Diseño de una metodología para auditar la seguridad de la información en productos de software orientados a servicios de gestión e información en instituciones de educación superior

Design of a methodology to audit the security of information in software products that are oriented to management services and information in post secondary institutions

Arelis Gómez Nova
Universidad Autónoma de Bucaramanga
Candidata Magister
Bucaramanga - Colombia
E-mail agomez439@unab.edu.co

Reinaldo Mayol Arnao, PhD
Universidad Pontificia Bolivariana
Director de Tesis
Medellín - Colombia
E-mail: reinaldo.mayol@upb.edu.co

Resumen

El artículo, describe el diseño de una metodología para auditar la seguridad de la información en productos de software orientados a servicios de gestión e información académica. La investigación se planteó a partir de la identificación de riesgos de seguridad de la información materializados en los procesos organizacionales y en la carencia de procesos de auditoría en seguridad de la información en instituciones de educación superior. Se optó por implementar una guía sistemática que evalúe el estado de la gestión en seguridad de la información, con el fin de contribuir a la detección de amenazas y vulnerabilidades para mitigar el riesgo informático. La estructura metodológica se diseñó para evaluar tres dimensiones dentro de la organización: gobierno universitario, sistemas de información y mantenimiento y soporte tecnológico. Se diseñaron tres criterios que reúnen los controles recomendados en la norma ISO/27000 y el marco de referencia COBIT 5.

Palabras Claves: Información, metodología, seguridad, riesgo, software.

Abstract

His paper describes the design of a methodology to audit information security in software products, for academic information services. The research is supported on the identification of information security risks materialized in the organizational processes. We have implemented a guide to evaluate the state of security management process that can be used for the detection of risks and vulnerabilities as well as the lack of controls that mitigate them. In our methodology there are three dimensions that decompose the organization, ie: Government, Information Systems, Maintenance and Support. All the work is based on the criteria emanated from ISO 27001 and COBIT 5 standards.

Keywords: Information, methodology, security, risk, software

1. **Introducción**

En las organizaciones la información que se genera y se consume, se convierte en un factor relevante para la toma de decisiones. Por ello, para garantizar su efectividad, debe ser fiable, confidencial, integra y estar disponible en el momento indicado. La conservación de estas características, requiere del compromiso y gestión en todas las estructuras organizacionales, mediante la incorporación de estrategias de desempeño para la gestión de la calidad y seguridad de los datos [1]. La información, como activo no se cuantifica ni se refleja en los estados económico-financieros. No obstante, su incidencia en la creación de valor para la organización y el sistema económico es de vital importancia, al señalar su potencial en términos estratégicos y en la toma de decisiones para optimizar los recursos y generar competitividad[2].

Las organizaciones tienen riesgos asociados a su gestión, que son de diversos tipos y condiciones, incluyendo los generados a partir del uso de recursos informáticos. Este contexto presiona a la evaluación periódica de los procesos y las soluciones de tecnología para identificar, prevenir y controlar los riesgos de seguridad de la información. A partir de este contexto se diseñó una metodología, que evalúe la inclusión y calidad de los criterios de seguridad en los sistemas orientados a la gestión académica de las instituciones de educación superior[1][2]. El interés por las universidades, fue el resultado de la identificación de riesgos de seguridad de la información materializados en los procesos organizacionales y de la carencia en procesos de auditoría para su evaluación y detección de planes de mejora continua.

En el artículo "*Information Security Management in Academic Institutes of Pakistan*"[3], los autores referencian algunos estudios en donde se evidencia que en las universidades se ha ido creando ambientes propicios y atractivos para la ciberdelincuencia. Por su diversidad de usuarios, por el alto consumo de tecnología y por la combinación de esquemas de trabajo que están reunidos en un mismo escenario con enfoques orientados a la prestación de diversos servicios de tipo académico - administrativo[3]. Según investigaciones, las universidades han ocupado los primeros lugares entre las listas de los sectores más afectados por incidentes de seguridad informática, después del sector financiero y la industria farmacéutica[3].

El desarrollo de una metodología para auditar la seguridad de la información, se enfocó en implementar una guía sistemática qué, basada en las buenas prácticas que propone la norma ISO/27000 y en estándares internacionales como COBIT 5 e ITIL, facilite y motive la incorporación de procesos de autoría en las universidades; para identificar riesgos de seguridad de la información tempranamente y tomar acciones correctivas que sean oportunas[4][5]. Con esta propuesta, se da una alternativa para que las instituciones de educación superior incorporen una herramienta que apoye la gestión de la seguridad de la información a través, de un patrón metodológico aplicable, repetible, adaptable, flexible y medible. Al finalizar el desarrollo de la tesis, se obtuvo los componentes propuestos en el planteamiento inicial, los cuales serán abordados en cada sesión del artículo, de acuerdo con el proceso de desarrollo del trabajo de grado.

El artículo, se estructurará de la siguiente forma: En la sección 1: Se realizó la introducción; en la sección 2: Se define las dimensiones organizacionales que serán auditadas. En la sección 3: Se describe el diseño de la metodología, compuesto por 3 criterios, sobre los que se basará la evaluación. En la sesión 4: Se describirá los instrumentos de medición construidos para aplicar la metodología. En la sección 5, se detalla la estructura del programa de auditoria a aplicar. En la sesión 6: Se describirá la aplicación de la metodología, en la sesión 7: Se informa sobre los resultados obtenidos a partir de la aplicación. Para finalizar se emiten las conclusiones a partir del trabajo desarrollado.

2. DIMENSIONES

Son los escenarios organizacionales que fueron considerados relevantes durante el desarrollo de la tesis. Por la incidencia que tiene la seguridad de la información en su desempeño y por el impacto negativo que se podría reflejar para una institución de educación superior, sí llegaran a materializarse en incidentes de seguridad[1][5][6]. A continuación, se describe cada dimensión:

2.1 Gobierno universitario: Es el conjunto de políticas y lineamientos institucionales formales que adopta toda institución para orientar su desarrollo y crecimiento. Para la tesis, se consideró importante su evaluación, a partir de la iteración e incidencia que tiene en la adquisición, implementación y uso de los sistemas de información. El gobierno universitario tiene la misión de velar porque que se cumplan las leyes estatales, las políticas y los lineamientos institucionales; es responsabilidad de los funcionarios que lo integra generar procesos y procedimientos que estructuren organizacionalmente las instituciones[1]. En un ambiente organizacional es fundamental que los sistemas de información estén sincronizados con las decisiones estratégicas. La combinación de la gestión del gobierno universitario con los sistemas de información tiene relevancia en el alcance de los resultados en la gestión institucional; siendo herramientas para automatizar los procesos, respaldar la labor operacional y gestionar la información[1][5].

2.2 Sistemas de información: Su función principal es, ser el apoyo operacional que genera información estratégica y táctica a partir del registro y procesamiento de datos. Estas funcionalidades hacen que sean un factor determinante en una auditoría asociada a la gestión y seguridad de la información, al ser herramientas tecnológicas que han ido cambiando la forma de gestión y operación en las organizaciones[7][8]. El aporte de los sistemas de información, se refleja en la automatización de los procesos y en suministrar información para la toma de decisiones fundamentadas en datos procesados y transformados a partir del desempeño de las organizaciones[8]. Los sistemas de información bien implementados y con un funcionamiento óptimo, brindan ventajas competitivas frente a otras entidades de su mismo entorno[1].

2.3 Mantenimiento y soporte: Esta dimensión representa las revisiones y actualizaciones permanentes que se realizan a las plataformas y a la infraestructura tecnológica. Para el desarrollo de la tesis, se consideró importante evaluar la calidad del mantenimiento y soporte asociado a los sistemas de información, las buenas prácticas y los controles implementados. El

propósito es identificar la efectividad que cumplen cada uno de los componentes requeridos para la gestión de la seguridad de la información y la mitigación del riesgo informático.

3. DISEÑO DE LA METODOLOGÍA

El diseño, se basó en literatura conceptual estudiada en libros, artículos y normas; especialmente se destacan los siguientes: "Isaca, *A Business Framework for the Governance and Management of Enterprise IT*"[5], "Fundamentos del Gobierno de TI basados en ISO/IEC 38500[6], "*CERT C Programming Language Secure Coding Standard Document No . N1255*"[9], "*Tracing known security vulnerabilities in software repositories - A Semantic Web enabled modeling approach*"[10], "Norma técnica ntc-iso-iec colombiana 27001 2013-12-11"[4], "Norma Técnica Colombiana NTC - ISO 31000, Gestión del Riesgo Principios y Directrices"[11].

3.1 Criterios de seguridad para evaluar las dimensiones establecidas

Se definieron tres criterios con el objetivo de emitir un concepto técnico de la situación de seguridad de la información, a partir de los hallazgos que se identifiquen en la auditoria. Cada criterio está compuesto por una lista de controles de seguridad de la información, según las recomendaciones de la norma ISO – 27000 para aplicar una auditaría en este campo[4]. A continuación, se describe cada criterio.

3.1.1 Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión universitaria

Su objetivo es verificar la implementación de controles de seguridad efectivos y coherentes con el desempeño de la institución. La lista de controles se definió a partir de la propuesta que hace la Norma Técnica Colombiana ISO 27000 y el marco de referencia COBIT 5 de ISACA [4][5]. Estas entidades determinan que, para auditar la gestión y apropiación del gobierno universitario, es necesario evaluar el entorno institucional desde la legislación, las políticas, la estructura organizacional, la disponibilidad de recursos, la cultura, la ética y el comportamiento.

3.1.2 Calidad de los criterios de seguridad de la información en ambientes en producción

Su definición, se da a partir de las buenas prácticas que recomiendan entidades como: ISO[12], ISACA[5], OPWAS[10] y NITS[13], para la gestión y evaluación de los criterios de seguridad en sistema de información. Según estas instituciones, se requiere evaluar: Manejo de errores y de eventos de registro, tratamiento de usuarios y contraseñas de acceso, políticas y técnicas de autenticación, administración de sesiones de trabajo, transporte de datos, gestión de cambios, gestión de la capacidad, segregación de los ambientes de desarrollo en pruebas y producción, protección contra código malicioso, controles criptográficos, gestión de las vulnerabilidades, técnicas y gestión anti robo de información.

3.1.3 Calidad de los criterios de seguridad en el soporte y mantenimiento

El objetivo de este criterio es determinar la calidad, eficiencia y coherencia del soporte y mantenimiento tecnológico que las instituciones realizan a los sistemas información, a través de sus dependencias de tecnología o por la contratación de terceros que son proveedores de este tipo de servicios. Los controles recomendados por la norma ISO 27002[4], para una adecuada gestión de la seguridad de la información en el soporte y mantenimiento de los sistemas de información son: Gestión de activos, clasificación de la información, gestión de la prestación de servicios de proveedores, seguridad en los equipos de procesamiento de activos de información, control operacional del software, gestión de copias de respaldo, gestión de las comunicaciones, seguridad de las redes.

3.2 Estructura de la metodológica

Las dimensiones organizacionales, el diseño de los criterios y la lista de controles para la aplicación de la metodología propuesta, representan la figura 1 y se convierte en la estructura gráfica de la metodología. Su objetivo será ser la guía durante la aplicación del programa de auditoría.

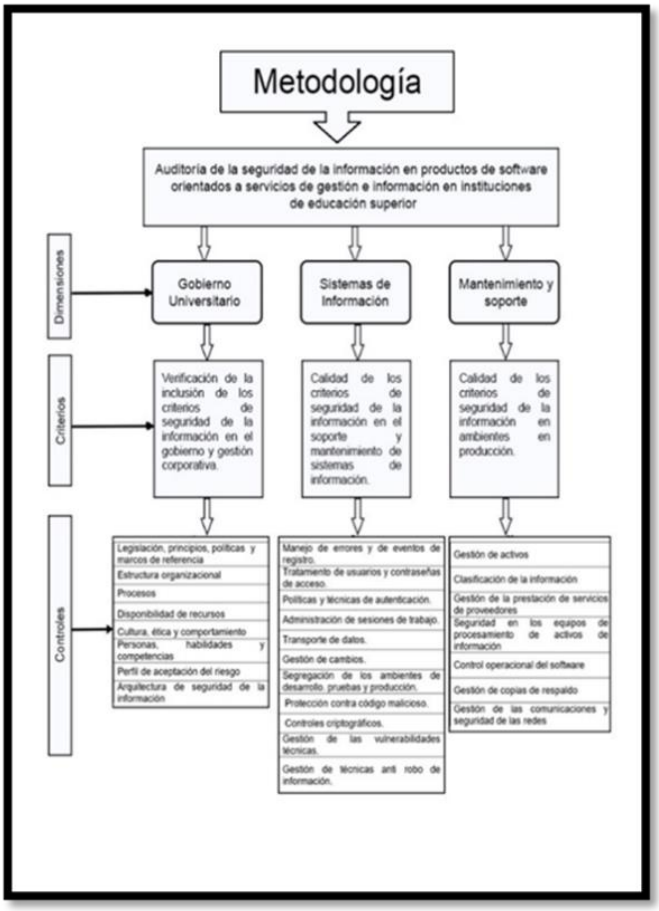

Figura 1. Estructura Metodológica

4. DISEÑO DE LOS INSTRUMENTOS

Los instrumentos, corresponden a un cuestionario y una matriz para el análisis de riesgos y la identificación de hallazgos por la ausencia de controles de seguridad de la información. Durante el programa de auditoria, se aplicarán para obtener un diagnóstico de las dimensiones evaluadas a través de los criterios de seguridad establecidos.

4.1 Cuestionario

Elaborado para medir la apropiación del gobierno universitario en la adopción y aplicación de prácticas adecuadas en la gestión de la seguridad de la información. Se diseñó un conjunto de preguntas dirigidas a diagnosticar el grado de conocimiento de quienes gestionan el gobierno universitario y su involucramiento en la aplicación de controles de seguridad de la información y la mitigación del riesgo informático.

Para su evaluación, se definió una escala que asegure una interpretación coherente de los datos capturados durante la inspección. El objetivo es encontrar un equilibro que permita determinar de forma responsable la existencia de controles de seguridad y su efectividad en la gestión del gobierno universitario. Los resultados se obtendrán a través de respuestas emitidas por en entrevistado; las cuales se ubicaran en una escala de Likert[1], las opciones se cuantificarán del 1 al 4, según la valoración definida. Al terminar la aplicación del instrumento, se hallarán los resultados por procedimiento aritmético y serán traducidos a intervalos de porcentaje que mostrarán el grado de cumplimiento del criterio evaluado como se ilustra en la tabla 1.

Tabla 1. Criterios para evaluación del cuestionario

Escala de Likert	Nivel de calificación	Interpretación	Rango de ubicación
1	No alcanzado	No está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro.	0 y 25%
2	Parcialmente alcanzado	Alcanza su propósito, Está implementado.	>25 y 50%
3	Ampliamente alcanzado	Implementado de forma gestionada (planificado, supervisado y ajustado). Los resultados de su ejecución están establecidos, controlados y mantenidos apropiados.	>50 y 75%
4	Completamente alcanzado	Implementado usando un proceso definido, que es capaz de alcanzar sus resultados de proceso.	>75 y 100%

[1] Escala de Likert: También denominada método de evaluaciones sumarias, es la más utilizada para la aplicación de encuestas.

4.2 Matriz para el análisis de riesgos

La matriz se diseñó cómo un instrumento que identificará la calidad e inclusión de los criterios de seguridad a través del hallazgo de vulnerabilidades y amenazas, para determinar su probabilidad de ocurrencia e impacto sobre los procesos de valor. El instrumento será aplicado al software de gestión que está orientado a la prestación de servicios académicos y al soporte y mantenimiento tecnológico realizado a cada producto. Para la valoración es necesario realizar una clasificación previa que, defina la criticidad del servicio que presta cada sistema de información, con el objetivo de hallar la magnitud del daño en un escenario en donde una probabilidad se convierta en ocurrencia.

La escala de medición, se diseñó a través de una matriz de 4 x 4, con una posibilidad máxima de un valor de 16, que representa el mayor nivel de riesgo posible. A medida que disminuye el número, representa un nivel de riesgo menor, hasta llegar a un valor óptimo de 1. Dependiendo de los valores de la probabilidad de amenaza y la magnitud de daño, la matriz calcula por procedimiento aritmético el producto de dos variables y visualiza el grado de riesgo. El método de análisis de riesgo se calculará por la fórmula: Riesgo = (probabilidad de amenaza x magnitud de daño). El riesgo se clasificará en bajo, medio o alto, según el resultado obtenido. Los resultados, permitirán determinar el nivel de riesgo alcanzado por la institución.

Tabla 2. La probabilidad de amenaza estará representada por la escala

1	Insignificante
2	Baja
3	Media
4	Alta

Tabla 3. La magnitud de daño, se verá reflejada en la escala

1	Insignificante
2	Baja
3	Media
4	Alta

Tabla 4. Clasificación del riesgo

Color	Categoría	Mínimo	Máximo
Gris Claro	Bajo	1	2
Gris Oscuro	Medio	3	6
Negro	Alto	8	16

La matriz está diseñada para ser aplicada por un experto técnico en seguridad de la información. Los valores de probabilidad de amenaza y magnitud del daño deben ser asignados después de observar el escenario a auditar y la verificación de evidencias. El resultado, corresponde a los datos generados, para emitir un concepto técnico del nivel de riesgo al que están expuestos los activos de información, ante la posibilidad de sufrir un daño significativo, causado por una amenaza o vulnerabilidad.

5. ESTRUCTURA PROGRAMA DE AUDITORÍA

El alcance de la metodología está estructurado para desarrollar un programa de auditoria interna. Es decir, libre de cumplir con responsabilidades para procesos de certificación, resolver conflictos de interés o dar cumplimiento a solicitudes legales.

La aplicación, se regirá por los principios y generalidades establecidos dentro de la Norma Internacional ISO 19011[14], caracterizándose por ser una herramienta fiable y eficaz para apoyar las políticas y controles de gestión. Su principio rector, siempre será emitir información veraz, para apoyar la toma de decisiones en el mejoramiento del desempeño institucional. Los principios se convierten en los elementos por los cuales se proporciona conclusiones suficientes y pertinentes sobre la auditoría realizada, de forma objetiva e imparcial[14][7].

5.1 Planeación del programa de auditoria

Corresponde a las actividades que se organizan con anterioridad al desarrollo de la auditoria, para garantizar y asignar las responsabilidades, la disponibilidad de los recursos y las condiciones necesarias para el desarrollo del programa. Las principales actividades son:

- Responsabilidades que se asumirán.
- Roles de las personas que participaran.
- Procedimientos a aplicar desde la apertura del programa hasta el cierre.
- Protocolo de las actividades secuenciales a realizar durante la ejecución del programa.
- Recursos asignados para cumplir el programa.
- Riesgos a los que se enfrenta el equipo durante la ejecución del programa.

5.1 Implementación del programa

Son las actividades que se deberán desarrollar para cumplir con el objetivo de la auditoria.

- Reunión de apertura, todos los implicados en el programa.
- Presentación del equipo evaluador.
- Presentación del equipo evaluado.
- Registro de los asistentes.
- Informar los objetivos, el alcance, los procedimientos y actividades a realizar durante todo el programa.
- Informar la metodología del programa de auditoria.
- Informar el cronograma aprobado.
- Informar la norma, los procesos y recursos a auditar.
- Informar la forma como se solicitará y auditará la parte documental, los recursos, las entrevistas y verificaciones a realizar. El equipo auditor no podrá retirar ningún documento proporcionado durante la auditoria, solo tomar evidencias.
- Elaboración de informe.
- Reunión para presentación resultados e informe
- Cierre del programa de auditoria.

6. APLICACIÓN DE LA METODOLOGÍA

Se seleccionó una institución de educación superior para aplicar los instrumentos en las dimensiones establecidas, utilizando los criterios de seguridad diseñados. El objetivo estuvo enfocado a la utilización de la guía metodológica para recopilar la información necesaria durante el desarrollo del programa de auditoria y realizar el análisis para obtener información cuantitativa y cualitativa, según los hallazgos identificados.

la metodología se convierte en una guía para determinar el estado de la institución con relación a la gestión de la seguridad de la información; basándose en el cumplimiento de la legislación, en las políticas establecidas, en la implementación de controles de seguridad y en el análisis de riesgos.

6.1 Componentes del programa de auditoria para la institución de educación superior seleccionada

Son los factores identificados como necesarios para desarrollar la auditoria. Cada factor fue elegido de acuerdo con la estructura de la metodología diseñada. El propósito es demostrar su aplicación para determinar la inclusión de los criterios de seguridad de la información en la gestión que ejerce la institución en la prestación de servicios académicos.

Tabla 5. Componentes del programa de auditoria

Criterios de seguridad de la información	Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión universitaria			
	Calidad de los criterios de seguridad de la información en ambientes en producción			
	Calidad de los criterios de seguridad en el soporte y mantenimiento			
Macro-procesos intervenidos	Docencia y aprendizaje			
	Administración y finanzas			
Sistemas de información intervenidos	Gestión académica	Pagos en línea	Publicación de horarios	Medios audiovisuales
	Gestión financiera	Biblioteca	Prácticas empresariales	
Servicios tecnológicos	Gestión de activos de información	Gestión de infraestructura tecnológica y comunicaciones		Gestión de copias de respaldo
	Gestión de proveedores	Gestión de planes de continuidad		

6.2 Aplicación de instrumentos

6.2.1 Cuestionario

El propósito, es recopilar información para evaluar la apropiación del gobierno universitario en la adopción y aplicación de prácticas adecuadas. Su estructura está diseñada para medir los aspectos relevantes de la gestión del gobierno universitario con respecto a seguridad de la seguridad. El entrevistado, tendrá la opción de seleccionar una respuesta de la escala de Licket diseñada, según su criterio frente a la pregunta realizada.

- **Ficha técnica:** Contienen el resumen de la información requerida para la aplicación de los instrumentos, con base en la estructura de la institución seleccionada. Para cada institución es necesario construir la ficha técnica, a partir de sus condiciones organizaciones y sus procesos de desempeño.

Tabla 6. Ficha técnica cuestionario

Dimensión	Gobierno universitario
Criterio	Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión corporativa.
Controles	Estructura organizacional
	Legislación, principios, políticas y marcos de referencia
	Disponibilidad de recursos
	Procesos
	Cultura, ética y comportamiento
	Personas, habilidades y competencias
	Perfil de aceptación del riesgo
	Arquitectura de seguridad de la información
Método de recolección de datos	Cuestionario
Método de aplicación	Entrevista personal y aplicación de cuestionario en línea
Método para selección de la muestra	No probabilístico
Muestra	Funcionarios altamente involucrados en la gestión de los sistemas de información
Población objeto de medición (categorías)	Directivo
	Jefe
	Oficial de seguridad de la información
	Profesional
	Ingeniero de soporte técnico Sistemas de Información
	Líder Funcional – ERP Institucional
Herramienta para aplicación:	Google docs
Link de acceso al cuestionario	https://docs.google.com/forms/d/1hCv8NqqHvGnwgi3YGSzB-d9Orv6yQqLYFKgFCZLKb5U/
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

6.2.2 Matriz análisis de riesgos

Para la evaluación de los criterios 2 y 3, se elaboró una matriz cuyo objetivo fue, detectar las vulnerabilidades y amenazas a las que se encuentran expuestos los activos de información.

6.2.2.1 Calidad de los criterios de seguridad de la información en ambientes en producción

Con los datos recopilados, se halló la probabilidad de ocurrencia de los eventos y magnitud del daño.

- **Ficha técnica:** Describe los elementos que se consideraron necesarios para evaluar la seguridad en los sistemas de información seleccionados, en cumplimiento de la estructura metodológica.

Tabla 7. Ficha técnica matriz de riesgo - criterio 2

Dimensión	Sistemas de Información
Criterio	Calidad de los criterios de seguridad de la información en ambientes de producción.
Controles	Manejo de Errores y de eventos de registro
	Tratamiento de usuarios y contraseñas de acceso
	Políticas y técnicas de autenticación
	Transporte de Datos
	Administración de sesiones de trabajo
	Gestión de cambios
	Gestión de la capacidad
	Segregación de los ambientes de desarrollo. Pruebas, preproducción y producción
	Protección contra código malicioso
	Controles criptográficos
	Gestión de las vulnerabilidades técnicas
	Gestión de técnicas anti robo de información
Método de recolección de datos	Formato de matriz de riesgo
Método de aplicación	Entrevistas y criterio de experto en seguridad de la información
Método para selección de la muestra	No probabilístico
Muestra	Plataformas tecnológicas
Población objeto de medición (categorías)	Equipo administrador de la plataformas tecnológicas
	Oficial de seguridad de la Información
	Líder Funcional – ERP Institucional
	Ingeniero de Soporte Técnico Sistemas de Información
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

Muestra de activos de información: Para la aplicación y análisis, se seleccionó una muestra de las plataformas tecnológicas implementadas en la institución, las cuales fueron clasificadas por el nivel de criticidad del servicio académico que soporta y el impacto que tendría su indisponibilidad para los procesos de valor.

Tabla 8. Sistemas de información para evaluación

Tipo	Plataforma Tecnológica	Clasificación	Bases de Datos	Lenguaje de Desarrollo
Aplicaciones de Software	Sistema de Información para la Gestión Académica	Crítico	ORACLE	PL / SQL. JAVA
	Sistema de Gestión Financiera	Crítico	ORACLE	PL / SQL. JAVA
	Sistema de Pagos en Línea	Crítico	ORACLE	PL / SQL. JAVA
	Audiovisuales	Bajo	MYSQL	PHP
	Biblioteca	Medio	MYSQL	PHP
	Publicación de Horarios	Medio	MYSQL	PHP
	Prácticas Empresariales	Bajo	MYSQL	PHP

Criterios de seguridad para la valoración de activos de información: Se utiliza para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en un criterio de seguridad especifico, corresponde a la medida de perjuicio para la institución, si el activo se ve dañado por la falta de este criterio[15].

Tabla 9. Criterios de seguridad (tomado de la Metodología MAGERIT Versión 3)

D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de la información
A	Autenticidad

Valoración activos de información en función de la magnitud del daño: Se utilizó para elaborar una matriz guía de la magnitud del daño sobre la afectación de un activo, según la importancia de este y para el caso que una amenaza se materialice por ausencia o manejo inadecuado de uno o varios criterios de seguridad de la información. Esta guía, es referente durante la identificación y valoración de riesgos informáticos; no es de estricto cumplimiento, considerando que cada activo opera diferente, según el servicio académico que atiende y su criticidad[15].

Tabla 10. Escala de valoración de la magnitud del daño (elaborada a partir de la Metodología MAGERIT Versión 3.0)

Magnitud de Daño			Aplicación de Software	Criterios			
				D	I	C	A
1	Bajo	B	Sistema de Información para la Gestión Académica	C	C	C	C
2	Medio	M	Biblioteca	A	A	B	M
3	Alto	A	Sistema de Pagos en Línea	C	C	C	C
			Publicación de Horarios	B	M	M	M
4	Critico	C	Sistema de Gestión Financiera	C	C	C	C
			Audiovisuales	B	B	B	M
			Prácticas Empresariales	B	M	B	B

Valoración de los controles de seguridad en función de probabilidad de amenaza: Se utilizó para elaborar una matriz guía de la probabilidad de amenaza con base en el control evaluado, según la importancia de este en la operación e impacto en un activo de información, por ausencia o manejo inadecuado de uno o varios criterios de seguridad. Esta guía es un referente para la identificación y valoración de riesgos de informáticos; no es de estricto cumplimiento, considerando que cada control actúa según las condiciones de exposición al riesgo del activo, la relevancia del servicio académico y su criticidad[15].

Tabla 11. Escala de valoración en función de la probabilidad de amenaza (elaboración a partir de la Metodología MAGERIT Versión 3.0)

Probabilidad de Amenaza			Control	Criterios			
				D	I	C	A
1	Insignificante	I	Manejo de errores y de eventos de registro	A	A	A	A
2	Baja	B	Tratamiento de usuarios y contraseñas de acceso	A	A	A	A
3	Mediana	M	Políticas y técnicas de autenticación	A	A	M	A
4	Alta	A	Transporte de Datos	A	A	A	A
			Administración de sesiones de trabajo	B	M	M	M
			Gestión de cambios	I	B	I	B
			Gestión de la capacidad	A	M	M	I
			Segregación de los ambientes de desarrollo, pruebas, preproducción y producción	I	I	I	I
			Protección contra código malicioso	A	A	A	A
			Controles criptográficos	M	A	A	A
			Gestión de las vulnerabilidades técnicas	M	A	M	M
			Gestión de técnicas anti robo de información	A	A	M	M

6.2.2.2 Calidad de los criterios de seguridad en el soporte y mantenimiento

Ficha técnica: Se resume la información considerada relevante para desarrollar las actividades que son necesarias en la aplicación del instrumento y el análisis de resultados con base en los datos obtenidos.

Tabla 12. Ficha técnica matriz de riesgo - criterio 3

Dimensión	Mantenimiento y soporte
Criterio	Calidad de los criterios de seguridad en el soporte y mantenimiento
Controles	Estructura organizacional
	Clasificación de la información
	Gestión de la prestación de servicios de proveedores
	Seguridad en los equipos de procesamiento de activos de información
	Control operacional del software
	Gestión de copias de respaldo
	Gestión de las comunicaciones y seguridad de las redes
Método de recolección de datos	Formato de matriz de riesgo
Método de aplicación	Entrevistas y criterio de experto en seguridad de la información
Método para selección de la muestra	No probabilístico
Muestra	Plataformas tecnológicas
Población objeto de medición (categorías)	Equipo de soporte técnico plataformas de información e infraestructura tecnológica.
	Oficial de seguridad de la información
Fecha de aplicación	22 – 23 y 24 de noviembre de 2016

Muestra de servicios técnicos para evaluar: Se describe los principales servicios que se han considerado relevantes para atender la administración, mantenimiento y soporte técnico de los sistemas de información implementados para prestar servicios de tipo académico.

Tabla 13. Servicios tecnológicos para evaluación

Tipo	Servicio
Servicios Técnicos para plataformas tecnológicas	Gestión de activos de información
	Gestión de proveedores
	Gestión de la infraestructura y comunicaciones tecnológicas
	Gestión de planes de continuidad
	Gestión de copias de respaldo

Criterios de seguridad para la valoración de activos de información: Para la valoración se tuvo en cuenta los mismos criterios de seguridad de la matriz de evaluación del criterio uno, (tabla 10). Se utiliza para valorar las consecuencias de la materialización de una amenaza.

Valoración servicio tecnológico en función de la magnitud del daño: Corresponde a una matriz guía de la magnitud del daño sobre la afectación en la prestación de un servicio tecnológico, según la importancia de este y las consecuencias ante una amenaza que se materialice por ausencia o manejo inadecuado de uno o varios criterios de seguridad de la información. Esta guía, es un referente para la identificación y valoración de riesgos informáticos durante la evaluación de la matriz de seguridad[15].

Tabla 14. Valoración servicios tecnológicos en función de la magnitud del daño (tomada de la metodología MAGERIT versión 3.0)

Magnitud de Daño				Aplicación de Software	Criterios			
					D	I	C	A
1	Bajo	B		Gestión de proveedores	A	A	A	A
2	Medio	M		Gestión de la infraestructura y comunicaciones tecnológicas	C	C	C	C
3	Alto	A		Gestión de planes de continuidad	C	A	A	A
4	Critico	C		Gestión de copias de respaldo	A	C	C	C

- **Valoración controles de seguridad en función de la probabilidad de amenaza:** Se utilizará para elaborar una matriz guía de la probabilidad de amenaza con base en el control evaluado, según la importancia de este en la operación e impacto en un activo de información, por ausencia o manejo inadecuado de uno o varios criterios de seguridad. Esta guía es un referente para la identificación y valoración de riesgos de informáticos; no es de estricto cumplimiento, considerando que cada control actúa según las condiciones de exposición al riesgo, la relevancia del servicio académico y su criticidad[15].

Tabla 15. Valoración controles de seguridad en función de la probabilidad de amenaza (tomada de la Metodología MAGERIT Versión 3.0)

Probabilidad de Amenaza			Control	Criterios			
				D	I	C	A
1	Insignificante	I	Gestión de activos de información	A	A	A	M
2	Baja	B	Gestión de proveedores	A	A	A	A
3	Mediana	M	Gestión de la prestación de servicios de proveedores	A	A	A	M
4	Alta	A	Gestión de la infraestructura, redes y comunicaciones tecnológicas	A	A	A	A
			Gestión de planes de continuidad	A	A	A	M
			Gestión de copias de respaldo	A	A	A	A

7. RESULTADOS DE LA APLICACIÓN

A continuación, se presentará los resultados obtenidos a partir de la aplicación de los tres instrumentos de medición y la evaluación de cada criterio de seguridad de la información diseñados dentro de la metodología propuesta.

7.1 Verificación de la inclusión de los criterios de seguridad de la información en el gobierno y gestión universitaria.

Tabla 16. Resultados aplicación del instrumento uno (cuestionario)

Control	Valoración	Rango
Legislación, principios, políticas y marcos de referencia	No alcanzado	>0% - 25%
Estructura organizacional	Parcialmente alcanzado	>25% - 50%
Disponibilidad de recursos	No alcanzado	>0% - 25%
Procesos	No alcanzado	>0% - 25%
Cultura, ética y comportamiento	No alcanzado	>0% - 25%
Personas, habilidades y competencias	No alcanzado	>0% - 25%
Arquitectura de seguridad de la información	No alcanzado	>0% - 25%

En la tabla 16, se visualiza el consolidado de la evaluación obtenida en cada uno de los controles de seguridad de la información, según las respuestas emitidas por los entrevistados durante la aplicación del instrumento. Los resultados muestran que el 87,5% de los controles de seguridad

de la información auditados se ubican en un rango de 0 a 25%; indicando qué, los controles de seguridad no están implementados o no alcanzan su propósito.

7.2 Calidad de los criterios de seguridad de la información en ambientes en producción

A continuación, se describirán los resultados de la aplicación del instrumento 2 (matriz de riesgo). Los hallazgos ubicados entre el umbral de riesgo alto, serán considerados como el apetito de riesgos; es decir, el riesgo con el que se está dispuesto a convivir en las en las operaciones normales diarias. Todo riesgo en el umbral medio, será interpretado como tolerancia al riesgo; es decir, el nivel aceptable del riesgo. Todo riesgo en el umbral bajo, se considerará como la capacidad de riesgo; es decir, el riesgo que la institución puede aceptar. La intensidad de color, representa el nivel del riesgo (RN) hallado. En la franja negra se ubica el riesgo alto. En la franja gris oscuro: riesgo medio y en la franja gris claro: nivel de riesgo bajo. Los controles auditados están representados por la letra C y el consecutivo de cada control, según fueron definidos en la metodología propuesta.

Sistemas de Información	C1		C2		C3		C4		C5		C6		C7		C8		C9		C10		C11		C12	
	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%	NR	%
Gestión Académica		88		100		100		100		100		100		100		100		100		100		100		100
Biblioteca		50		54		78		60		63		67		60		50		78		100		91		50
Pagos en Línea		88		100		100		100		100		100		100		100		100		100		100		100
Publicación de Honorarios		50		54		78		60		63		67		60		50		66		100		91		50
Gestión Financiera		88		100		100		100		100		100		100		100		100		100		100		100
Audiovisuales		81		100		89		100		100		78		100		63		78		57		91		83
Prácticas Empresariales		81		100		89		100		100		78		100		63		78		57		91		83

Figura 2. Resultado nivel de riesgo alcanzado

En la figura 2, se expone el resultado del nivel de riesgo alcanzado con base en la aplicación del instrumento, que consistió en obtener información de cada plataforma tecnológica. Con la información que se recopiló, se procedió a valorar los elementos de cada control, de acuerdo a las variables y componentes de medición definidos. Previamente se asignó el valor de magnitud de daño a cada plataforma tecnológica, según el servicio que presta, criticidad de operación y e impacto que tendría para la institución su indisponibilidad o daño.

Tabla 17. Clasificación riesgos de seguridad

Plataforma Tecnológica	Zona de clasificación del riesgo	Impacto procesos de valor
Gestión académica		SI
Biblioteca		NO
Pagos en línea		SI
Publicación de honorarios		NO
Gestión financiera		SI
Audiovisuales		NO
Prácticas empresariales		NO

En la tabla 17, se visualiza la clasificación del riesgo alcanzada para cada plataforma evaluada; conforme en la valoración realizada. La tabla muestra que 3 de las 7 plataformas obtuvieron una calificación de riesgo alta. Se recomienda intervención inmediata para implementar planes de mejora, que sean abordados y gestionados desde los diversos niveles jerárquicos de la institución, como: gobierno universitario, dirección de TI, administradores de operación y soporte de las plataformas tecnológicas, usuarios responsables del tratamiento los activos y la emisión de información; para detectar, proponer e implementar planes estructurados y disponibilidad de recursos.

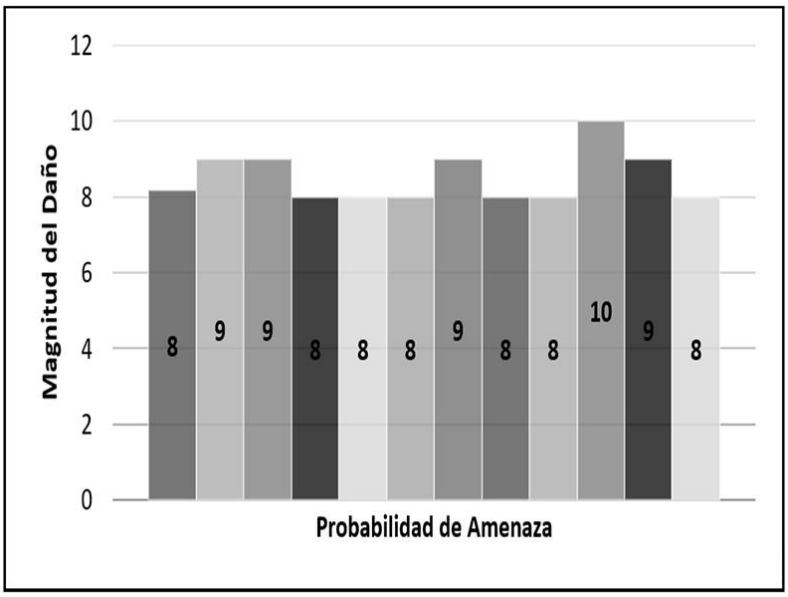

Figura 3. Promedio de riesgo criterio 2

La figura 3, visualiza la evaluación cuantitativa de cada control de seguridad de la información, proyectando un escenario para la institución en situación de riesgo alto. La probabilidad de amenaza es alta y ante la materialización de un daño su impacto sería crítico. El resultado evidencia carencia en la gestión de la seguridad de la información, del riesgo informático y baja garantía de la inclusión y calidad de los criterios que definen la información como: fiable, confidencial, integra y disponible.

Análisis de riesgos

La evaluación de los controles de seguridad en los sistemas de información para la gestión académica, pagos en línea y gestión financiera; se ubicó en una valoración de riesgo alto. En el resultado se halló una situación de riesgo superior al 85%, teniendo como referencia la criticidad que representan las tres plataformas tecnológicas en la prestación de los servicios. Ante la posibilidad de materialización de la amenaza, la magnitud del daño es crítica para la institución e impactaría los procesos de valor.

En las plataformas tecnológicas: Biblioteca y publicación de horarios, al igual que en los sistemas descritos anteriormente, se identificó ausencia de los elementos considerados relevantes, para preservar las condiciones de seguridad. Sin embargo, estos sistemas están clasificados dentro de la criticidad de operación y servicio en un nivel medio. El umbral de riesgo, se ubicó entre los valores 3 y 16 de acuerdo con la valoración asignada para cada componente, con tendencia a ubicarse en una clasificación de riesgo alto, al obtener en la evaluación un porcentaje entre el 50% y el 100% (tabla 17). La indisponibilidad de las plataformas o daño, no impactaría los procesos de valor. No obstante, si la calidad del servicio al afectar toda la población institucional.

Las plataformas tecnológicas: Audiovisuales y prácticas empresariales están clasificadas en criticidad del servicio baja. La probabilidad de amenaza es media y la magnitud del daño mediana. A pesar de ser soluciones tecnológicas clasificadas en el nivel más bajo del servicio; se identificó ausencia de los controles evaluados. La indisponibilidad del servicio afectaría a un grupo minoritario en comparación con el total de la población, sin posibilidad de impactar los procesos de valor y con una afectación del servicio baja.

7.2 Calidad de los criterios de seguridad en el soporte y mantenimiento

A continuación, se presenta la evaluación de la aplicación del instrumento 3, a través del instrumento matriz de riesgo. Los hallazgos entre el umbral de riesgo alto, serán considerados como el apetito de riesgo, es decir, el riesgo con el que se está dispuesto a convivir en las operaciones normales diarias. Todo riesgo en el umbral medio, será interpretado como tolerancia al riesgo, es decir, el nivel aceptable del riesgo. Todo riesgo en el umbral bajo, se considerará como la capacidad de riesgo, es decir, el riesgo que la institución puede aceptar.

Servicio Tecnológico	C1		C2		C3	C4		C5	C6		C7	
	NR	%	NR	%	NR	NR	%	NR	NR	%	NR	%
Gestión de activos de información		83		60			80			60		83
Gestión de proveedores		83		60			80			60		83
Gestión de la Infraestructura y Comunicaciones Tecnológicas		100		100			55			100		83
Gestión de planes de continuidad		83		60			80			60		83
Gestión de copias de respaldo		100		100			55			100		83

Figura 4. Nivel de riesgo por servicios tecnológicos

La figura 4, muestra los resultados del nivel de riesgo alcanzado, con base en la aplicación del instrumento 3. Consistió en obtener información de cada servicio tecnológico durante la entrevista con funcionarios del área de TI responsables del soporte técnico y mantenimiento, y la verificación de evidencias. Con la información que se recopiló, se procedió a valorar los elementos de cada control, de acuerdo a las variables y componentes de medición definidos. Previamente se asignó el valor de magnitud de daño a cada servicio, su criticidad e impacto que tendría para la institución su indisponibilidad o daño.

Tabla 18. Clasificación del riesgo servicios tecnológicos

Plataforma Tecnológica	Zona de clasificación del riesgo	Impacto procesos de valor
Gestión de activos de información		SI
Gestión de proveedores		SI
Gestión de infraestructura y comunicaciones tecnológicas		SI
Gestión de planes de continuidad		SI
Gestión de copias de respaldo		SI

En la tabla 18, se visualiza la clasificación del riesgo alcanzada para los servicios evaluados. La tabla muestra que en el 100% se obtuvo una calificación de riesgo alta. Situación crítica en la prestación del servicio tecnológico; ante la materialización de un incidente de seguridad se impactaría la totalidad de los procesos de valor de la institución y en general la prestación de los servicios de tipo académico y administrativo.

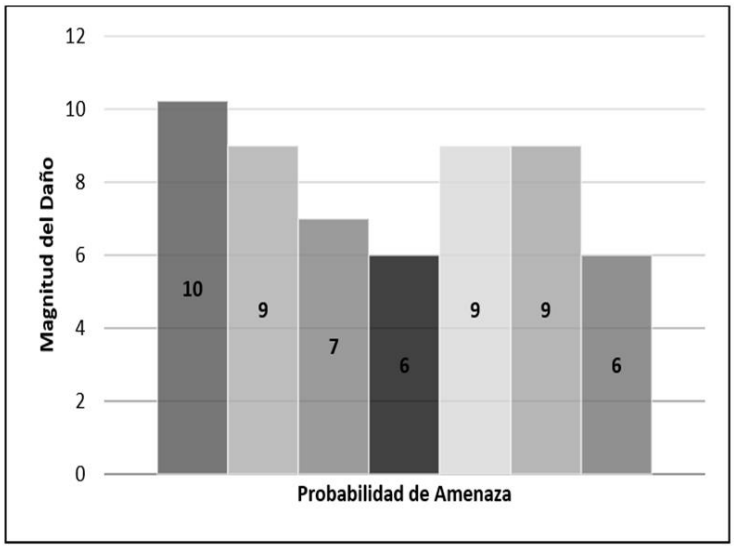

Figura 5. Promedio de riesgo criterio 2

La figura 5, visualiza la evaluación cuantitativa de cada control evaluado, proyectando un escenario para la institución en situación de riesgo alto al ubicarse en un rango superior a 6. La probabilidad de amenaza es alta y ante la materialización de un daño su impacto sería crítico y afectaría todas las plataformas tecnológicas evaluadas.

Análisis de riesgos

Con base en los resultados de la matriz de riesgo, los servicios tecnológicos se ubican en una zona de riesgo alta. Se recomienda su intervención desde la implementación de políticas, lineamientos y normalización de procesos. Se detecta qué, a pesar que la institución hace inversiones importantes en recursos tecnológicos, mantiene una situación de informalidad en la adopción de prácticas de gestión de seguridad. Los servicios evaluados, afectan positivamente o negativamente el desempeño de los sistemas de información y de los servicios institucionales.

Hallazgos generales identificados durante la aplicación de la metodología

- Las condiciones de riesgos fueron obtenidas en su totalidad mediante la auditoria en seguridad de la información en productos de software orientadas a servicios de gestión académica e información en instituciones de educación superior. Al analizar el conjunto de la evaluación los resultados arrojan un eminente hallazgo de riesgo alto sobre sus activos de información.

- Los principales hallazgos negativos, se dan por falta de políticas, procesos, procedimientos y documentación insuficiente; es decir por ausencia de formalización de las actividades, que denota una brecha entre el gobierno universitario y la gestión tecnológica; poniendo de manifiesto la carencia de controles de seguridad en la gestión de la información.

- La organización no tiene cultura de auditar los procesos estratégicos ni operacionales de las tecnologías de información y comunicación. Si bien existe un departamento de control interno; su ejercicio se enfoca a los procesos financieros y contables. Dentro de su planta de personal, no tiene funcionarios formados ni capacitados para realizar auditorías internas en la operación de la estructura gerencial y operativa del departamento de TI.

- No existen métricas definidas para medir la operación y el desempeño de la dependencia de TI. Se han adquirido herramientas, no obstante, no se han definido las estratégicas de utilización, la funcionalidad y las métricas para evaluar el desempeño y apoyar la toma de decisiones de tipo estratégico, gerencial, funcional y operacional.

- Los funcionarios dedicados a la administración, operación, mantenimiento y soporte de las tecnologías de información y comunicación, no realizan actividades de I+D; hecho que hace que las soluciones para la institución sean aportadas en alto porcentaje por los proveedores; sin verificación robusta que cumple con la necesidad de la institución.

- El Área de Seguridad de la Información, está conformada por un profesional y es relativamente nueva, situación que aporta para que la calificación de la seguridad de la información institucional se determine en un nivel de inmadurez y para que los controles de seguridad no estén definidos.

- Se concluye que la institución no tiene implementado un sistema de gestión de seguridad de la información; realiza una serie de actividades de seguridad descentralizadas e individuales que no pueden ser consideradas un sistema, al no estar integradas, articuladas y no funcionar como un todo en la búsqueda de un beneficio común.

8 CONCLUSIONES

El desarrollo de la tesis, fue el resultado de la materialización de una necesidad identificada, relacionada con riesgos y la falta de procesos de auditoría de seguridad de la información en instituciones de educación superior. La propuesta desde su planteamiento estuvo enfocada en aportar al sector de la educación superior un patrón de buenas prácticas a través de un diseño metodológico; que facilite y motive los procesos de auditoría para verificar la calidad e inclusión de los criterios de seguridad de la información.

Desarrollar un esquema que apoye la detección de los riesgos de seguridad mitiga la posibilidad que las organizaciones sean víctimas de ataques informáticos. El objetivo es brindar un apoyo a la estabilidad corporativa y al cumplimiento de sus objetivos de valor. Por ello es necesario que continuamente se trabaje en concientizar y culturizar a los funcionarios para convertir la gestión de la seguridad y prevención del riesgo en una cultura institucional.

Existen diversas propuestas metodológicas para realizar este proceso. Lo importante para las organizaciones es tomar conciencia de la importancia y el valor que tiene el adoptar un mecanismo que se ajuste al entorno y a su desempeño y que los métodos utilizados aporten para determinen la situación de seguridad y el riesgo en que se encuentran los activos de información, a partir de diagnósticos imparciales. La ventaja que ofrece la metodología propuesta, es el diseño de un esquema que estructura los elementos necesarios para auditar la seguridad de la información y emitir un concepto técnico, basado en una metodología que permita una medición cuantitativa y cualitativa de los datos obtenidos.

El diseño de la metodología se desarrolló pensado en un esquema flexible, repetible e innovador; que, responsada a las necesidades de las instituciones de educación superior, según sus modelos organizacionales y sus requerimientos. La estructura metodológica permite que la aplicación se realice de forma completa o parcial; bien sea para evaluar todos los escenarios, criterios y controles o cada uno de ellos de forma descentralizada, según la disponibilidad de recursos y necesidades de las instituciones.

La metodología propuesta es susceptible a mejoras, a través de otras líneas de investigación con enfoque en la prevención del riesgo informático desde la implementación de controles de seguridad de la información en las diversas etapas de desarrollo de software.

9 AGRADECIMIENTOS

A Dios, que inspira mi vida y patrocina el emprendimiento de cada proyecto, asegurándose de proporcionar los elementos necesarios para culminarlos con éxito.

A mis padres, por ser mi orientación y por la constancia en amor infinito, bondad, respeto y generosidad. A mis hermanos y mis sobrinos, por su inmenso amor y ejemplo. Son la razón para esforzarme a ser mejor persona cada día.

A mi Director Reinaldo Mayol Arnao, por su valiosa y acertada orientación; por su tiempo, dedicación y paciencia; por sus notables aportes, comentarios, correcciones y sugerencias, que fueron un pilar fundamental para el desarrollo mi tesis.

A la Universidad Pontificia Bolivariana seccional Bucaramanga, que ha sido mi segundo hogar y centro de crecimiento personal y profesional, mi eterno agradecimiento por acogerme en la gran familia Bolivariana. El apoyo de sus directivos ha sido determinante para alcanzar mí éxito profesional.

A mi equipo de trabajo del CTIC, compañeros permanentes de construcción con aciertos y desaciertos. Han sido guía y aprendizaje durante estos años de trabajo, motivando siempre mi formación y aprendizaje.

10 REFERENCIAS

[1] REDCLARA; TICAL, “Las Tecnologías de la Información y la Comunicación potenciado la Universidad del Siglo XXI,” 2015.

[2] H. S. B. Herath and T. C. Herath, “IT security auditing: A performance evaluation decision model,” *Decis. Support Syst.*, vol. 57, no. 1, pp. 54–63, 2014.

[3] H. Rehman, A. Masood, and A. R. Cheema, “Information Security Management in academic institutes of Pakistan,” *2013 2nd Natl. Conf. Inf. Assur.*, pp. 47–51, 2013.

[4] N. T. Ntc-iso-iec, “Norma técnica ntc-iso-iec colombiana 27001 2013-12-11,” no. 571, 2013.

[5] Isaca, *A Business Framework for the Governance and Management of Enterprise IT*. 2013.

[6] H. Hamidovic, I. Researcher, and I. Sec, “Fundamentos del Gobierno de TI basados en ISO/IEC 38500,” no. November, 2015.

[7] C. Manuel, F. Sánchez, and P. Velthuis, *Modelo para el gobierno de las TIC basado en las normas ISO*. 2012.

[8] M. Piattini Velthuis, Mario; Del Peso Navarro, Emilio; Del Peso Ruiz, *Auditoría de Tecnologías y Sistemas de Información, Ra – Ma Editorial*. 2008.

[9] L. Notice, “CERT C Programming Language Secure Coding Standard Document No . N1255,” *Programming*, p. 480, 2007.

[10] S. S. Alqahtani, E. E. Eghan, and J. Rilling, “Tracing known security vulnerabilities in software repositories - A Semantic Web enabled modeling approach,” *Sci. Comput. Program.*, vol. 121, pp. 153–175, 2016.

[11] I. C. de N. T. y C.- (ICONTEC), *Norma Técnica Colombiana NTC - ISO 31000, Gestión del Riesgo Principios y Directrices*. 2011.

[12] ISACA, “State of Cybersecurity : Implications for 2015,” p. 22, 2015.

[13] Institution National Standards and Technology, “NITS.” [Online]. Available: http://www.nist.gov/.

[14] “Directrices para la auditoría de Sistemas de Gestión DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR,” *ISO*, 1901.

[15] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, “Taxonomy of Information Security Risk Assessment (ISRA),” *Comput. Secur.*, vol. 57, pp. 14–30, 2016.