes del Grupo de Periodismo Digital (GPD).

ESET latinoamericana (2015) encuestó a 3 369 ejecutivos en el año 2014 para recopilar información sobre el panorama actual de la seguridad de la información. La figura 1 muestra que diversas empresas han sufrido infecciones de malware, phishing, denegación de servicios, falta de disponibilidad de servicios, acceso indebido, fraudes

[1]Facultad de Ingeniería de Sistemas, Universidad Nacional del Centro del Perú. Huancayo-Perú. E-mail: Henry.maquera@gmail.com, henry.maquera@uncp.edu.pe
[2] Facultad de Ingeniería de Sistemas, Universidad Nacional del Centro del Perú. Huancayo–Perú. E-mail: paolaserpaguillermo@gmail.com

Presentado: 16/11/16 Aprobado: 01/08/17

interno/externos, entre otros. La figura 1 indica que la infección de malware, acceso indebido a aplicaciones o base de datos son los tipos de incidentes más frecuentes en diversos tipos de empresa.

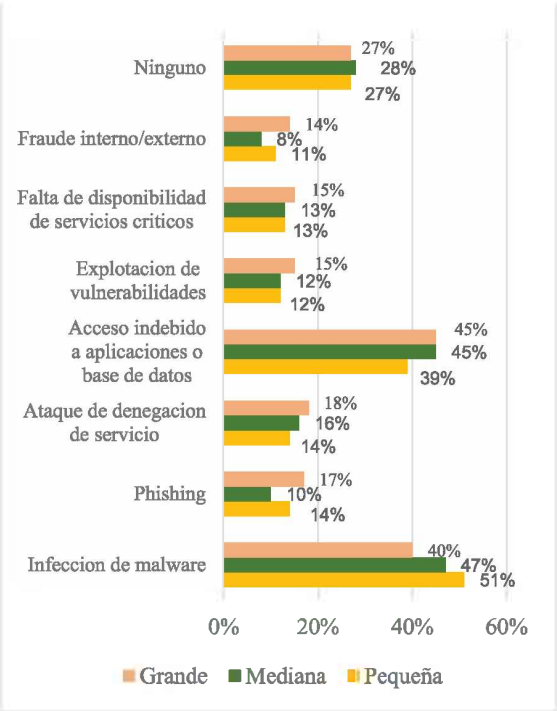

Figura 1. Incidentes sufridos por empresas latinoamericanas
Fuente: ESET (2015)

Las mejores prácticas para garantizar seguridad de la información se basan en el uso de tecnología de información. La figura 2 expone que el 92% de empresas utilizan software antivirus, el 85%, firewalls, el 74%, backup de información y que existe una desatención en los controles de los tipos de doble autenticación, soluciones de seguridad de móviles y tecnologías de cifrado.

El Grupo de Periodismo Digital (GPD) es un empresa que agrupa la información de diversos diarios de circulación nacional y medios de periodismo digital que busca como meta mantenerse en el mercado peruano como el principal medio informático y lograr consolidar una sólida marca. Los ejecutivos del GPD son conscientes de la importancia de la información gestionada por los sistemas de información; sin embargo, no logran comprender la criticidad de la misma en los procesos de la empresa. De igual manera, advierten la presencia de amenazas e impacto generado que es producto del éxito en aprovechar alguna vulnerabilidad existente.

El área de proyectos digitales del GPD ha sufrido diversos tipos de ataque que han generado deficiencias en el normal funcionamiento en los procesos de la empresa. La figura 3 expone el porcentaje de tipos de ataque que se han venido suscitando durante los años 2014 y 2015. Se aprecia que la mayor cantidad de ataques que han afectado a la empresa son del tipo de virus con un 55% y el ataque del tipo de sabotaje con un 2% ha sido el que se ha suscitado en menor cantidad.

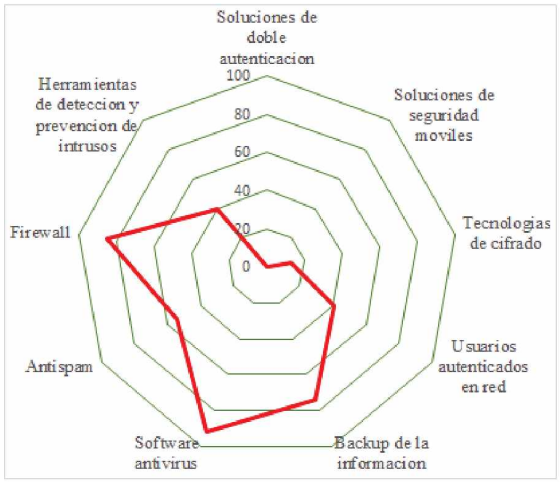

Figura 2. Implementación de controles tecnológicos.
Fuente: ESET (2015)

Estas incidencias se encuentran registradas de manera informal en una bitácora de incidentes sin un registro auditable y menos controlable que permitiría establecer el punto de inicio de mecanismos de control sostenibles en el tiempo. Lo que ha quedado establecido son los impactos en el área de proyectos digitales del GPD que se establecen en la figura 4, donde el mayor impacto negativo se identifica en los servicios internos afectados o detenidos con un 28% mientras que, los impactos de disponibilidad, confidencialidad e integridad de la información o datos fueron afectados con 18%, 17% y 16% respectivamente.

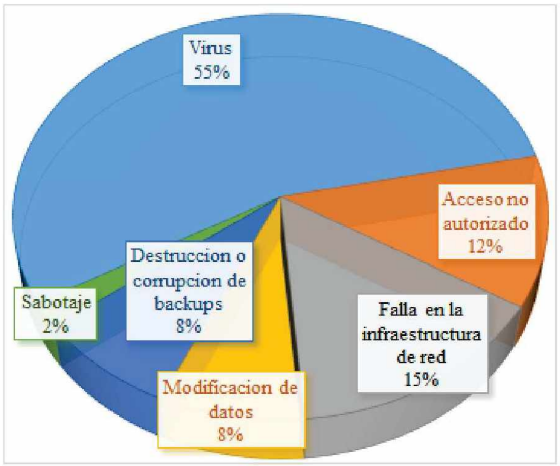

Figura 3. Incidencias de ataque-Grupo de Periodismo Digital (GPD)
Fuente: Elaboración propia

De la figura 4 se puede interpretar que la información ha sufrido un 51% de impacto negativo en los diversos tipos de ataque que han afectado al área de proyectos digitales del GPD. Ello se debe a que esta empresa

tiene como objetivo gestionar diferentes espacios publicitarios en diversos medios de comunicación masiva, por lo que la información es su principal activo para generar valor. Debido al rubro empresarial, la empresa tiene una alta dependencia a la información; sin embargo, no se tiene establecido una categorización de los tipos de activos de información o políticas de seguridad basadas en algún estándar internacional. Por lo que la investigación se enmarcó en determinar el impacto de la gestión de activos de información en el nivel de seguridad de la información del área de proyectos digitales del GPD basada en la norma internacional ISO/IEC 27002.

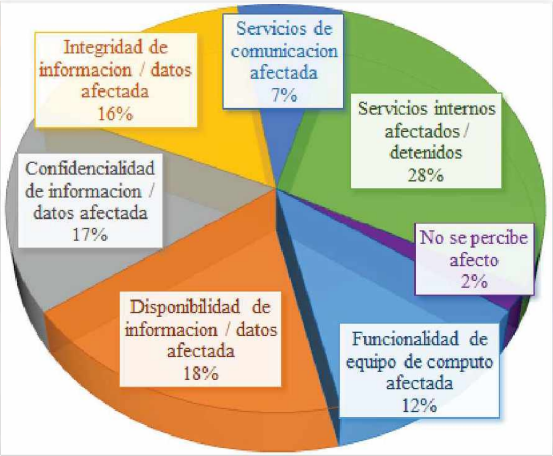

Figura 4. Impacto de ataques a la seguridad de la información del GPD
Fuente: Elaboración propia

MATERIAL Y MÉTODOS

La investigación llevada a cabo fue no experimental transeccional correlacional-causal, puesto que se han recolectado datos en un solo momento, en un tiempo único cuyo propósito fue describir las variables y analizar su incidencia e interrelación en un momento dato (Hernández, 2014) y se determinó la relación entre la variable independiente *gestión de activos de información basada en la ISO/IEC 27002* a fin de estudiar el efecto sobre la variable dependiente *nivel de seguridad de la información*. La tabla 1, resume los indicadores utilizados en la investigación.

Tabla 1. *Indicadores de variables de investigación*

Variable Independiente: Gestión de activos basada en la ISO/IEC 27001	
Indicador	**Unidad de medida**
Nivel de implementación	Escala de Likert – Muy adecuada – Adecuada – Medianamente adecuada – Inadecuada – Inexistente
Nivel de uso de los controles de gestión de activos	Escala de Likert – Siempre – Casi siempre – A veces – Nunca – Casi nunca
Variable dependiente: Nivel de seguridad de la información	
Indicador	**Unidad Medida**
Porcentaje del presupuesto del GPD dedicada a la seguridad de activos de información.	%
Porcentaje de vulnerabilidades mitigadas dentro de periodos de tiempo definidos por el GPD después de su identificación.	%
Porcentaje de puntos de acceso restringidos para evitar el acceso no autorizado.	%
Porcentaje de personal entrenado en sus funciones y responsabilidades relacionadas a la seguridad de la información.	%
Porcentaje de registros revisados bajo actividad inapropiada	%
Porcentaje de nuevos activos de información que han completado la certificación y acreditación previa a su implantación.	%
Porcentaje de activos de información que han llevado a cabo planes de contingencia.	%
Porcentaje de usuarios identificados y autenticados.	%
Porcentaje de incidentes reportados dentro de un plazo establecido y permitido.	%
Porcentaje de activos de información sometidos a planes de mantenimiento formales.	%
Porcentaje de medios de almacenamiento sujetos a pruebas de desinfección	%
Porcentaje de accesos físicos con protección física adecuada.	%
Porcentaje de usuarios autorizados a activos sólo después de firmar reglas de comportamiento para el buen uso de activos de información.	%
Porcentaje de usuarios analizados para concederles acceso a activos de información.	%
Porcentaje de activos de información evaluados periódicamente.	%
Porcentaje de contratos de adquisición de activos de información que contengan requisitos o especificaciones de seguridad.	%

Fuente: Elaboración propia

La población bajo estudio fue establecida en la cantidad de activos de información asignados al área de proyectos digitales. La investigación identificó 6 tipos de activos de información que fueron clasificados bajo las categorías: *Hardware, Software, recursos humanos, lugares*; de ello, se identificaron 61 activos de información en producción. La muestra fue establecida como muestra no probabilística en la que la elección de los elementos depende de la característica de la investigación (Hernández, 2014). La muestra se ha establecido en 40 activos de investigación cuyo nivel de criticidad es mayor a 1.

La gestión de activos basada en la ISO/IEC 27002 establece la identificación precisa sobre los activos dentro de la organización a fin de establecer y reducir los riesgos relacionados a los mismos. Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información (López, 2014). El Departamento de Seguridad Informática (2015) determinó que la gestión de riesgos es una actividad clave para el resguardo de activos de información y proteger la capacidad de la organización de cumplir sus principales objetivos. Se ha utilizado criterios de valorización según las características básicas de seguridad de la información: *Confidencialidad*, *integridad* y *disponibilidad (CIA)* a la que deben ser sometidos los activos de información para generar valor. La tabla 2 presenta los criterios utilizados para establecer el valor de criticidad de los activos de información en el área de proyectos digitales del GPD que se ha establecido en relación al máximo valor de entre los criterios.

Tabla 2. *Criterio de valorización de activos de información*

Confidencialidad	Integridad	Disponibilidad	Valor
Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la Universidad.	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la Universidad.	Información cuya inaccesibilidad no afecta la actividad normal de la Universidad.	0
Información que puede ser conocida y utilizada por todos los agentes de la Universidad.	Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la Universidad o terceros.	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la Universidad.	1
Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la Universidad o terceros.	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la Universidad.	2
Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la Universidad o terceros.	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la Universidad.	3

Fuente: Departamento de Seguridad Informática, (2015)

El análisis del riesgo en la seguridad de la información se basó en la probabilidad en que las amenazas exploten una vulnerabilidad. La valorización del riesgo permite cuantificarlo o describirlo cualitativamente y permite a los directores priorizarlos de acuerdo a su gravedad percibida (NTC-ISO/IEC 27005, 2015). La tabla 3 presenta los criterios de probabilidad de ocurrencia de amenazas y vulnerabilidades, y el criterio de valor del impacto en la organización establecidas para el análisis de riesgos.

Tabla 3. *Criterio de probabilidad de ocurrencia de amenazas, vulnerabilidades e impacto*

Valor		Criterio: Probabilidad Ocurrencia	Criterio: Valor de Impacto
5	Muy alto	Frecuente	Daño muy grave a la organización.
4	Alto	Probable	Daño grave a la organización.
3	Medio	Posible	Daño importante a la organización.
2	Bajo	Improbable	Daño menor a la organización.
1	Muy bajo	Muy improbable	Irrelevante a efectos prácticos

Fuente: Elaboración propia

A fin de determinar el valor del riesgo, se utilizó la matriz presentada en la tabla 4, que se basa en la probabilidad de ocurrencia de una vulnerabilidad detectada y del valor de impacto correspondiente. Los valores de la tabla se establecen en: Riesgo bajo (1-4), medio (6-10) y alto (12-25).

Tabla 4. *Escala para la valoración del riesgo*

		Probabilidad de ocurrencia				
Impacto en el negocio	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Fuente: Elaboración propia

Para recolectar información de las características de los activos de información presentes en el Área de proyectos digitales del GPD, se ha utilizado la tabla 5.

Tabla 5. *Ficha: Activos de información*

Ficha		Activos de información			
Fecha					
Lugar					
ID	Nombre	Función	Área	Cantidad	Tipo

Fuente: Elaboración propia

La tabla 6 ha sido utilizada para recabar información de amenazas y vulnerabilidades de cada activo de información.

Tabla 6. *Ficha: Amenaza y Vulnerabilidad*

Ficha		**Amenaza y Vulnerabilidades**				
Fecha						
Lugar						
ID	**Nombre**	**Obs. Propietario**		**Validación Oficial Seguridad**		
		A	**V**	**A**	**V**	**Obs.**
A: Amenaza V: Vulnerabilidad						

Fuente: Elaboración propia

La tabla 7 fue utilizada para recabar información sobre el estado de implementación de los controles para la gestión de activos según la norma ISO/IEC 27002.

Tabla 7. *Ficha: Implementación de control de gestión de activos*

Ficha	**Implementación de Control de Gestión de Activos**			
Fecha				
Lugar				
Objetivos de Control	**Controles**	**¿Se cumple el objetivo de control?**	**Actividades realizadas**	**Evidencias de implementación**
Responsabilidad sobre los activos.	Inventario de activos			
	Propiedad de los activos			
	Uso aceptable de los activos			
Clasificación de la información	Directrices de clasificación			
	Etiquetado y manipulado de la información			

Fuente: Elaboración propia

La tabla 8 fue utilizada para establecer las acciones ante cada riesgo identificado por activo de información. Para la aplicación de la tabla 8 se ha considerado la política del GPD y el criterio de aceptación del riesgo. Los ejecutores del plan de tratamiento de riesgo fueron el jefe de seguridad de la información y responsables de los activos de información establecidos por el GPD.

La tabla 9 se ha utilizado para realizar el etiquetado y clasificación de la información de acuerdo a la política y directivas aprobadas por el GPD para la clasificación, etiquetado y tratamiento de la información administrada por el área de proyectos digitales.

Tabla 8. *Ficha: Plan de Tratamiento de Riesgo*

Ficha	**Plan de Tratamiento de Riesgo**									
Fecha										
Lugar										
							PTR			
Activo	Valor	Amenaza	Vulnerabilidad	Consecuencias	Nivel de Riesgo		Responsable de activo	Oficial de Seguridad	Aprobación de directiva	Aprobación de Gerencia

Fuente: Elaboración propia

Tabla 9. *Ficha: Etiquetado de información*

Ficha	**Etiquetado de Información**					
Fecha						
Lugar						
			Tipo			
ID	**Nombre Activo**	**Información**	**[P] Publica**	**[I] Uso Interno**	**[C] Confidenci**	**Observación Oficial de Seguridad**

Fuente: Elaboración propia

La tabla 10 fue utilizada para medir el nivel de implementación de los mecanismos de control que fueron propuestos para gestionar los activos de información. Los valores fueron establecidos mediante la escala de Likert, debido a la participación de personal propio del área de proyectos digitales del GPD.

Tabla 10. *Ficha: Implementación del control de gestión de activos de información*

Ficha		**Nivel de Implementación de mecanismos de control gestión de activos**					
Fecha							
Lugar							
Valor Nivel de implementación		[5] Muy Bueno [4] Bueno	[3] Regular [2] Malo [1] Inexistente				
Objetivos de Control	**Controles**	**Ítems a Observar**	**1**	**2**	**3**	**4**	**5**
Responsabilidad sobre los Activos	Inventario de activos	Identificación de activos					
		Elaboración de inventario de activos importantes					
		Identificación de la importancia de cada activo					
		Identificación del tipo de activo,					

		formato, ubicación, información de respaldo, información de licencias y valor comercial.					
	Propiedad de activos	Designación de Propietario y custodio para cada activo.					
	Uso aceptable de activos	Establecimiento de Políticas de uso aceptable de activos.					
		Establecimiento de Requisitos mínimos de uso aceptable de activos					
Clasificación de la información	Directrices de clasificación	Establecimiento de Directrices de clasificación					
		Identificación de Información					
		Valoración de Información					
		Asignación de Nivel de protección adecuado a la información					
	Etiquetado y gestión de la información.	Desarrollo e Implementación de procedimientos de etiquetado y manejo de información					
		Información clasificada y ordenada					

Fuente: Elaboración propia

La tabla 11 fue utilizada para medir el nivel de utilización de los mecanismos de control que fueron implementados para gestionar los activos de información. Los valores fueron establecidos mediante la escala de Likert debido a la participación de personal propio del área de proyectos digitales del GPD.

Tabla 11. *Ficha: Nivel de utilización del control gestión de activos*

Ficha		**Nivel de Uso de mecanismos de control gestión de activos**					
Fecha							
Lugar							
Valor Nivel de uso		[5] Muy Bueno [4] Bueno	[3] Regular [2] Malo [1] Inexistente				
Objetivos de Control	**Controles**	**Ítems a Observar**	**1**	**2**	**3**	**4**	**5**
Responsabilidad sobre los Activos	Inventario de activos	Uso del inventario de activos.					
		Tratamiento de cada activo de acuerdo a su importancia.					
		Uso de cada activo de acuerdo a su tipo y valor comercial.					
	Propiedad de activos	Propietarios aseguran una apropiada clasificación de activos e información.					
	Uso aceptable de activos.	Cumplimiento de Políticas de uso aceptable de activos.					
		Cumplimiento los Requisitos mínimos de Uso aceptable de Activos					
Clasificación de la información	Directrices de clasificación de activos	Cumplimiento de Directrices de clasificación					
		Tratamiento de Información de acuerdo al nivel de protección.					
	Etiquetado y gestión de la información.	Uso de procedimientos de etiquetado y gestión de información.					
		Mantenimiento de Información clasificada y ordenada.					

Fuente: Elaboración propia

RESULTADOS

En la investigación se identificaron los principales activos de información del área de proyectos digitales del GPD. El proceso de recolección de información se ha realizado mediante el método de observación directa con la participación de los propietarios y usuarios de los activos de información, y de un oficial de seguridad designado por el GPD que procedió a validar los resultados obtenidos. La tabla 12 resume los tipos y los activos de información identificados. Los activos de información han sido evaluados en relación a la escalas de valoración de las características de Confidencialidad, Integridad y Disponibilidad definidas en la tabla 2 que ha permitido establecer los valores de la columna *Criticidad (CIA)*. Mientras que los valores de la columna *Impacto* se han obtenido a través de la valoración de impacto definida en la tabla 3. El valor de probabilidad de ocurrencia (*PO*) se estableció haciendo uso de la escala de valoración definida por la tabla 3. El valor de riesgo del activo (*NRA*) se obtuvo al multiplicar el valor de probabilidad de ocurrencia (*PO*) con el valor de nivel de *Impacto* obtenido previamente. Esta información ha sido tratada con la escala de valoración de riesgos definida en la tabla 4, a fin de formular la mejor estrategia para implementar el plan de tratamiento de riesgo (*PTR*). La columna *Etiquetado* presenta el resultado del tratamiento de la información de acuerdo a la clasificación propuesta por la tabla 9 que guarda relación con el esquema de clasificación adoptado por

el GPD. La tabla 12 permite apreciar el cambio del nivel del riesgo del activo antes de la investigación y después de la investigación. El cambio de estos valores indica que existe una íntima relación entre el nivel de riesgo del activo (*NRA*) y la implementación del plan de tratamiento de riesgo (*PTR*). La reducción de los valores en la probabilidad de ocurrencia tiene un efecto directo en los nuevos niveles de riesgo de los activos. Para implementar el plan de tratamiento del riesgo, se necesitó de la participación de cada personal integrante del área de proyectos digitales y del compromiso activo de la gerencia del GPD. La norma ISO/IEC 27002 proporciona diversas estrategias y recomendaciones para mitigar los riesgos identificados en el área de proyectos digitales del GPD. La implementación de los mecanismos de control para la gestión de activos han reducido los riesgos a través de la reducción de amenazas y vulnerabilidades para cada activo analizado.

Tabla 12. *Activos de información del Área de proyectos digitales del Grupo de Periodismo Digital (GPD)*

Activos de información		Criticidad (CIA)	Impacto	Antes del estudio		Etiquetado	PTR	Después del estudio	
				PO	NRA			PO	NRA
Proceso del negocio	1.1. Buenas prácticas de desarrollo de software	2	5	4	20	I/C/P	R	2	10
	1.2. Proceso de análisis e implementación de buenas prácticas de SEO	2	5	4	20	C/P	T	2	10
	1.3. Procesos de soporte de plataformas web	3	5	4	20	C	R	2	10
Información	2.1. Información periodística contenida en las plataformas web.	3	4	3	12	I	R	1	4
	2.2. Bases de datos de la plataforma Web	3	4	3	12	C/I	R	2	8
	2.3. Bases de datos de los clientes	3	3	2	6	C	R	1	3
	2.4. Copias de seguridad	3	4	2	8	C	T	1	4
	2.5. Documentos de claves de acceso a servidores	3	4	4	16	C/I	R	2	8
	2.6. Correos electrónicos del personal de proyectos digitales	3	3	3	9	C	R	1	3
	2.7. Información importante impresa (en papel)	2	3	2	6	C	R	1	3
	2.8. Acuerdos de confidencialidad con los clientes	3	4	2	8	C	R	1	4
	2.9. Repositorio de proyectos	3	5	3	15	C	R	1	5
Hardware	3.1. Equipos de computación portátil	2	2	5	10	C	TRA	4	8
	3.2. Equipos de computación fijos	2	2	5	10	C	TR	4	8
	3.3. Periféricos para procesamiento - impresoras multifuncionales	1	2	5	10	C	TR	4	8
	3.4. Servidores de desarrollo	2	3	4	12	I	TR	2	8
	3.5. Servidores de producción	3	4	3	12	C	TR	2	8
Software	4.1. SO Windows 7	2	2	2	4	I	TR	1	2
	4.2. SO Linux	2	2	2	4	I	TR	1	2
	4.3. Software Git	3	3	2	6	C	R	1	3
	4.4. Plataforma Bitbucket	2	3	3	9	C	AR	1	3
	4.5. Aplicaciones servidor	2	1	4	4	I/C	T	3	3
	4.6. Antivirus	3	4	3	12	I/P	TR	1	4
	4.7. Firewall	3	4	3	12	I/P	TR	1	4
	4.8. Antimalware	3	4	2	8	P	T	1	4
Recursos Humanos	5.1. Jefes de Proyectos Digitales	2	4	3	12	C	R	1	4
	5.2. Coordinador de Desarrollo	2	3	3	9	C	R	1	3
	5.3. Desarrolladores Frontend	2	3	3	9	I	R	1	3
	5.4. Desarrolladores Backend	2	3	3	9	I	R	1	3
	5.5. Coordinador de Plataforma Web.	3	3	4	12	C	R	2	6
	5.6. Analistas de Plataforma Web.	3	3	4	12	C	R	1	3
	5.7. Diseñadores UX.	2	2	2	4	I	R	1	2
Lugares	6.1. Edificación de GPD – Jr. Camaná N°320	3	5	2	10	I	R	2	10
	6.2. Oficina del área de desarrollo y plataforma web	3	4	2	8	I	R	1	4
	6.3. Oficina del área de jefatura de proyectos	3	4	2	8	I	R	1	4
	6.4. Gabinetes de Protección.	3	4	2	8	C	R	1	4
	6.5. Servicio de soporte técnico y mantenimiento de equipos	3	3	3	9	I	T	2	6
	6.6. Sala de internet	3	5	2	10	P	A	2	10
	6.7. Sala de correo electrónico	2	4	2	8	C	A	1	4
	6.8. Área de suministro de energía	3	5	1	5	I	R	1	5

PO: Probabilidad de Ocurrencia. NRA: Nivel de Riesgo del Activo de Información.
PTR – Plan de tratamiento del riesgo: [R] Reducción, [T] Transferencia, [A] Aceptación.
Etiquetado: [P] Publica, [I] Uso Interno, [C] Confidencial.

Fuente: Elaboración propia

La tabla 13 presenta las actividades que se llevaron a cabo para el logro del tratamiento del riesgo. El desarrollo eficiente y eficaz de estas actividades debieron ser respaldadas por documentos de gestión, previamente formulados y aprobados. La implementación del inventario de activos ha afectado positivamente a los procesos del GPD, puesto que permite establecer el estado e importancia de cada activo de información a fin de establecer la mejor estrategia de protección. De la misma manera, la asignación de propietarios de activos ha tenido un efecto favorable debido a su participación activa en el cuidado y salvaguarda de los activos de información. La directiva de uso aceptable de los activos de información ha establecido lineamientos adecuados para que el activo pueda generar el mayor valor posible en los procesos implantados por el GPD. Las directrices para la clasificación de información establecidas han permitido identificar y clasificar y determinar el valor de la información, esto ha permitido elevar los índices de toma de decisiones y formular la mejor estrategia para salvaguardar este activo.

Tabla 13. *Implementación de mecanismos de control en la gestión de activos*

Objetivos de control	Controles	Implementación Inicial		Implementación Final	
		Estado	**NI**	**Estado**	**NI**
Responsabilidad sobre los Activos	Inventario de activos	El inventario de activos de información se basa en un listado de bienes tangibles (hardware y licencias de software). No se cuenta con información detallada de los activos de información o del valor que éste proporciona en los procesos y servicios demandados.	2	Se realizó el inventario de activos considerando Nombre, Propietario, Fecha de clasificación, Tipo de activo, Formato, Ubicación, Información de respaldo, Información de licencias. Se generó documentación sobre el inventario respecto al tipo de activo inventariado a fin de establecer el valor que proporciona dentro y fuera del GPD.	5
	Propiedad de activos	No se cuenta con una designación oficial del propietario de un activo.	1	Se estableció al propietario de cada activo en el área de proyectos digitales. Esta designación se fundamentó en el análisis de servicios resultados del consumo de activos de información.	5
	Uso aceptable de activos	No se cuenta con documentación, reglamentos o directivas que aseguren el uso adecuado de los activos de información.	1	Se formuló, aprobó y ejecutó la directiva: *Uso aceptable de los activos de información en el área de proyectos digitales del GPD* cuya meta está orientada en mejorar la cultura de uso de los activos de información.	5
Clasificación de la información	Directrices de clasificación	La información registrada no se encuentra clasificada de acuerdo su valor, sensibilidad o criticidad dentro de los procesos establecidos.	1	Se formuló, aprobó y ejecutó la directiva: *Clasificación, etiquetado y tratamiento de la información administrada por el área de proyectos digitales del GPD* cuya meta está orientada a organizar la información de manera que proporcione el mayor valor posible dentro de los procesos establecidos. La ejecución de esta directiva reduce el consumo de activos innecesarios para lograr identificar información de acuerdo a su valor dentro y fuera del GPD.	5
	Etiquetado y manejo de la información	No se cuenta con procedimientos adecuados para etiquetar y clasificar la información. Tampoco se cuenta con procedimientos de manipulación segura que incluya almacenaje, transmisión, de-clasificación y destrucción.	1		5
NI : Nivel de implementación					

Fuente: Elaboración propia

En la investigación, se ha examinado el nivel de implementación y uso de los controles formulados. Para analizar el Nivel de implementación de los mecanismos de control de gestión de activos, se utilizó el método de medición basado en la observación directa contando con la participación de los propietarios de los activos de información y un jefe de seguridad designado por el GPD. La primera medición del nivel de implementación se realizó entre los meses de setiembre y noviembre del 2015, mientras que la segunda medición se realizó entre los meses de setiembre y noviembre del 2016. Los valores presentes en las columnas NI (*Nivel de implementación*) indican la variación positiva de los niveles de implementación de los mecanismos para la gestión de activos propuesto por norma ISO/IEC 27002 para lo cual se utilizó los valores establecidos en la tabla 10.

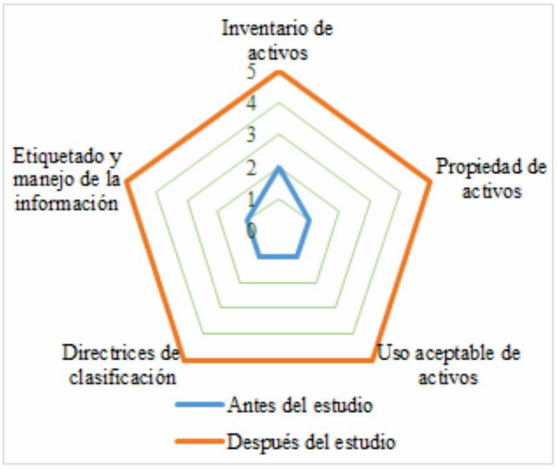

Figura 5. Nivel de implementación de los mecanismos de control
Fuente: Elaboración propia

La figura 5 expone los cambios en los niveles de implementación en su conjunto. Los valores presentados en la tabla 13 y en figura 5 se fijaron mediante el uso de los valores establecido en la tabla 11.

El proceso de implementación de los mecanismos de control fue llevado a cabo en forma continua y puesto en producción en forma oportuna.

El proceso de implementación de mecanismo de control se asoció al nivel de utilización de los mismos en los procesos y servicios establecidos por el GPD. La investigación ha examinado el nivel de utilización de los mecanismos de control implementados a través del método de medición basado en la observación directa contando con la participación de los propietarios de los activos de información y un jefe de seguridad designado por el GPD. La primera medición del nivel de utilización se realizó entre los meses de setiembre y noviembre del 2015 mientras que la segunda medición se realizó entre los meses de setiembre y noviembre del 2016. Los valores presentes en las columnas NU (*Nivel de utilización*) indican la variación positiva de los niveles de utilización de los mecanismos para la gestión de activos propuesto por norma ISO/IEC 27002 para lo cual se utilizó los valores establecidos en la tabla 11. La 14 resume la variación del nivel de utilización de los mecanismos control implementados.

Tabla 14. *Utilización de mecanismos de control en la gestión de activos*

Objetivos de control	Controles	Implementación Inicial		Implementación Final	
		Estado	NU	Estado	NU
Responsabilidad sobre los Activos	Inventario de activos	El inventario de activos de información se orienta al control de bienes tangibles (hardware y licencias de software). El inventario no está orientado a mantener actualizada información detallada de los activos de información o del valor que este proporciona en los procesos y servicios demandados.	1	El inventario forma parte de las herramientas para la adecuada toma de decisiones puesto que está constituido por documentación que abarca el tipo de activo y de su valor dentro y fuera del GPD.	5
	Propiedad de activos	Al no contar con una designación oficial del propietario de un activo no es posible utilizar este mecanismo de control.	1	Al establecer un propietario de cada activo en el área de proyectos digitales, se logró una participación activa y colaborativa en la toma de decisiones basada en la seguridad del activo y el consumo del mismo en los procesos establecidos.	5
	Uso aceptable de activos	Al no contar con documentación reglamentos o reglamentos o directivas no es posible utilizar este mecanismo de control.	1	La ejecución y uso de la directiva: *Uso aceptable de los activos de información en el área de proyectos digitales del GPD* ha logrado mejorar el uso de los activos involucrados en los procesos establecidos en el área de proyectos digitales del GPD.	5
Clasificación de la información	Directrices de clasificación	Al no contar con documentación de activos en forma clasificada no es posible utilizar este mecanismo de control.	1	La ejecución y uso de la directiva: *Clasificación, etiquetado y tratamiento de la información administrada por el área de proyectos digitales del GPD* se logró establecer criterios formales para que han permitido controlar el uso del consumo de activos en el desarrollo de los procesos establecidos en el área de proyectos digitales del GPD.	5
	Etiquetado y manejo de la información	Al no contar con procedimientos adecuados para etiquetar o manejo de información no es posible utilizar este mecanismo de control.	1		5
NU : Nivel de utilización					

Fuente: Elaboración propia

La figura 6 expone los cambios en los niveles de implementación en su conjunto. Los valores presentados en la tabla 14 y en figura 5, se fijaron mediante el uso de los valores establecido en la tabla 11. El monitoreo de uso de los mecanismos de control se llevó a cabo en forma continua, a fin de garantizar estabilidad en los servicios proporcionados en el Área de proyectos digitales del GPD.

El éxito de los cambios en los niveles de implementación y utilización de los mecanismos de control para la gestión de activos de información se debió en mayor parte al compromiso de la gerencia del GPD en fomentar la nueva política de seguridad de la información al llegar de tener pleno conocimiento del valor de criticidad de cada activo de información.

Para determinar el nivel de seguridad en los activos de información, se utilizó las métricas establecidas para la variable dependiente en la tabla 1. Los valores presentados en la tabla 15 evidencian un incremento en los niveles de seguridad de la información, por lo que, la utilización de mecanismos de control para la gestión de seguridad de activos de información propuesta por la norma ISO/IEC 27002 han logrado una mejora significativa en el GPD al mismo tiempo que han colaborado significativamente en el cumplimiento de los objetivos de seguridad establecidas en el área de proyectos digitales. La figura 7 presenta el cambio significativo en diversas dimensiones de estudio que se resaltan en los indicadores 4, 6, 9, 11, 13 y 14 que han evidenciado un incremento significativo durante la investigación.

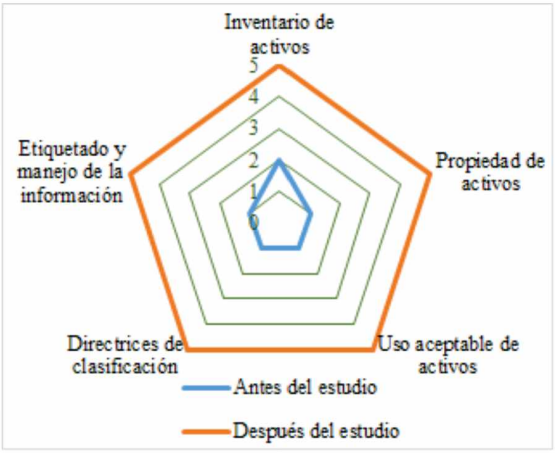

Figura 6. Nivel de utilización de los mecanismos de control
Fuente: Elaboración propia

Tabla 15. *Evaluación de métricas del nivel de seguridad de la información*

	Indicador	Dimensión de estudio	Medida Inicial	Medida Final
1	Porcentaje del presupuesto del GPD dedicada a la seguridad de activos de información.	Presupuesto de seguridad	14%	25%
2	Porcentaje de vulnerabilidades mitigadas dentro de periodos de tiempo definidos por el GPD después de su identificación.	Gestión de vulnerabilidades	18%	32%
3	Porcentaje de puntos de acceso restringidos para evitar el acceso no autorizado.	Control de acceso	80%	80%
4	Porcentaje de personal entrenado en sus funciones y responsabilidades relacionadas a la seguridad de la información.	Sensibilización y capacitación	0%	90%
5	Porcentaje de registros revisados bajo actividad inapropiada	Auditoría	0%	16%
6	Porcentaje de nuevos activos de información que han completado la certificación y acreditación previa a su implantación.	Certificación, acreditación y evaluaciones de seguridad	16%	50%
7	Porcentaje de activos de información que han llevado a cabo planes de contingencia.	Planes de contingencia	14%	25%
8	Porcentaje de usuarios identificados y autenticados.	Identificación y autenticación	90%	90%
9	Porcentaje de incidentes reportados dentro de un plazo establecido y permitido.	Gestión de incidentes	35%	64%
10	Porcentaje de activos de información sometidos a planes de mantenimiento formales.	Mantenimiento	0%	20%
11	Porcentaje de medios de almacenamiento sujetos a pruebas de desinfección	Protección de medios	0%	90%
12	Porcentaje de accesos físicos con protección física adecuada.	Seguridad física	28%	40%
13	Porcentaje de usuarios autorizados a activos sólo después de firmar reglas de comportamiento para el buen uso de activos de información.	Planificación	0%	90%
14	Porcentaje de usuarios analizados para concederles acceso a activos de información.	Seguridad de personal	25%	90%
15	Porcentaje de activos de información evaluados periódicamente.	Evaluación de riesgos	23%	48%
16	Porcentaje de contratos de adquisición de activos de información que contengan requisitos o especificaciones de seguridad.	Adquisición de activos y servicios	16%	25%
	Promedio		**23%**	**55%**

Fuente: Elaboración propia

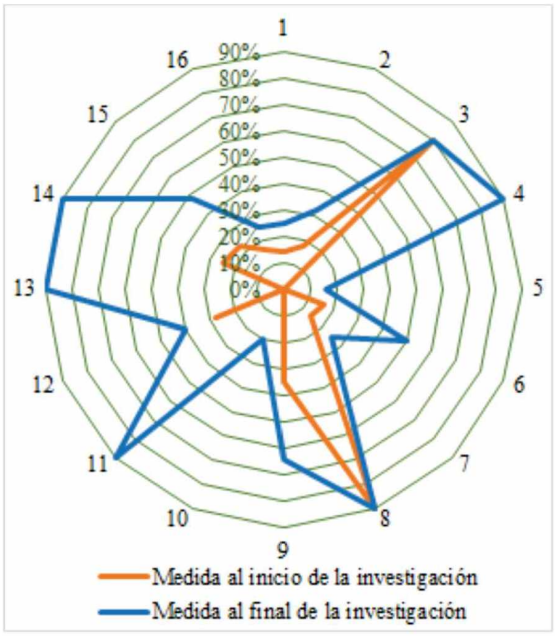

Figura 7. Evaluación de métricas del nivel de seguridad de la información
Fuente: Elaboración propia

DISCUSIÓN

La utilización de mecanismos de control recomendados por la norma ISO/IEC 27002 ha permitido reducir los niveles de riesgo de un activo de información. La tabla 12 indica que se han logrado cambios en los niveles de riesgos del Área de proyectos digitales del GPD. Estos se debieron a la implementación y utilización de los mecanismos de control definidos en las tablas 13 y 14. La figura 8 presenta el porcentaje de reducción de los niveles de riesgos por cantidad de activos. Se estableció que 01 activo ha reducido su nivel de riesgo en un 75%; 18 activos de información han reducido su nivel de riesgo en un 50%;10 en 66,67%; 04 en un 33,33%; 01 en un 25%; 03 en un 20% ; y solo 03 activos de información no han reducido su nivel de riesgo.

Arévalo (2015) indica que la identificación de la actividad de la organización permite establecer las debilidades empresariales, incluyendo las de la información, que una vez identificadas sirven para diseñar espacios de formación, adquisición de habilidades y prácticas gerenciales. La investigación de Arévalo (2015) señala que la implementación de mecanismos de control se relaciona directamente con la asignación presupuestal asignada. En el desarrollo de esta investigación, se experimentó que la implementación de muchos de los mecanismos de control para la gestión de activos propuesto por la norma ISO/IEC 27002 han sido sometidos a una reducción significativa en el presupuesto solicitado, debido a que no se ha tenido establecida la importancia de los activos de información en el área de proyectos digitales del GPD. La tabla 12 resume el análisis de los activos de información y ha servido de punto inicial para el cambio en la cultura organizacional en cada una de las áreas del GPD. Este cambio fue muy importante, debido a que se logró el compromiso de la gerencia a fin de implementar y fomentar la utilización de los mecanismos de control para la gestión de activos de información.

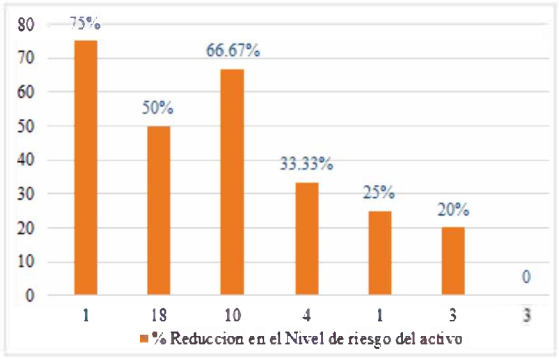

Figura 8. Porcentaje de reducción en los niveles de riesgos por cantidad de activos
Fuente: Elaboración propia

Angarita (2015) manifiesta que la información es el activo más importante en la organización, por lo que es importante implementar técnicas cada vez más sofisticadas para protegerla. Propone aplicar las propiedades de lógica difusa con el fin de realizar el análisis de riesgos de la seguridad de la información a partir de criterios y experiencia de especialistas, ya que ha logrado concluir que se generan y entregan datos más exactos a nivel de riesgo. Esta investigación ha utilizado la técnica de observación directa conjuntamente con la metodología convencional cualitativa, debido a la rápida interpretación del propietario, usuario y jefe de seguridad designado por el GPD. La metodología cualitativa ha permitido fomentar rápido entendimiento de los niveles de criticidad de los activos de información basado en el control de los riesgos que amenazan las vulnerabilidades encontradas en cada activo analizado. Asimismo, esta investigación ofrece adicionalmente estudios comparativos basados en el análisis de riesgos a fin de garantizar controles orientados a la formulación e implementación de estructuras de seguridad que garanticen la salvaguarda de los activos relacionados con los procesos establecidos en el área de proyectos digitales del GPD.

La utilización de mecanismos de control propuestos por el estándar internacional ISO/IEC 27002 para la gestión de activos ha permitido reducir los niveles de riesgo de los activos de información. Para la implementación de los mecanismos de control, ha sido necesario el análisis de riesgos de los activos administrados por el área de proyectos digitales del GPD. Monsalve-Pulido (2014) expone la creación y aplicación de un plan de gestión de vulnerabilidades que se inició con el levantamiento del inventario tecnológico para identificar los problemas que puedan causar alguna vulnerabilidad que afecta la seguridad de la información. Dentro del plan de gestión de

vulnerabilidades, establece un plan de monitoreo, y creación de una base de datos y pruebas que permiten el despliegue adecuado de soluciones a incidentes registrados. Esta investigación comparte la iniciativa de la investigación de Monsalve-Pulido al establecer mecanismos de seguimiento de incidentes a fin de establecer un sistema de gestión de conocimiento para garantizar la seguridad de los activos de información bajo un enfoque de continuidad de servicios.

CONCLUSIONES

La tabla 15 evidencia que la implementación y utilización de mecanismos de control para la gestión de activos basada en el estándar internacional ISO/IEC 27002 permite elevar los niveles de las métricas del Nivel de seguridad de la información. Este incremento ha garantizado que se logren los objetivos de seguridad de información y los objetivos de la organización, además de garantizar la seguridad de los activos de información para elevar los niveles de valor generados en el Área de proyectos digitales del GPD.

La gestión de inventarios, propiedad de activos, uso aceptable de activos, directrices de clasificación, etiquetado y manejo de la información basado en la norma ISO/IEC 27002 han permitido elevar los niveles de implementación y utilización de los mecanismos de control para la gestión de activos que han posibilitado el cambio en los estado de los controles de seguridad. Este cambio, en los controles de seguridad, ha servido de catalizador para la adecuada toma de decisiones e identificar los factores que causan bajo rendimiento y establecer acciones correctivas apropiadas.

La norma ISO/IEC 27002 ha suministrado el modelo y conjunto de mejores prácticas que permiten establecer roles, responsabilidades y mecanismos para proteger activos de información (tablas 13 y 14) con el fin de lograr un adecuado conjunto de controles administrativos, técnicos y físicos de acuerdo a las necesidades del área de proyectos digitales del GPD.

REFERENCIAS BIBLIOGRÁFICAS

Angarita, A., Tabares, C., y Rios, J. (2015). 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, 9*(17), 71-80. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672015000100010&lng=es&tlng=es.

Arévalo, J., Bayona, R. y Rico, D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. *Revista Tecnura, 19*(46), 123-134. Recuperado de: http://dx.doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10.

ESET – Enjoy Safer Technology. (2015). *ESET Security Report - Latinoamérica 2015*. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf.

Hernández, R., Fernández, C., y Baptista, M. (2014). *Metodología de la Investigación*. México D.F., México: McGraw-Hill/Interamericana Editores, S.A. de C.V.

Departamento de Seguridad Informática. (2015). *Seminario Taller Riesgo vs. Seguridad de la Información*. Recuperado de: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf.

DRI Internacional. (2016). *ISO 27002.es*. España: DRI Internacional. Recuperado de: http://iso27000.es/iso27002.html#home.

Indecopi. (2014). *Norma Técnica Peruana NTP ISO/IEC 27005*. Lima, Perú: Indecopi.

Indecopi. (2014). *Norma Técnica Peruana NTP ISO/IEC 27001* (2da. Edición). Lima, Perú: Indecopi.

López, A. y Ruiz, J. (2014). *El portal de ISO 27001 en Español*. España. GES Consultor. Recuperado de: http://www.iso27000.es/iso27002_8.html.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2015). *Guía para la Gestión y Clasificación de Activos de Información*. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf.

Ministerio de Hacienda y función pública. (2017). *Guía de seguridad de las TIC CCN-STIC 804*. Recuperado de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html.

Monsalve, J., Aponte, F. y Chaves, D. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Revista Facultad de Ingeniería, 23*(37), 65-72. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lng=es&tlng=es.

National Institute of Standards and Technology. (2006). *Guide for Developing Performance Metrics for Information Security*. Recuperado de: http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/sp80080GuideForDevelopingPerformanceMetricsForInformationSecurity-Draft-NIST.pdf.

National Institute of Standards and Tecnology. (2008). *Performance Measurement Guide for Information Security*. Recuperado de: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

ONGEI - Oficina Nacional del Gobierno Electrónico e Informática. (2015). *NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición.* Recuperado de: http://www.ongei.gob.pe/docs/Aprobacion%20NTP%20ISO%20IEC%2027001%202014.pdf.

NTC-ISO/IEC 27005 (2015). *Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.* Recuperado de: https://tienda.icontec.org/wpcontent/uploads/pdfs/NTC-ISO-IEC27005.pdf.