AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN DE LA CARRERA INFORMÁTICA DE LA ESPAM MFL

Autora: Ing. Loor Párraga Amarilis Carolina, Ing. Espinoza Castillo Verónica Alexandra

RESUMEN

La presente investigación tiene la finalidad de evaluar la seguridad de los recursos de tecnología de información existentes en la carrera Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, con este fin, se realizó una auditoría de seguridad física y lógica, entre octubre de 2013 y febrero de 2014, para el efecto, se empleó la metodología establecida en las Normas Internacionales de Auditoría que se divide en tres fases, la primera corresponde a la planificación e incluye un análisis integral de todos los elementos involucrados en la entidad que se complementa con la evaluación de control interno, cuya normativa es emitida por la Contraloría General del Estado; la segunda es la ejecución donde se aplican los programas de auditoría por componentes como la protección de los activos tangibles entre otros, en esta sección, adicionalmente se evidencian los principales hallazgos suscitados en la entidad. Finalmente, la fase de comunicación de resultados, en la que se describen las conclusiones y recomendaciones mediante la presentación del informe final de auditoría. Con los resultados obtenidos de la evaluación de control interno, se determina que la entidad auditada aplica lineamientos generales de seguridad, situación que se comprueba al obtener el coeficiente de concordancia de Kendall de 0.85; por lo que se concluye que la entidad evaluada cuenta con un bajo control documentado de procedimientos aprobados, por tal motivo, deberían elaborar normativas de control tal como política de seguridad, entre otras.

Palabras clave: Seguridad, Control, Información, Procedimientos, Recursos.

INTRODUCCIÓN

Las entidades, actualmente, dan relevancia al mantenimiento y establecimiento de la seguridad de sus equipos de tecnologías de información por el activo que representan, es así, que la realización de auditorías, se ha vuelto una necesidad imperiosa, como lo declaran (Piattini *et al*., 2008), al indicar que es una herramienta que sirve para la gestión de la tecnología de información de las entidades, que minimizan los posibles riesgos a los que están expuestos. Sin embargo, (Martínez, 2012), amplia este

concepto al señalar que la auditoría va más allá de la detección de errores, sino que es un examen crítico donde el objetivo es evaluar la eficiencia y la eficacia de un área u organismo a través de métodos para emitir un criterio basado en la evidencia. Es así, que (Ramírez y Álvarez, 2008) definen que la auditoría de seguridad física y lógica es una serie de procedimientos para salvaguardar el hardware, software de las entidades. La auditoría se complementa con el análisis de control interno que (Delgado, 2009) define como cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos y (Pinket, 2006) manifiesta dos tipos de controles: el control general y el control detallado de los sistemas de información. El control general involucra a todos los sistemas de información y el control detallado está diseñado para controlar el procesamiento de la información, que (Lara y Párraga, 2010) añaden que se lo realiza mediante técnicas que permiten al auditor/a evidenciar y fundamentar sus opiniones y conclusiones.

Considerando entonces, que la carrera Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, cuenta con importantes recursos tecnológicos que podrían ser víctimas potenciales de daños producidos por los usuarios o por desastres naturales, lo que le ocasionaría graves pérdidas de información y económicas, por ello, es necesario evaluar y cuantificar los bienes a proteger y en función de ese análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables (Franco *et al.,* 2013). Considerando también, implantar medidas efectivas a medio y largo plazo desde un punto de vista estratégico y táctico (James, 2009), para la mitigación de vulnerabilidades de seguridad tal como lo plantea (Morlanes, 2012), en su artículo sobre seguridad informática, y (Castro, 2009) establece que todos los métodos de seguridad adoptados variarán dependiendo de cada organización.

En este artículo, se presenta por tanto el empleo de la metodología basadas en las Normas Internacionales de Auditoría, para la realización de evaluaciones de seguridad física y lógica de los recursos de tecnología, que es el principal objetivo planteado en esta investigación, se expone su desarrollo y proceso metodológico, hasta llegar a las conclusiones adecuadas, entre las cuales se presenta la necesidad de políticas de seguridad en la entidad para la salvaguarda de dichos recursos.

MATERIALES Y MÉTODOS

El método de auditoría utilizado está basado en las Normas Internacionales de Auditoría aceptadas en el Ecuador desde 2009 y emitidas por el Consejo de Normas Internacionales de Auditoría y Aseguramiento, con sede en Nueva York, el cual nos permite determinar la seguridad de los recursos tecnológicos; la primera fase fue la planificación, donde se definen los procedimientos de trabajo, objetivos, recursos, talento humano y el tiempo estimado para efectuar la revisión; complementariamente, se diseñó el programa general de auditoría que registró los procedimientos permanentes, instrumento que facilitó la ejecución del plan de auditoría esperado; este proceso se documenta mediante el memorando de planificación preliminar, adicionalmente se establecieron las técnicas de trabajo como entrevistas y aplicación de cuestionarios a los responsables de las áreas de recursos tecnológicos.

La planificación se divide en dos tiempos diferentes entre sí, como lo es la planificación preliminar y la planificación específica. La primera subfase permite recopilar información general sobre la entidad auditada, mediante la aplicación de cuestionarios de control interno para determinar los componentes que permitirán seguir con el estudio. Estos fueron: a) Seguridad del data center, b) Protección de activos tangibles, c) Protección de activos intangibles, d) gestión de mantenimiento de hardware y software y e) Gestión de software. La segunda subfase, recopila información detallada de los controles internos, para lo cual se empleó una evaluación de control interno basada en las Normas de Control Interno (CGE, 2009), mediante la aplicación de cuestionarios cerrados o dicotómicos con preguntas de sí o no (Chávez y Rodríguez, 2012).

La composición de cada cuestionario consistió en una serie de preguntas dicotómicas, estructuradas mediante una ponderación de diez puntos para cada pregunta, cuya calificación es asignada según el rango de puntuación (0-10) donde, cero indica que los procesos no se cumplen, cinco que los procesos se cumplen en un 50% y diez establece que los procesos se cumplen en su totalidad, es decir, en un 100%.

Concluido lo anterior, se elaboró la matriz de riesgo – confianza, para la obtención del grado de confianza y nivel de riesgo, resultante de la fórmula en el manual general de auditoría (CGE, 2003).

$$\mathrm{CP} = \frac{\mathrm{CT} * 100}{\mathrm{PT}} \qquad \textbf{[1]}$$

Donde, CP es la calificación porcentual, CT es la calificación total y PT es la ponderación total. Para identificar el grado de confianza y nivel de riesgo de cada componente se utilizó el cuadro 1 (CGE, 2003).

Cuadro 1. Matriz que determina el grado de confianza y el nivel de riesgo.

Calificación porcentual	Grado de Confianza	Nivel de riesgo	Colores
15 – 50	Bajo	Alto	Rojo
51 – 75	Moderado	Moderado	Amarillo
76 - 95	Alto	Bajo	Verde

Fuente: Contraloría General del Estado, 2003.

El cuadro 1 está divido en columnas, donde la calificación porcentual se detalla en escala, e inicia en el 15% porque no existe entidad totalmente sin control, y termina con el 95% porque tampoco hay una empresa con control total eficiente y efectivo, debido a que toda entidad está sujeta a una mejora continua. En la columna de grado de confianza se detalla el nivel, que puede ser bajo, moderado o alto, estos valores porcentuales son proporcionales al nivel de riesgo, definidos en la tercera columna y que alcanza la calificación de alto, moderado o bajo; en la última columna, se asigna un color dependiendo del grado de confianza; rojo para un grado de confianza bajo y nivel de riesgo alto, amarillo para el grado de confianza moderado y nivel de riesgo moderado y verde para el grado de confianza alto y nivel de riesgo bajo. Los resultados obtenidos se detallan en una matriz individual donde se describe el análisis.

Un primer paso para plantear la solución del problema de la baja documentación de los procesos, es mediante el diseño del diagrama de Ishikawa (Rodríguez y Ordoñez, 2012), el cual resume las causas y el efecto de la investigación. Para establecer la fidelidad de datos se observaron respuestas coherentes de los cuestionarios, en cuatro preguntas escogidas con idéntica formulación, este mismo proceso se realizó en todos los cuestionarios. El análisis de las respuestas se realiza con el método estadístico no paramétrico del coeficiente de concordancia de Kendall (w*,)* (Ruiz, 2012), que ofrece un valor que posibilita establecer el nivel de concordancia, como lo indica su nombre, entre los encuestados. La comprobación se lleva a cabo evaluando la respuesta de cada persona, clasificándola en base a una escala del uno a cuatro,

donde, uno es el parámetro con mayor nivel de cumplimiento y cuatro el parámetro con menor nivel (Romero y Díaz, 2010).

La fórmula del coeficiente de coincidencias de Kendall utilizada es la siguiente:

$$w = \frac{12\sum A^2}{n^2\, n(k^2 - 1)} \qquad \textbf{[2]}$$

Donde (w) es coeficiente de coincidencia; $\sum A^2$ la suma de ponderaciones; n es el número de personas entrevistadas y, k el número de preguntas. Para obtener la ponderación A**,** ésta es realizada para cada pregunta evaluada y, aplicada a la siguiente fórmula:

$$A = \sum aij - T \qquad \textbf{[3]}$$

Donde, A es la ponderación; ($\sum$aij) es la suma de puntuación; $\sum aij$ es la sumatoria de ponderación, y T es el factor de comparación. A continuación se presenta la fórmula de T***:***

$$T = \frac{\sum aij}{K} \qquad \textbf{[4]}$$

Donde T es el factor de comparación; $\sum aij$ es la suma de puntuación y K es el número de preguntas*.* Para el análisis es necesario que Si *w* ≥ 0.5 existe concordancia en las respuestas, si w < 0.5 entonces debería repetir el estudio porque no existe concordancia, es decir, los datos no son confiables. Finalmente se ha de comprobar que Si n ≥ 7 y w < 0.5 el estudio no sería válido (Pérez, 2007).

En el cuadro 2 se muestran los valores de cumplimiento de control interno, asignados a cada persona responsable, en la columna de ∑aij figuran los valores sumados por cada pregunta estudiada, la columna de A muestra los valores de la fórmula [2] y la última columna muestra la ponderación elevada al cuadrado.

Para la fase de la ejecución, se aplicaron los programas de auditoría por componente, en el que se determinan las pruebas de cumplimiento, que sirven, para evaluar los controles y verificar su operación, por lo que se documentan las medidas existentes en cada proceso que lleva a cabo la entidad, detallando las actividades desarrolladas en la carrera Informática según la información recopilada, se expone la información mediante hojas de hallazgos que describen como son llevados los controles, basados y justificados en la legislación ecuatoriana.

Finalmente, la fase de comunicación de resultados, resume los eventos significativos obtenidos en las fases anteriores, estos insumos permitieron la elaboración del informe final de auditoría, que describe los: a) Objetivos y alcance de la auditoría

según el plan de auditoría, b) Antecedentes generales, c) Observaciones, d) Conclusiones y recomendaciones, sobre las características de seguridad y confiabilidad de los recursos de tecnología de información. Este informe es presentado a la persona que dirige la entidad.

RESULTADOS Y DISCUSIÓN

Aplicada la evaluación de control interno a la carrera Informática, se analizaron los componentes planteados, de los que se presenta el resumen de los niveles de riesgo y grados de confianza mediante una matriz general.

Como se observa en el gráfico 1, los datos presentados están basados en la calificación porcentual contemplada en la matriz de riesgo **-** confianza del manual de auditoría para las entidades del sector público del Ecuador, emitido por la Contraloría General del Estado, por lo cual establecieron los siguientes resultados: en el data center, el nivel de confianza sobre las medidas de seguridad implantadas es de un 62.50% frente a la proporcionalidad de riesgo un 37.50%, situación que se presenta por la aplicación de directrices generales de seguridad, debido a que no se han documentado políticas específicas de funcionamiento y protección de los recursos que posee esta área.

Por consiguiente, la protección de activos tangibles en la carrera Informática tiene un nivel de confianza del 56.25% y la proporción de riesgo es del 43.75%; escenario que surge debido a que no se han establecido programas documentados de mantenimiento para los recursos tecnológicos, ni políticas de uso o medidas a seguir en caso de desastres. En la protección de activos intangibles el porcentaje de confianza es del 67.85%, ante un porcentaje proporcional de riesgo del 32.15%; es decir, las personas conocen, cuáles son sus funciones y de qué son responsables en cuanto al manejo de información de la entidad, sin embargo, no existen procedimientos documentados que certifiquen dicha acción.

En la gestión de mantenimiento, el 44.11% corresponde a la confianza y el 55.89% es de riesgo; manteniéndose así, un nivel considerable de riesgo, debido a que no existen planes documentados que certifiquen el mantenimiento continuo y buen uso de los recursos que posee la entidad. Por último, en el área de gestión de desarrollo de software, el nivel de confianza es del 50%, y el riesgo es del 50%.

En conclusión, que el sector con mayor nivel de confianza está en la protección de los activos intangibles con una confianza del 67.85% y el componente con menor nivel de confianza es la gestión de mantenimiento con un 44.11%.

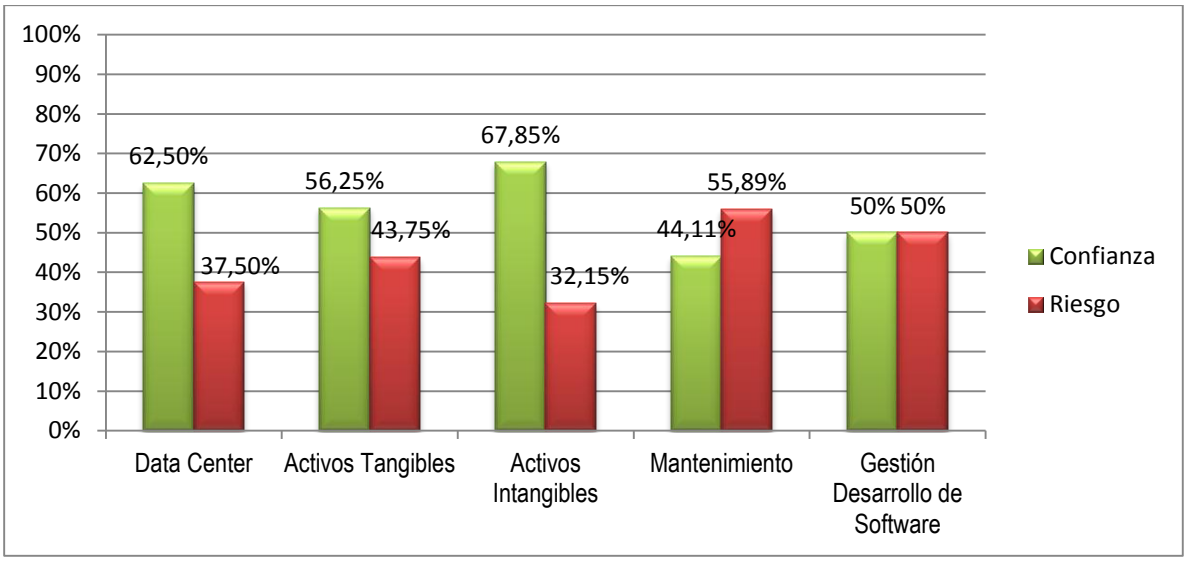

Gráfico 1. Nivel porcentual del riesgo confianza en la carrera Informática

Previo a la aplicación del análisis estadístico no paramétrico de Kendall, se diseñó el diagrama de Ishikawa para determinar las causas y el efecto referido a la seguridad de la carrera para los recursos de tecnología de información, como lo muestra la figura 1:

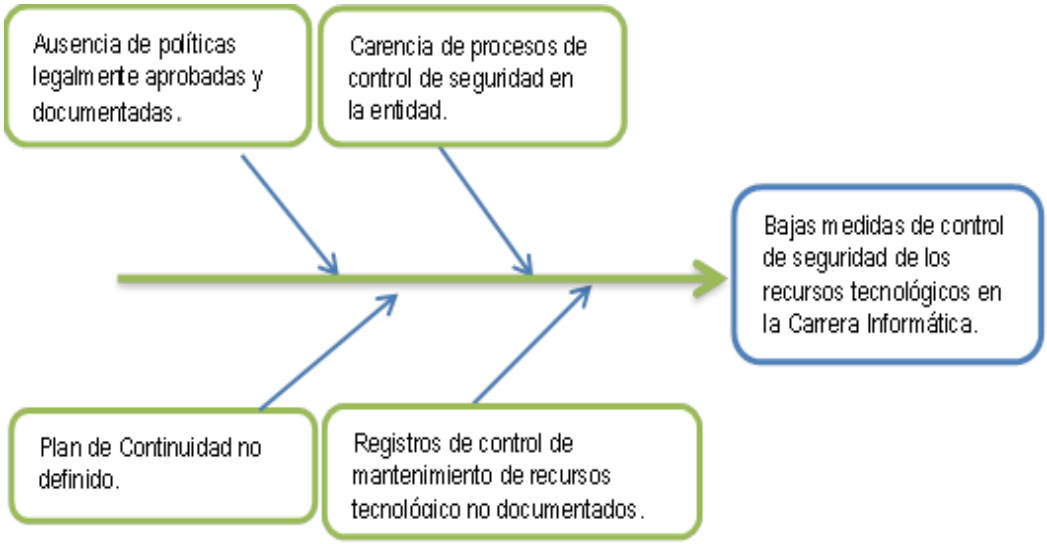

Figura 1. Diagrama de Ishikawa de medidas de seguridad.

Aplicándose la fórmula de coeficiente de concordancia de Kendall, para demostrar la coincidencia o no de las respuestas, se obtuvieron los siguientes valores reflejando en el cuadro 2 una vez aplicadas las fórmulas, [2], [3], [4].

Cuadro 2. Concordancia de preguntas similares de los cuestionarios aplicados

Ítem K	Preguntas	Director de carrera	Administración de data center y redes	Asistencia de TIC	Coordinador de UPS	∑ aij	A	A^2
1	Existencia de políticas de seguridad documentadas.	4	4	3	4	15	5	25
2	Existencia de mecanismos de acceso físico al área.	2	1	2	2	7	-3	9
3	Existencia de registro de entrada y salida de recursos tecnológicos.	3	3	4	3	13	3	9
4	Existencia documentada de las funciones y responsabilidades en las áreas.	1	2	1	1	5	-5	25
						40		**68**

Fuente: Cuestionarios de control interno

Obtenidos los datos se trasladaron a la fórmula de concordancia, logrando un nivel de w = 0.85, valor que claramente supera el valor base, es decir, el de w = 0.5, esto significa que existe concordancia en las respuestas de los encuestados. En definitiva, que se cumplen los dos parámetros establecidos por Kendall: w y n, datos que permiten elaborar las conclusiones.

Para el análisis de los procedimientos desarrollados en la presente auditoría, se realizaron comparaciones con otros trabajos investigativos, cuyas características fueran lo más similar a la auditoría aplicada en la carrera Informática, como la auditoria en seguridad informática realizada en el departamento de tecnologías de la Universidad Estatal de Milagro (Bermeo, 2012), y la Auditoria a los Centros de Cómputo de almacenes Carito de la ciudad de Guayaquil (Cortés y Machuca, 2011), las cuales usaron la metodología basada en las Normas Internacionales de Auditoría, que se complementaron con las Normas de Control Interno, emitidas por la Contraloría General del Estado que permite calificar la eficacia de los controles relacionados con la confiabilidad de la información.

Es así, que se concuerda con los trabajos mencionados anteriormente, con respecto al uso de la normativa legal vigente en el país, que admite evaluar el control interno

en el uso de los recursos tecnológicos de las entidades auditadas, cuya metodología sirve de referencia para posteriores evaluaciones, proporcionando seguridad en la ejecución de los procesos de la entidad. A diferencia de los trabajos citados, el presente incluye el método estadístico no paramétrico, denominado coeficiente de concordancia de Kendall, para determinar el nivel de similitud entre las respuestas de las personas a las que se les aplicó el cuestionario y así obtener mayor confiabilidad de los datos.

CONCLUSIONES

Mediante la aplicación de la evaluación de control interno y la observación se determina que la auditoría de seguridad física y lógica de los recursos de tecnología de información en la carrera Informática han establecido lineamientos generales de seguridad que no están documentados, ratificado por el resultado del coeficiente de concordancia de Kendall con un valor equivalente al 0.85 de coincidencia, lo que demuestra que conocen las vulnerabilidades a las que están expuestos.

Para el cumplimiento de la seguridad de los recursos de tecnología, los pilares importantes a considerar son, los recursos tecnológicos, los procesos y las personas que interactúan con ellos, por lo que las medidas adoptadas, han de normarse, a través de una política de seguridad para dar cumplimiento a las Normas de Control Interno emitidas por la Contraloría General del Estado, la misma que hade incluir a todas las actividades donde los recursos de tecnología de información estén presentes con el fin de garantizar la continuidad de sus operaciones.

La entidad debe elaborar un plan de continuidad de operaciones y un plan de mantenimiento, como medida preventiva y correctiva para evitar que las vulnerabilidades se materialicen y así dar cumplimiento a lo establecido en la normativa ecuatoriana y para que la cultura de seguridad sea adoptada con un sentido de responsabilidad compartida en todos los niveles de la entidad, requiriendo del apoyo de todo el personal involucrado.

LITERATURA CITADA

Bermeo, J. (2013). Análisis de la auditoria en seguridad informática. Maestría en Gerencia de Tecnologías de la Información. UNEMI. Milagro. EC. p. 1-206.

Castro, E. 2009. Tendencias de la auditoria informática. Cali, CO. Revista Ingenlum Ciencia & Tecnología. 4(8): 69-98.

CGE (Contraloría General del Estado). 2003. Manual General de Auditoría Gubernamental de las Entidades y Organismo del Sector Público y para las

Firmas privadas de auditorías contratadas. Acuerdo 012-CG-2003, RO 107 19 de Jun.

CGE (Contraloría General del Estado). 2009. Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. Acuerdo Nº 039 CG-2009. San Francisco de Quito, EC. 16 de nov.

Cortes, M; Machuca, J. 2011. Auditoría de Centros de Cómputo. Escuela Superior Politécnica del Litoral. p. 58.

Chávez, J. y Rodríguez, E. 2012. La auditoría interna como herramienta de gestión de las organizaciones públicas y privadas. Revista Ciencia y Tecnología, PE. 8(22): 163-178.

Delgado, A. 2009. Sistema Informático de Apoyo a la Evaluación del Control Interno. Revista de Arquitectura e Ingeniería, 3(19): 1-61.

Franco, D; Perea, J; Tovar, L. 2013. Herramienta para la detección de vulnerabilidades basada en la identificación de servicios. Revista de Información tecnológica. La Serena. 24(5): 1-10.

James, M. 2009. Medidas de Seguridad. Pereira, CO. Revista Tecnológica de la Universidad Tecnológica de Pereira. Año XV(X):12.

Lara, A. y Párraga, F. 2010. Aplicación de la teoría de los procesos transformados y alterados a la auditoría informática. Sangolquí, EC. Revista Digital ESPE. 1(1): 1-80.

Martínez, Y. 2012. Auditoria en Informática. CU. Revista de Ingeniería. 6(2): 14.

Morlanes, G. 2012. Seguridad Informática, Matanzas, CU. Revista de Arquitectura e Ingeniería, 6(2): 1-14.

Pérez, H. 2007. Estadísticas para las ciencias sociales, del comportamiento y de la salud, 3ed, MX. Cengaee Learning Editores S.A.: 545-547

Piattini, M; Del Peso, E.; Del Peso, M. 2008. Auditoria de Tecnologías y Sistemas de Información. 4ed. Madrid, ES. RA-MA. 1378: 38.

Pinket, F. 2006. Automating System Security Audits. Information Systems Control Journal. ISACA. 1: 45–46.

Ramírez, G. y Álvarez, E. 2008. Auditoría a la gestión de las tecnologías y sistemas de información. Revista de Investigación. PE. 6(1): 99-102.

Rodríguez, M. y Ordoñez, R. 2012. Modelo de gestión para la calidad en las prácticas de pedagogía. Profesorado. Revista Iberoamericana de Ciencia, Tecnología y Sociedad. 16(3): 1-16.

Romero, E y Díaz, J. 2010. El uso del diagrama causa-efecto en el análisis de casos. MX. Revista Latinoamericana de Estudios Educativos. XL(3-4): 127-142.

Ruiz, T. 2012. Utilización del Método de los expertos (Delfos) para la validación de una estrategia pedagógica. Revista Órbita Científica. 18(69):1-12.