Análisis de Riesgos tecnológicos en la cooperativa de ahorro y crédito Calceta Limitada

Luis Cristóbal Cedeño Valarezo, Jessica Johanna Morales Carrillo, Mayra Alexandra Dávila Muñoz, Gema Vanessa Párraga Andrade

Carrera de Informática, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Campus Politécnico El Limón, Calceta – Manabí – Ecuador.
lcedeno@espam.edu.ec, jmorales@espam.edu.ec, mayradavila22@outlook.com, gemivane_201712@hotmail.com

Resumen. La investigación tuvo como objetivo desarrollar un análisis de riesgos para determinar el grado de exposición de eventos no deseados en la infraestructura de Tecnologías de Información (TI) en la Cooperativa de Ahorro y Crédito Calceta Limitada del Cantón Bolívar. Para el desarrollo del mismo se utilizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, que permite indagar los riesgos que tienen los sistemas de información de las organizaciones y la búsqueda de medidas apropiadas para controlarlos. El proceso fue el siguiente: se determinaron los activos de la institución susceptibles a riesgo, luego se identificaron las potenciales amenazas, se establecieron pasos a ejecutar para prevenir riesgos y daños y por último se realizó una propuesta de salvaguardas de la infraestructura de TI de la institución. Luego de realizado el procedimiento se determinó que los riesgos tecnológicos de la institución tienen alto impacto en el desarrollo social, económico y productivo de la zona. Por lo tanto el análisis de riesgo realizado, estableció el peso medio del riesgo en la institución, el cual está distribuido de la siguiente manera: para daños de tipo natural de 3/5, de origen industrial de 2.91/5, para errores y fallos no intencionados 2.56/5 y para daños intencionados 2.58/5, lo cual reflejó un riesgo medio, por lo que se realizó una propuesta de salvaguardas a la institución, para así mantener la integridad, confidencialidad y disponibilidad de los servicios y datos.

Palabras clave. Magerit, infraestructura tecnológica, amenaza.

1. Introducción

Monsalve *et al.* (2014) Señalan que las empresas tanto del sector público como del privado priorizan la seguridad de la información, que es catalogada como uno de los bienes más preciados para la continuidad del negocio y el punto de diferencia con la competencia. Sin embargo, estos requieren un estudio, un presupuesto y una aplicación, ya sea preventiva o correctiva, sobre los temas de seguridad que se puedan encontrar, ya que cada día se descubren nuevos riesgos en distintos niveles.

El riesgo ha existido inherente a cada acción que realiza el ser humano; sin embargo, en la sociedad actual, inmersa en un ambiente altamente tecnológico y donde la información es el centro de las actividades, se ha desarrollado una creciente dependencia de las Tecnología de la Información lo que las ha convertido en un gran factor de riesgo y quizás, uno de los más importantes de este siglo (Gómez *et a.,* 2010). Puesto que la dimensión que ha adquirido el riesgo y su cuantificación en las organizaciones, ha hecho que más autores dediquen tiempo a proponer modelos que contribuyan con aproximar la exposición asumida del daño medido en valor monetario (Bracho *et al.,* 2010).

Como es bien sabido, no existe tecnología perfecta; todas presentan deficiencias, vulnerabilidades, errores, entre otros. Si los procesos de negocio dependen de tecnologías de información, el riesgo incrementa y más aún si esta tecnología es utilizada por personas en el desarrollo de dichos procesos, lo que genera, se conoce como riesgo de TI. Lo que provoca pérdida de la disponibilidad, confidencialidad o integridad de la información (Montesino *et al*., 2013). De allí que sea necesario que los responsables de la seguridad de la información en las organizaciones, tomen conciencia de su papel y deban contrastar los riesgos a los que están sometidos sus activos (Freitas, 2010).

Eterovic y Pagliari (2011) consideran que el análisis de riesgos es el primer punto de la gestión de la seguridad de la información de una organización, y es necesario para realizar la gestión de los riesgos, es decir, tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos. Arias *et al.* (2010) menciona que el riesgo está presente en la totalidad de las actividades que realiza el ser humano, por lo que antes de implementar cualquier mecanismo de seguridad en TI, es necesario conocer la prioridad de aplicación y qué tipo de medidas se pueden aplicar.

Muñoz (2012) indica, que la ocurrencia de eventos accidentales modifica dramáticamente la percepción del público en general, ya que la misma puede poner en riesgo el papel que desempeña la institución dentro de la sociedad, perdiendo el prestigio que han ganado a lo largo de los años, por lo que es necesario conocer a tiempo que tan vulnerables están de que una amenaza se materialice y cómo actuar frente a ello.

Considerando lo señalado, realizar un análisis de riesgos tecnológicos es preciso, ya que permite identificar, analizar y observar los riegos de TI, que sin lugar a duda pondrían en peligro la continuidad del negocio. Más aún, en instituciones financieras, que aportan al desarrollo socioeconómico de la población (Vanegas y Pardo, 2014). Por lo tanto, el análisis de riesgos realizado en la Cooperativa Calceta sirvió de apoyo para determinar el grado exposición ante eventos no deseados en la infraestructura de TI y por ende orientar a los directivos de la misma en la toma de decisiones.

2. Materiales y métodos

El desarrollo del análisis de riesgos tecnológicos se llevó a cabo en la Cooperativa de Ahorro y Crédito Calceta Limitada, entre marzo y julio de 2015, para esto se utilizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) en su versión 3.0, que dispone de cinco fases y de la cual se creyó oportuno el uso de cuatro de ellas, las cuales son: determinar los activos relevantes para la organización, determinar a qué amenazas están expuestos los activos, estimar el impacto y estimar el riesgo (Dirección General de Modernización Administrativa, 2012).

En la primera fase se determinaron los activos relevantes de la institución, obteniendo un inventario actualizado del hardware y el software, la nómina de talento humano, los procesos de la institución por departamentos, la dependencia que tienen los activos y el análisis FODA del área de tecnología, el levantamiento de información se llevó a cabo en matrices.

En la segunda fase se identificaron las posibles amenazas que se pueden materializar en los activos, que son eventos que pueden ocurrir causando daños en los activos y perjuicios para la institución, motivo por el cual es necesario que se identifiquen a tiempo para mitigar eventos no deseados. Para la identificación de las amenazas se tomó en cuenta cuatro clasificaciones importantes que establece la metodología, tales como: desastres de origen natural, desastres de origen industrial, desastres de manera no intencionada y desastres de manera intencionada, como se muestra en la tabla 1.

Tabla 1. Matriz para identificar las amenaza por tipos (naturales, industriales, no intencionadas e intencionadas).

Origen	Amenazas	Tipos de activos
Desastres naturales	[N.1] Fuego	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[N.2] Daños por agua	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[N.*] Desastres naturales	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar

Luego se procedió a la estimación del impacto y la estimación del riesgo tomando en cuenta: la perdida de la dimensión de seguridad en caso que se materialice la amenaza, la degradación que sufre los activos y la frecuencia de que ocurra dicho evento, para cada amenaza existe una matriz donde se detalla los tipos de activos, las dimensiones, la descripción de la amenaza, el valor del impacto y del riesgo y la causa, como se muestra en la tabla 2. Las siglas significan lo siguiente: MA (Muy alta), A (Alta), M (Media), B (Baja), MB (Muy baja), MF (Muy frecuente, a diario), F (Frecuente, mensual), FN (Frecuencia normal, anual), PF (Poco frecuente, cada varios años)

Tabla 2. Matriz para estimar la valoración del impacto y el riesgo

<table>
<tr><td colspan="11">[CÓDIGO] Descripción sucinta de lo que puede pasar</td></tr>
<tr><td colspan="5">Tipos de activos:
Que se puede ver afectado por este tipo de amenazas.</td><td colspan="6">Dimensiones:
De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante.</td></tr>
<tr><td colspan="11">Descripción:
Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.</td></tr>
<tr><td colspan="5">Estimación del impacto</td><td colspan="6">Estimación del frecuencia</td></tr>
<tr><td colspan="2" rowspan="2">Impacto</td><td colspan="3">Degradación</td><td colspan="2" rowspan="2">Riesgo</td><td colspan="4">Frecuencia</td></tr>
<tr><td>1%</td><td>10%</td><td>100%</td><td>PF</td><td>FN</td><td>F</td><td>MF</td></tr>
<tr><td rowspan="5">Valor</td><td>MA</td><td>M</td><td>A</td><td>MA</td><td rowspan="5">Impacto</td><td>MA</td><td>A</td><td>MA</td><td>MA</td><td>MA</td></tr>
<tr><td>A</td><td>B</td><td>M</td><td>A</td><td>A</td><td>M</td><td>A</td><td>MA</td><td>MA</td></tr>
<tr><td>M</td><td>MB</td><td>B</td><td>M</td><td>M</td><td>B</td><td>M</td><td>A</td><td>MA</td></tr>
<tr><td>B</td><td>MB</td><td>MB</td><td>B</td><td>B</td><td>MB</td><td>B</td><td>M</td><td>A</td></tr>
<tr><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>B</td><td>M</td></tr>
<tr><td colspan="11">MOTIVO:
Razón detallada por la cual se considera el impacto y el riesgo de la amenaza.</td></tr>
</table>

Con la identificación de las posibles amenazas y los activos que se verían afectados por la misma, se pudo estimar de forma cualitativa el valor del impacto, el mismo que fue de complemento para obtener el valor del riesgo en una matriz, tal como se ilustra en la tabla 3.

Estos valores fueron cuantificados de acuerdo a las siguientes magnitudes: muy alto=5, alto=4, medio=3, bajo=2 y muy bajo=1. Posteriormente, se calculó el peso medio de riesgo que tiene cada tipo de amenaza en la institución.

Tabla 3. Valoración cuantitativa de amenazas

Tipo de amenaza		
Código	**Amenaza**	**Valor Cuantitativo**
[N.1]	Amenaza 1	Valoración
[N.2]	Amenaza 2	Valoración
[N.*]	Amenaza n	Valoración
	Total	Sumatoria
	Media	Promedio

Después se hizo una lista de actividades para mitigar, eliminar o reducir los riesgos que necesitan de intervención inmediata por cada tipo de amenaza, considerando que esto es sólo una propuesta, quedando en manos de la institución su aplicación.

Posteriormente se realizó una propuesta de salvaguarda para ayudar a mitigar los riesgos, con el fin de proteger los activos de hardware y software de la institución, ya que para selección de salvaguardas se consideró el tipo de amenaza, los activo a proteger, las dimensiones de seguridad, y la valoración cuantitativa del riesgo por cada amenaza según el impacto y la frecuencia, realizando también el cálculo del valor que tiene cada salvaguarda a ser implementada.

3. Resultados y discusión

El inventario del hardware de la Cooperativa de Ahorro y Crédito Calceta Limitada dio como primer resultado el valor de adquisición de los equipos de hardware y software con un valor de $188.842,59.

De acuerdo con la tabla 2, se estimó la valoración de impacto y riesgo. En la tabla 4 y tabla 5, se muestran dos de los 48 análisis de amenazas realizados.

Tabla 4. Origen industrial – Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [MEDIA] soporte de información • [COM] redes de comunicaciones • [AUX] equipamiento auxiliar	**Dimensiones:** **1.** [D] Disponibilidad
Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta,... **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Estimación del impacto						Estimación del riesgo					
Impacto		Degradación				Riesgo		Frecuencia			
		1%	10%	100%				PF	FN	F	MF
Valor	MA	M	A	MA		Impacto	MA	A	MA	MA	MA
	A	B	M	A			A	M	A	MA	MA
	M	MB	B	M			M	B	M	A	MA
	B	**MB**	MB	B			B	MB	B	M	A
	MB	MB	MB	MB			MB	**MB**	MB	B	M

Causa: En la institución se presentó una vez este tipo de sucesos, debido a la interferencia que presentaban los transformadores cercanos aun así no se presentaron daños por lo cual el impacto y el riesgo es muy bajo.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Tabla 5. Ataques intencionados – Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad 4. [A_S] Autenticidad del servicio 5. [A_D] Autenticidad de los datos
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

Estimación del impacto				
Impacto		Degradación		
		1%	10%	100%
Valor	**MA**	M	**A**	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Estimación del riesgo					
Riesgo		Frecuencia			
		PF	FN	F	MF
Impacto	MA	A	MA	MA	MA
	A	M	**A**	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Causa: En la cooperativa Calceta no se han registrado este tipo de incidentes, pero en caso de darse podría afectar en el buen funcionamiento tanto del hardware como del software por lo que se considera que tanto el riesgo como el impacto son altos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo

PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente

Con la identificación de las posibles amenazas y los activos que se verían afectados por la misma, se pudo estimar de forma cualitativa el valor del impacto, obteniendo como resultado la media de cada tipo de amenaza. Lo que indicó el riesgo medio que tiene la organización a que una amenaza se materialice en un activo tecnológico, como se detallan en las tablas: 6,7, 8 y 9.

Tabla 6. Valoración cuantitativa amenazas naturales

Desastres Naturales		
Código	**Amenaza**	**Valor Cuantitativo**
[N.1]	Fuego	4
[N.2]	Daños por agua	2
[N.*]	Desastres naturales	3
	Total	**9**
	Media	**3**

Tabla 7. Valoración cuantitativa amenazas por errores y fallos no intencionados

De origen industrial		
Código	**Amenaza**	**Valor Cuantitativo**
[I.1]	Fuego	4
[I.2]	Daños por agua	2
[I.*]	Desastres industriales	1
[I.3]	Contaminación mecánica	4
[I.4]	Contaminación electromagnética	1
[I.5]	Avería de origen físico o lógico	4
[I.6]	Corte del suministro eléctrico	4
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	1
[I.8]	Fallo de servicios de comunicaciones	4
[I.9]	Interrupción de otros servicios y suministros esenciales	3
[I.10]	Degradación de los soportes de almacenamiento de la información	4
	Total	**32**
	Media	**2,91**

Tabla 8. Valoración cuantitativa amenazas de origen industrial

Errores y fallos no intencionados		
Código	**Amenaza**	**Valor Cuantitativo**
[E.1]	Errores de los usuarios	2
[E.2]	Errores del administrador	3
[E.4]	Errores de configuración	3
[E.7]	Deficiencias en la organización	1
[E.8]	Difusión de software dañino	4
[E.9]	Errores de [re-]encaminamiento	2
[E.10]	Errores de secuencia	1
[E.14]	Escapes de información	3
[E.15]	Alteración accidental de la información	2
[E.18]	Destrucción de información	3
[E.19]	Fugas de información	3
[E.20]	Vulnerabilidades de los programas (software)	4
[E.21]	Errores de mantenimiento / actualización de programas (software)	3
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3
[E.24]	Caída del sistema por agotamiento de recursos	2
[E.28]	Indisponibilidad del personal	2
	Total	**41**
	Media	**2,56**

Tabla 9. Valoración cuantitativa amenazas por ataques

Ataques intencionados		
Código	**Amenaza**	**Valor Cuantitativo**
[A.4]	Manipulación de la configuración	3
[A.5]	Suplantación de la identidad del usuario	4
[A.6]	Abuso de privilegios de acceso	3
[A.7]	Uso no previsto	2
[A.8]	Difusión de software dañino	4
[A.11]	Acceso no autorizado	3
[A.12]	Análisis de tráfico	1
[A.13]	Repudio	2
[A.14]	Interceptación de información	2
[A.15]	Modificación deliberada de la información	2
[A.18]	Destrucción de información	4
[A.19]	Revelación de información	3
[A.22]	Manipulación de programas	3
[A.25]	Robo	4
[A.26]	Ataque destructivo	2
[E.28]	Indisponibilidad del personal	2
[A.29]	Extorsión	3
[A.30]	Ingeniería social	3
	Total	**50**
	Media	**2,78**

Finalmente se tomó en cuenta la valoración cualitativa, se desarrolló una propuesta de salvaguardas por cada tipo de amenaza, la misma que ayudará a reducir el riesgo asegurando la continuidad de las funciones que realiza la organización, como se aprecia en la tabla 10.

Tabla 10. Valoración económica de las salvaguardas

Código	Amenaza	Valor salvaguarda	Detalle
[I.2]	Daños por agua	$ 300	Por mantenimiento a las instalaciones de agua se estima un pago por hora de $15, trabajando 4 horas diaria por cinco días, esta salvaguarda se hace una vez al año
[I.3]	Contaminación mecánica	$1920	El mantenimiento de equipos se lo realiza 2 veces al año, teniendo la institución un total de 80 equipos pagando $12,00 por cada uno.
[I.5]	Avería de origen físico o lógico	$1920	El mantenimiento preventivo de equipos se lo realiza 2 veces al año, teniendo la institución un total de 80 equipos pagando $12,00 por cada uno.
[I.6]	Corte del suministro eléctrico	$ 750	El mantenimiento a la planta generadora se realizara tres veces al año, pagando por cada mantenimiento $250.
[I.6]	Corte del suministro eléctrico	$ 1500	La adquisición del sistema de UPS tiene un valor total de $ 1500
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	$ 4800	El mantenimiento de los equipos de climatización se realizara una vez al año, trabajando 4 horas diarias por tres días, pagando la institución por hora de trabajo $150
[I.8]	Fallo de servicios de comunicaciones	$ 3000	La implementación de enlace redundante se la realiza por un monto en total de $ 3000
[I.8]	Fallo de servicios de comunicaciones	$ 400	El mantenimiento a las redes de comunicación se las realiza una vez al año, trabajando 2 horas por 8 días, cancelando $50 la hora
[I.10]	Degradación de los soportes de almacenamiento de la información	$ 500	El respaldo se la puede realizar en discos duros extraíbles, cd y flash memory, estimando un costo de adquisición de los mismos de $500.
[E.1]	Errores de los usuarios	$ 500	Se capacitara a los usuarios 2 veces al año, el cual se cancelara a la persona un valor de $250 por capacitación.
[E.2]	Errores del administrador	$ 800	Se capacitara a los administradores de la institución dos veces al año, el cual se cancelara a la persona un valor de $400 por capacitación.
[E.8]	Difusión de software dañino	$2300	La adquisición del antivirus para implementar a los computadores de la institución tuvo un costo de $ 2300
[E.9]	Errores de [re-]encaminamiento	$ 200	La capacitación a los usuarios se realizara una vez al año, el cual se cancelara a la persona un valor de $200.

[E.15]	Alteración accidental de la información	$ 300	La capacitación al personal se la realizara dos veces al año, el cual se cancelara a la persona un valor de $150 por capacitación.
[E.18]	Destrucción de información	$ 400	Se estima que el costo por adquisición de soportes de información es de $ 400
[E.19]	Fugas de información	$ 100	La capacitación al personal se la realizara una vez al año, el cual se cancelara a la persona un valor de $100.
[E.19]	Fugas de información	$ 600	Se estima que la adquisición de un sistema de perdida de información es de $ 600
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	$ 400	Para evitar la pérdida de datos, se debe realizar mantenimiento preventivo a los equipos por un costo de $ 400
[A.5]	Suplantación de la identidad del usuario	$ 50	La capacitación del personal antes de ser contratado se la realiza una hora por un valor de $ 50
[A.8]	Difusión de software dañino	$ 700	Se estima que el costo de actualización del software de la institución es de $700
[A.18]	Destrucción de información	$ 150	Se capacitara al 2 veces al año, pagando a la persona un valor de $150 por capacitación.
[A.22]	Manipulación de programas	$ 500	La auditoría a las aplicaciones la realiza la misma institución pero esta puede generar un cargo de $ 500 por el trabajo.
[A.25]	Robo	$ 100	Las capacitaciones al personal para que no libere información confidencial de la institución tiene un costo de $ 100
[A.25]	Robo	$ 5000	Se estima que la institución debe pagar por un seguro que ampare sus activos un valor de $5000 por año.
[A.25]	Robo	$ 2500	La implementación de cámaras en las instalaciones de la institución tienen un costo de $2500

El análisis de riesgos realizado, permitió inventariar los activos, determinar las amenazas a que están expuestos, valorar los riesgos, valorar el impacto y plantear la propuesta de salvaguardas sobre los activos con amenazas más altas, según las tablas: tabla 6, 7, 8 y 9. La propuesta de salvaguardas planteada, contiene medidas preventivas y servirá de apoyo a la institución ante cualquier evento que se produzca.

Ante lo mencionado se evidencia el trabajo realizado en la Universidad Tecnológica de Pereira, con el fin de identificar las amenazas y los riesgos, permitiendo a la empresa entender la situación actual en niveles de seguridad y así tomar decisiones para mitigar los riesgos (Angarita y Tabares, 2012). Otros de los temas que sirvió de referencia fue el trabajo realizados por los estudiantes de la ESPAM MFL (Palacios *et al*., 2013); ambas

investigaciones implican el estudio de los activos de hardware y software, la importancia de la información, la estimación del impacto, el nivel de riesgo y la propuesta de salvaguardas, pero no aporta con el cálculo del peso medio que tiene cada amenaza, este proceso fue establecido por las autoras del presente trabajo permitiendo de manera relevante, identificar el nivel de riesgos que puede tener la institución ante cualquier amenaza a los activos.

4. Conclusiones

Al realizar una identificación de las amenazas potenciales a las que están expuestos los activos, se pudo determinar la vulnerabilidad al riesgo de la institución y se tuvo una idea aproximada del impacto que tendría en ella al materializarse.

Las salvaguardas que se plantearon, son una herramienta que permitirá mitigar los riesgos y servirá de apoyo a los directivos de la institución en la toma de decisiones en caso de ocurrencia de las amenazas.

Referencias

1. Angarita, A y Tabares, C. 2012. Análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de Pereira s.a e.s.p. Colombia. Formato PDF. Disponible en http://repositorio.utp.edu.co
2. Arias, A; Bolaños, B; Esparza, A. 2010. Unidades Tecnológicas de Santander: seguridad Informática. (En Línea). Colombia. Formato SWF. Disponible en http://es.calameo.com
3. Bracho, D; Rincón, C; Acurero, A. 2010. Modelo para la cuantificación del riesgo telemático en una organización. Revista Venezolana de Información, Tecnología y Conocimiento. 7(2): 65
4. Dirección General de Modernización Administrativa. 2012. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: libro I - Método. 3ed. España. NIPO. p 22-35
5. Eterovic, J y Pagliari G. 2011. Metodología de Análisis de Riesgos Informáticos. Revista Técnica Administrativa. 10(1): 1
6. Freitas, V. 2010. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Revista Venezolana de Información, Tecnología y Conocimiento. 6(1): 45
7. Gómez, R; Hernán, D; Donoso, Y; Herrera, A. 2010. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería. 1(31):110
8. Monsalve, J; Aponte, F; Chaves, D. 2014. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá. Revista facultad de Ingeniería. 23(37): 67

9. Montesino, R; Baluja, W; Porvén, R. 2013. Gestión automatizada e integrada de controles de seguridad informática. Revista de Ingeniería Electrónica Automática y Comunicaciones. 34: 1
10. Muñoz, F. 2012. Retos para el siglo XXI en la seguridad de procesos y análisis de riesgos. Revista de Ingeniería. 1(31): 48
11. Palacios, R; Quiroz, J; Buenaventura, J; Morales, J. 2013. Plan de contingencia de equipos y sistemas informático en el municipio de Junín. Tesis. Ing. Informática. ESPAM MFL. Calceta – Manabí, Ec. Pág. 8.
12. Vanegas, G y Pardo, C. 2014 Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Revista Sistemas & Telemática. 12(30): 44