EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27000

Ricardo Vallejo 1, Edwin Vivanco 2, Nancy Velásquez 3, Fidel Castro 4

1 Departamento Técnico; Universidad Tecnológica Equinoccial, Quito, Ecuador

2 Departamento Técnico; Universidad Tecnológica Equinoccial, Quito, Ecuador

3 Docente tutor de la Tesis; ESPE, Sangolquí, Ecuador

4 Docente Oponente de la Tesis; ESPE, Sangolquí, Ecuador

rvallejo@ute.edu.ec; evivanco@ute.edu.ec; Nancy.velasquez87@hotmail.com; flcastro@espe.edu.ec

Resumen:

El presente trabajo tiene como objetivo evaluar la seguridad de la información del proceso de admisión de estudiantes de pregrado en la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000 para determinar el nivel de seguridad y elaborar un plan de tratamiento de riesgos que permita dar respuesta a los riesgos de seguridad de la información asociados a este proceso.

En el desarrollo del trabajo se utiliza una metodología de evaluación de seguridad de la información basada en riesgos con su fundamento en la norma NTE INEN-ISO/IEC 27005:2012 elaborada por los autores, en la cual, se establecen los pasos a seguir y las actividades a realizar en cada etapa del proceso hasta obtener los resultados finales sobre la brecha de seguridad respecto a la norma ISO/IEC 27001:2005 y el plan de tratamiento que mitiguen los riesgos priorizados acorde a los criterios de aceptación definidos por el Rector de la UTE.

La investigación se apoya en entrevistas, encuestas, observaciones, pruebas de cumplimiento y sustantivas a los controles del proceso de Admisión de estudiantes, se realizan valoraciones cualitativas para obtener el nivel de estimación del riesgo, se evalúan y se priorizan los riesgos en función de los criterios definidos por el Rector de la Universidad para proporcionar las acciones de tratamiento.

Como resultado del estudio se determina el nivel de seguridad de la información a través del cumplimiento de la seguridad que realiza la Universidad respecto a los requisitos obligatorios y los controles de la norma ISO/IEC 27001:2005. También, se determinan los activos críticos que podrían tener afectación, la cantidad de

riesgos de nivel alto, medio y bajo, y se plantean acciones para mitigar los riesgos de nivel prioritario.

Palabras clave: Seguridad de la Información, ISO/IEC 27000, Proceso de Admisión, Gestión de Riesgos, Análisis de brecha de seguridad.

6. Abstract: *El mismo resumen traducido al idioma inglés y revisado por un angloparlante.*

This paper aims to assess the information security of the admission process of undergraduate in Universidad Tecnológica Equinoccial based on ISO/IEC 27000 international standard for determining the level of security and develop a risk treatment plan that allows responding to the risks of information security associated with this process.

In this research project the authors use an owner methodology for evaluating information security risks based in the NTE INEN-ISO/IEC 27005:2012 standard, in which the steps are set to continue to use and activities to be performed at each stage of the process to obtain the final results in the breach of security regarding the ISO / IEC 27001:2005 and the treatment plan to mitigate the risks prioritized according to the acceptance criteria defined by the President of UTE.

The research is based on interviews, surveys, observations, compliance testing and background testing to the controls of Admission process, qualitative estimation of the level of risk assessments are made, risks are evaluated and prioritized based on the criteria defined by the President of the University to provide treatment actions.

As a result of the study the level of information security is determined by compliance with safety making the University regarding to the mandatory requirements and controls of ISO/IEC 27001:2005. Critical assets that could have affected the amount of risk of high, medium and low are also determined, and actions were taken to mitigate the risks of priority level.

Key words: Information Security, ISO/IEC 27000, Admission, Risk Management, GAP analysis.

I. Introducción

Actualmente, en la Universidad existen mecanismos de seguridad informática implementados que intentan reducir los riesgos asociados al proceso, sin embargo, se han identificado incidentes de seguridad en la protección de los exámenes, divulgación de preguntas del examen, interrupción del servicio, explotación de vulnerabilidades técnicas por desconocimiento de los usuarios, entre otros. En este contexto, las autoridades de la Universidad preocupadas por la seguridad de la

información necesitan conocer el nivel de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos.

En el presente trabajo toma como referencia investigaciones realizadas sobre gestión de riesgos de la seguridad de la información, por ejemplo, el estudio de Arean Melo que enfatiza la alineación de las organizaciones a la norma ISO/IEC 27001:2005 para asegurar el cumplimiento jurídico relacionado con la seguridad de la información (Melo, 2008) y el estudio desarrollado por la Universidad Nacional de Malasia que comprueba que los riesgos más comunes y de mayor impacto en las Universidades son los riesgos financieros, de enseñanza y aprendizaje, estratégico y de reputación (Huber, 2011).

El estudio concluye que se debe realizar mediante un enfoque integrado de riesgos para mantener la uniformidad de criterios e identificar en un modelo macro los riesgos más importantes de las Universidades en todas las áreas, siempre basándose en una norma de general aceptación o marco común como las propuestas por la ISO, como la 9001, 27001 y 30001. (Sayef Sami Hassen, 2013, pp. 1–7)

Se utiliza la investigación de campo e investigación documentación – bibliográfica, con técnicas de recolección de datos basadas en la observación del proceso, entrevistas a los dueños de los procesos, autoridades y personal de apoyo, y el empleo de documentos para determinar el cumplimiento respecto a la norma.

Se realiza pruebas de cumplimiento y sustantivas de ciertas vulnerabilidades encontradas durante las etapas de observación y entrevistas. En la evaluación de riesgos se utiliza el método cualitativo descrito en la norma NTE INEN-ISO/IEC 27005:2012 para determinar el nivel de riesgos y la brecha de seguridad. El trabajo se complementa con la aplicación de encuestas a los aspirantes para conocer su apreciación respecto a la seguridad y confiabilidad del proceso.

El aporte del trabajo se enfoca a los resultados de la evaluación de seguridad de la información (brecha de seguridad y plan de tratamiento de riesgos) del proceso de admisión de estudiantes, que permite a las autoridades conocer el nivel de seguridad, proporcionar las acciones necesarias para mitigar los riesgos encontrados y dar los primeros pasos en la implantación de un sistema de gestión de seguridad de la información alineado a la ISO/IEC 27001:2005.

En tal sentido, el presente trabajo describe la metodología basada en la norma NTE INEN-ISO/IEC 27005:2012 que se utilizó en la evaluación de seguridad de la información y los resultados generales de la evaluación aplicada al caso de estudio: proceso de admisión de aspirantes de pregrado en modalidad presencial en Quito de la Universidad Tecnológica Equinoccial (UTE).

II. Metodología

En la investigación se aplica una metodología desarrollada por los autores, basada en la norma NTE INEN-ISO/IEC 27005:2012 y conformada por un conjunto de etapas a seguir para realizar la evaluación de seguridad de la información. En la figura 1 se ilustra la "Metodología de evaluación de seguridad de la información".

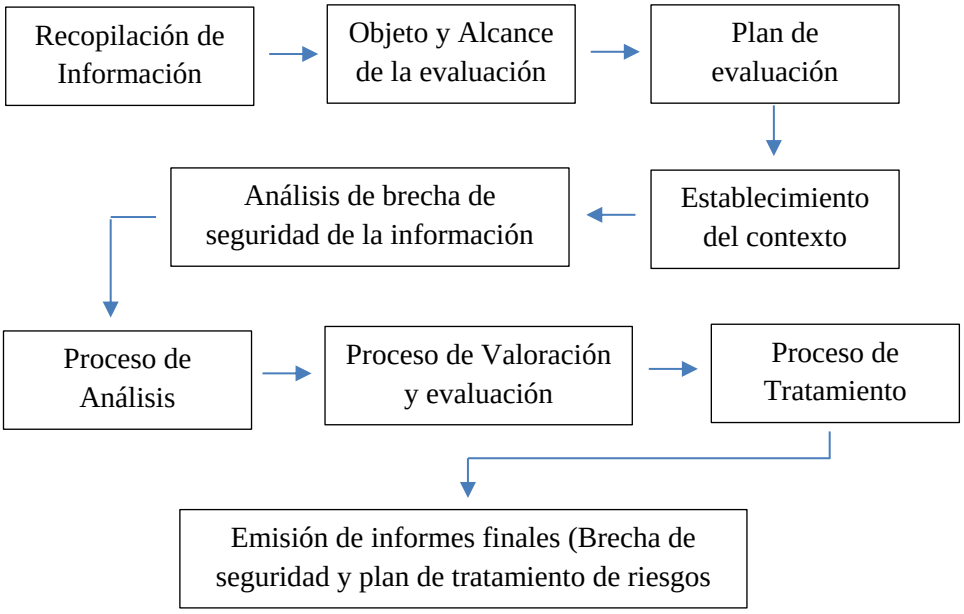

Figura 1: Metodología de evaluación de seguridad de la información

1. Recopilación de información: Consiste en realizar la observación inicial del entorno de la organización, por ejemplo, conocer su estructura, misión, visión, los procesos, sus detalles y las relaciones entre ellos. En esta etapa los evaluadores tendrán un acercamiento general a la documentación, registros y recursos que se utilizan en la institución y sus procesos.

2. Objeto y alcance de la evaluación: En esta etapa se define cual será el objeto que conduce a la evaluación de seguridad de la información y sobre qué procesos de la organización se aplicará la evaluación. El establecimiento del alcance permite enfocar la evaluación de riesgos a los requerimientos de la organización, con el fin de garantizar que todos los activos de información más importantes se toman en cuenta durante la evaluación de seguridad. Esta etapa debe ser aprobada por la alta dirección de la organización.

3. Plan de la evaluación: En etapa se evalúa la viabilidad de alcanzar los objetivos del proyecto, se detallan las actividades a realizar durante la evaluación de seguridad, la estimación de recursos y tiempos requeridos para la ejecución de

cada actividad. También, se establece un plan de evaluación que contiene los procesos que se van a evaluar, el centro, el día y hora, el evaluador asignado y el responsable del proceso. El plan de evaluación debe ser aprobado por los usuarios para acordar los tiempos de entrevistas y observaciones sobre el proceso.

4. Establecimiento del contexto: Consiste en establecer los criterios básicos definidos por la alta dirección de la organización:

- *Criterios de evaluación del riesgo* teniendo en cuenta el valor estratégico, criticidad de los activos, requisitos legales y reglamentarios, disponibilidad, confidencialidad e integridad y las expectativas de las partes interesadas.
- *Criterios de impacto.*- Se especifica en términos del daño o costo para la organización causados por un evento adverso de seguridad de la información.
- *Criterios de aceptación del riesgo (apetito del riesgo).*- Se especifica bajo qué criterios se aceptarán los riesgos, dependerán de las políticas, objetivos organizacionales y de las autoridades organizacionales.

5. Análisis de brecha de Seguridad de la Información: En esta etapa se determina donde los déficits pueden estar ocurriendo y que podrían afectar al cumplimiento de los objetivos de seguridad. Consiste en determinar el cumplimiento de los requisitos obligatorios de la norma ISO/IEC 27001:2005 y los controles del Anexo A. Se aplica un análisis cualitativo mediante la asignación de un valor y porcentaje de cumplimiento por cada requisito y control, en función la escala de cumplimiento que se muestra en el cuadro 1.

Cuadro 1: Escala de cumplimiento

Nivel	Cumplimiento	Porcentaje
0	No está definido ningún control	0%
1	No existen controles efectivos - Deficiencias considerables respecto a lo esperado	25%
2	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento	50%
3	El requerimiento se cumple de manera efectiva	100%

La determinación del nivel de cumplimiento de cada capítulo, dominio de control y del sistema de gestión de seguridad se obtiene a través del cálculo promedio de los valores parciales de cada requisito normativo.

6. Proceso de análisis: En esta etapa se identifica y se analiza los posibles riesgos que pueden afectar o causar daño a la organización, se compone de las siguientes fases:

Identificación del riesgo: En esta etapa se determina que podría suceder y causar una pérdida potencial, comprender cómo, dónde y por qué podría causar esta pérdida. Esta fase se compone de 4 actividades principales:

Identificación de activos: Consiste en identificar los activos más relevantes que forman parte del proceso evaluado, y que requieren protección. Se determinan los requerimientos de seguridad de la información especificados por los dueños del proceso y la valoración inicial asignada por la alta dirección. Los activos son clasificados en dos tipos: activos principales y activos de apoyo; cada activo con su categoría y subcategoría según se corresponda. El listado de categorías de activos sugeridos por los autores se basa el Anexo B de la norma NTE INEN-ISO/IEC 27005:2012 y el Libro II de Catálogos de elementos de Magerit.

Identificación de amenazas: Consiste en identificar las amenazas que potencialmente pueden causar daño a los activos, tales como información, procesos y sistemas. Como parte de la metodología se debe identificar el tipo de amenaza, la amenaza en sí y el origen de la misma: Deliberada (D), Accidental (A) y Ambientales (E).

Identificación de controles: Consiste en identificar los controles existentes para evitar trabajo o costos innecesarios, y los controles planificados por la organización. Se basa en la revisión de documentos, verificación con las personas responsables y la revisión en sitio.

Identificación de vulnerabilidades: En esta fase se deben identificar todas las vulnerabilidades que pueden ser explotadas por las amenazas y podrían afectar a los activos. Por cada amenaza se debe identificar las vulnerabilidades a nivel organizacional, en los procesos y procedimientos, gestión, personal, ambiente físico, configuraciones, hardware software e interacción con las partes externas.

7. Proceso de valoración y evaluación: En esta etapa se define la metodología de análisis que se utilizará para estimar el riesgo, siendo: cualitativa, cuantitativa o una combinación de las dos. Está compuesta de las siguientes fases:

Valoración de los activos: La valoración de los activos se realiza mediante métodos diferentes, dependerá del tipo de activo, se asigna un valor de 0 a 4 según corresponda. Para la valoración se realiza en función de la clasificación de información y escala de valoración inicial de los criterios de seguridad. En otros casos se utiliza valores monetarios de reposición del activo, de reconfiguración, pérdida, valor invertido en capacitación de personas, sueldos por año, entre otros.

Valoración de las consecuencias: La valoración de consecuencias permite determinar las acciones negativas que pueden producirse si se materializa una amenaza, en relación a los objetivos y requerimientos institucionales de la seguridad de la información. Por cada activo se debe especificar el impacto en función de la pérdida de confidencialidad, disponibilidad e integridad, en el

aspecto legal o reglamentario y las pérdidas económicas. El valor del impacto se asigna en base a una escala cualitativa: Alto, Medio y Bajo.

Valoración de los incidentes: La valoración de los incidentes se basa en la asignación de un valor a la facilidad de explotación de las vulnerabilidades y otro valor a la probabilidad de que una amenaza se materialice y afecte negativamente a las operaciones de la organización. El valor de un incidente se asigna en base a una escala cualitativa: Alto, Medio y Bajo.

Nivel de estimación: La estimación del riesgo se basa en el segundo método propuesto en el Ejemplo E.2.1 del anexo E de la norma NTE INEN-ISO/IEC 27005:2012, propone realizar la valoración de los riesgos en función de la amenaza y vulnerabilidad (probabilidad) y del impacto (consecuencia) en la organización, los datos se muestran en el Cuadro 4.

Cuadro 2: Matriz de valoración detallada de los riesgos de seguridad de la información

	Probabilidad de ocurrencia -Amenazas	**L**			**M**			**H**		
	Facilidad de explotación vulnerabilidades	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Impacto en el negocio	L	0	1	2	1	2	3	2	3	4
	M	1	2	3	2	3	4	3	4	5
	H	2	3	4	3	4	5	4	5	6

Evaluación del riesgo: En esta fase se compara los riesgos estimados con los criterios de evaluación del riesgo que se definieron en el establecimiento del contexto. La evaluación del riesgo provee de la información necesaria para tomar decisiones sobre las acciones futuras.

8. Proceso de tratamiento: En conformidad con la norma NTE INEN-ISO/IEC 27005:2012, en esta etapa se seleccionan las opciones para reducir (seleccionar y proponer controles adecuados), retener (necesario implementar controles adicionales), evitar (analizar la opción de retirar alguna actividad o modificar las condiciones en las cuales se desarrolla tal actividad) o transferir el riesgo (compartir algunos riesgos con partes externas a la organización). Los riesgos son priorizados en función del nivel de riesgo: Prioritario (5 y 6), medio (3 y 4) y Bajo (0, 1 y 2).

A partir de la decisión organizacional sobre las opciones de tratamiento, se elabora el plan de tratamiento no valorado o valorado, dependerá del alcance de la evaluación; en el primero se describe las acciones a tomar y los responsables de ejecutarlas, en el segundo se incluye además, los costos y tiempos requeridos para ejecutar dichas acciones.

9. Emisión de Informes Finales: Brecha de Seguridad y Plan de Tratamiento de los Riesgos

En esta etapa se elaboran los informes finales: la brecha de seguridad y el plan de tratamientos de riesgos priorizado. Cada informe final se entrega a la alta dirección de la organización, debe ser claro, conciso y ordenado, emitir recomendaciones fundamentadas en las mejores prácticas y en el contexto de la evaluación.

III. Evaluación de resultados y discusión

Respecto a los requisitos obligatorios de la norma NTE INEN-ISO/IEC 27001:2005 se determina que la Universidad alcanza un nivel bajo de cumplimiento, no dispone de un Sistema de gestión de seguridad de la información formalmente implantado y requiere invertir mayores esfuerzos para alinear la gestión a las mejores prácticas de la norma.

La Universidad posee documentos y registros de las actividades de seguridad de la información, sin embargo, no existen procedimientos formales implementados para realizar esta actividad y se encuentran fuera del contexto del SGSI. No existen revisiones de la gestión de seguridad de la información por parte de las autoridades de la institución, no se realizan auditorías para identificar las conformidades y no conformidades respecto a la norma, ni acciones correctivas, acciones preventivas y mejora continua.

Respecto a los controles del anexo A, el cumplimiento de la Universidad es de nivel medio bajo, se determina que carece de una política de seguridad de la información y no dispone de una unidad organizacional que se encargue de coordinar y ejecutar el sistema de gestión de seguridad de la información.

De los 131 controles del Anexo A aplicables al caso de estudio, la Universidad tiene un cumplimiento bajo, existen controles que se encuentran en estado básico, controles deficientes y controles que no se han implementado.

La debilidad mayor se encuentra en la seguridad organizativa, debido a la falta de procesos, procedimientos y políticas que orienten la gestión, y a la falta de una cultura institucional en temas de seguridad de la información.

De la evaluación de riesgos se determinó que existen 99 activos importantes para el proceso de Admisión, clasificados en las categorías: procesos, información, servicios, software, hardware, red, personal, sitios y organización, de los cuales, el 22.2% (22) de los activos están expuestos a riesgos de nivel alto que podrían afectar al servicio que brinda la Universidad.

Existen 524 riesgos identificados sobre los activos, el 58.6% (307) de los riesgos son de nivel bajo, el 32.1% (168) tiene una afectación media y el 9.4% (49) son

riesgos prioritarios con un impacto alto en la institución y que no han sido analizados antes del estudio.

A continuación se describen las acciones principales del plan de tratamiento sugeridas para mitigar los riesgos encontrados en el proceso de Admisión:

- Crear un organismo que se encargue de establecer las directrices del sistema de gestión y crear el área de seguridad de la información para coordinar y ejecutar las actividades relacionadas al sistema de gestión de seguridad.
- Desarrollar, aprobar y difundir una política de seguridad de la información para toda la Universidad.
- Definir las directrices generales para el buen uso de los activos más importantes de la Universidad
- Crear los procedimientos y protocolos relacionados a la seguridad de la información y difundirlos adecuadamente a todo el personal involucrado en el proceso de admisión.
- Capacitar y concientizar al personal sobre la seguridad de la información para minimizar la probabilidad de materialización de una amenaza.
- Implantar una metodología de gestión de riesgos formal que permita evaluar los riesgos y reajustar el plan de tratamiento de riesgos acorde a los cambios en la Universidad.

Conclusiones y trabajo futuro

- La metodología propuesta se diferencia de la norma NTE INEN-ISO/IEC 27005:2012 porque define el proceso a través de un conjunto de pasos específicos para realizar la evaluación de seguridad de la información y conseguir mejores resultados.
- La selección de la metodología de gestión de riesgos que se aplicará a una organización, depende de su situación actual y los requerimientos de seguridad definidos por la alta dirección.
- Las directrices de la gestión de riesgos basada en NTE INEN-ISO/IEC 27005:2012 brindan un soporte continuo a los requisitos del sistema de gestión de seguridad de la información basado en ISO/IEC 27001, permiten plantear recomendaciones oportunas y reducir el riesgo a un nivel aceptable.
- La gestión de la seguridad de la información y la gestión de riesgos son sistemas dinámicos que se adaptan fácilmente a los cambios organizacionales a fin de mantener o mejorar la efectividad de los controles implementados y el nivel de seguridad en toda la organización.
- Las organizaciones deben alinear las directrices de seguridad de la información y la gestión de riesgos a los requerimientos definidos por la alta dirección para asegurar el cumplimiento de los objetivos del negocio.
- La participación de la alta dirección en el proceso de gestión de riesgos y en el sistema de gestión de seguridad es de vital importancia para establecer un compromiso en toda la organización, definir los lineamientos de seguridad,

implementar el sistema y priorizar las acciones del plan de tratamiento que reducirán la ocurrencia de los riesgos.

La metodología propuesta cumple con lo requerido en la norma de gestión del riesgo en la seguridad de la información NTE INEN-ISO/IEC 27005:2012 y permite obtener resultados confiables y efectivos en una evaluación de seguridad de la información. A futuro se la puede ampliar agregando indicadores y métricas para medir la eficiencia de un SGSI.

Agradecimientos

Extendemos nuestro agradecimiento a la Universidad Tecnológica Equinoccial por brindarnos apoyo constante y la información necesaria para la investigación.

Referencias Bibliográficas

Huber, M. (2011, July). The risk university: Risk identification at higher education institutions in England. Monograph. Retrieved August 6, 2013, from http://www.lse.ac.uk/CARR

ISO 27000. (n.d.). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved August 5, 2013, from http://www.iso27000.es/sgsi.html Sección 2a - 2f

Melo, A. H. (2008). El derecho informático y la gestión de seguridad de la información. Una perspectiva con base en la norma ISO27001. *Revista de derecho, 29*, 336-366. Recuperado el 30 de 07 de 2013, de http://web.ebscohost.com/ehost/detail?sid=a59e203e-0dbc-4961-8e73-dbf6c42ce4a0%40sessionmgr11&vid=1&hid=26&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=a9h&AN=34969402

Sayef Sami Hassen, M. S. Z. (2013). Managing University IT Risks in Structured and Organized Environment. *Journal of Applied Sciences, Engineering and Technology*, 2270–2276.