EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES INFORMÁTICAS EN SISTEMAS ACADÉMICOS UNIVERSITARIOS, APLICANDO ISO 27000.

THREATS ASSESSMENT AND COMPUTER VULNERABILITY IN UNIVERSITY ACADEMIC SYSTEMS, APPLYING ISO 27000

(Entregado 19/08/2015 – Revisado 06/10/2015)

MARCO PUSDÁ CHULDE

Magíster en Evaluación y Auditoría de Sistemas Tecnológicos por Universidad de las Fuerzas Armadas – ESPE (2015). Magister en Administración de Negocios por la Universidad Técnica del Norte (2013). Ingeniero en Sistemas Computacionales por la Universidad Técnica del Norte (2003). Certificación Cobit 5.0 por APMG-Internacional (2015). Ingeniero Docente Ocasional TC por contrato en la Universidad Politécnica del Carchi.

DAISY IMBAQUINGO ESPARZA

Magíster en Evaluación y Auditoría de Sistemas Tecnológicos por Universidad de las Fuerzas Armadas – ESPE (2015). Ingeniera en Sistemas Informáticos y Computacionales por la Universidad Técnica del Norte (2007). Diplomado en Investigación y Dirección de Tesis por la Universidad Técnica del Norte (2009). Certificación Cobit 5.0 por APMG-Internacional (2015). Laboratorista de Informática de la Universidad Técnica del Norte- Facultad de Ingeniería en Ciencias Aplicadas.

Universidad Politécnica Estatal del Carchi – UPEC

Universidad Técnica del Norte - UTN

mrpusda@hotmail.com daysi30@hotmail.com

INFORMÁTICA

RESUMEN

La información es un recurso indispensable para el desarrollo de las organizaciones, en especial en las instituciones educativas de nivel superior como la Universidad Técnica del Norte, la misma es necesaria para ser competitivas, lograr objetivos, obtener ventajas, brindar buenos servicios. Con el avance del internet y dispositivos de conectividad, en la actualidad existen amenazas y vulnerabilidades que pueden ocasionar graves problemas a la seguridad de la información. El presente artículo se enfoca la determinación de amenazas y vulnerabilidades del módulo de gestión académica, utilizando controles del estándar ISO/IEC 27000, marco de gestión de la seguridad de la información, aplicable a cualquier tipo de organización. Siguiendo los controles recomendados por ISO 27002:2013, se utilizó la metodología para análisis y gestión de riesgos MAGERIT, que permite recomendar las medidas apropiadas adaptables para controlar todo tipo

de riesgos en seguridad informática. Para seguir las recomendaciones de la metodología se incorporó PILAR, software que considera diferentes campos de la seguridad como: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. Luego de un análisis de cumplimiento de la norma ISO/IEC 27002:2013 al módulo de gestión académica, se determinó que existen diversas debilidades relacionadas con la seguridad de la información: apoyo y concienciación de la dirección, el establecimiento de políticas, procedimientos y falta de personal cualificado.

PALABRAS CLAVE:

***ISO**: Organización Internacional de Normalización, **IEC:** International Electrotechnical Commission, **ISO/IEC 27000:** Conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, **MAGERIT:** Metodología de análisis y gestión de riesgos de los sistemas de información, **PILAR:** Software que utiliza la metodología MAGERIT.*

ABSTRACT

The information is an important aspect for the development of organizations, mainly for Universities as "Universidad Técnica del Norte", due to it lets to reach competitive advantages, goals and provide good services to customers.With the advancement of internet and connectivity devices, there are threats and vulnerabilities that can cause serious problems to the security of information. The present paper is focused on the determination of threats and vulnerabilities of academic management module, using the standard ISO / IEC 27000, which is part of the security management information that can be applied to any type of organization. Following the recommended controls for ISO 27002: 2013, it used the methodology for analysis and risk management MAGERIT that suggests the appropriate actions to control all kinds of informatics security risks. According with the methodology it was incorporated a software called PILAR, which takes into account different aspects of security, such as: confidentiality, integrity, availability, authenticity and traceability of information. After applying the standard ISO/IEC 27002:2013 to the academic management module, it determined the existence of several weaknesses related with the security of the information, which are evident in: support and awareness of management, establishing policy and procedures and lack of qualified staff.

KEYWORDS:

***ISO**: International Standarization Organization, **IEC**: International Electrotechnical Commission, **ISO/IEC 27000:** Set of standards that provide a framework for managing the security of information usable by any organization, **MAGERIT:** Risk Analysis and Management Methodogy for Information Systems, **PILAR:** Software that used the methodology MAGERIT.*

1. Introducción

En la actualidad, con la utilización de las tecnologías de información y comunicación (TIC), dentro de las de las universidades, el alto volumen de información de miles de estudiantes generada por el módulo de gestión académica del sistema integrado de la Universidad Técnica del Norte (UTN), y teniendo en cuenta que la tendencia tecnológica es permanecer interconectado las 24 horas del día y los 365 días del año, las universidades están expuestas a diversas vulnerabilidades y amenazas, lo que obliga a concientizar de la importancia de tener implantadas un conjunto de políticas de seguridad tendientes a garantizar la continuidad del negocio en caso de que se produzcan incidencias, fallas, actuaciones malintencionadas, pérdidas accidentales o desastres que afecten a los datos e información que son tratados por el módulo de gestión académica, dicha información es considerada como uno de los activos imprescindibles para poder brindar servicios educativos de calidad a la sociedad.

La Auditoría informática, está enfocada a la revisión y evaluación del cumplimiento de los controles y procedimientos, utilizados para la confidencialidad, integridad y disponibilidad de la información del sistema académico universitario integrado, verificando si los controles implementados son eficientes y suficientes, identificando las causas de los problemas existentes en el sistema académico y a su vez determinando las acciones preventivas y correctivas necesarias para mantener el módulo de gestión académica con todas sus aplicaciones confiables y disponibles. (Departamento Informática UTN, 2013)

En el departamento de desarrollo y transferencia tecnológica (DDTT) de la Universidad Técnica del Norte, la implementación de políticas y procedimientos de seguridad de la información en el módulo de gestión académica es muy baja. El personal que labora en esta dependencia ha venido trabajando con una seguridad relativamente empírica, aprendida en sus estudios universitarios y del conocimiento autónomo adquirido. Toda amenaza identificada contra el correcto funcionamiento del módulo de gestión académica y la consecución de sus objetivos, no se le da el correcto tratamiento ni la realización de un análisis minucioso de las causas y efectos.

Por lo antes expuesto, el DDTT de la UTN requiere de un conjunto de políticas, normas, procedimientos, reglas y buenas prácticas que garanticen plenamente la disponibilidad, integridad y confiabilidad de la información del módulo de gestión académica, los mismos deben cumplir con estándares internacionales. Los estándares destacados son ISO 27001:2013 e ISO 27002:2013, que ofrecen una guía de objetivos y controles que permiten gestionar de una manera adecuada y acorde con los objetivos institucionales. (ISO 27000, 2013)

Por tanto, el presente trabajo tiene como propósito identificar las vulnerabilidades y amenazas del módulo de gestión académica utilizando los controles y buenas prácticas que recomienda la norma ISO/IEC 27002:2013, tomando como referencia la metodología MAGERIT, la misma que permite analizar y gestionar los riesgos que soportan los sistemas de información a través de su herramienta PILAR, por medio del cual se logra una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. (CCN-CERT, 2013)

Materiales y métodos

1.1. Marco Teórico

Seguridad Informática: Consiste en la protección de la información que se encuentra en un computador o en una red y la protección de todos sus recursos de los sistemas de información. (SYBSEC S.A, 2012).

Vulnerabilidades: "Eventos de las Tecnologías de Información y Comunicación (TIC´s), que pueden desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos". (Piattini, 2010)

Amenazas: "Debilidad de un activo que puede ser explotada por una amenaza relacionada con las TIC´s, para materializar una agresión sobre dicho activo". (Echenique, 2012)

ISO 27002:2013: "Es el código de prácticas de seguridad de la información el cual tiene como objetivo proveer una guía para la implementación de controles para el Sistema de Gestión de Seguridad de la Información ISO 27001". (ISO 27002 ESPAÑOL, 2013)

Figura 1: Contenidos de la norma ISO 27002:2013

Fuente: (UNIT - Istituto Uruguayo de Normas Técnicas, 2014)

Según describe el sitio web http://iso27000.es/iso27002.html (2013). La versión de 2013 del estándar describe los dominios siguientes:

1. Políticas de seguridad: Estrategias, estructura, procesos, objetivos generales, políticas y requisitos.

2. Organización seguridad información: Administración de la seguridad de la información cumpliendo objetivos y actividades de la organización.

3. Seguridad ligada a los recursos humanos: Educar e informar al personal en forma continua sobre la seguridad y confidencialidad en sus funciones.

4. Gestión de Activos: Conocimiento de activos de la organización para la administración de riesgos.

5. Control de Accesos: Restricciones y excepciones a la información, procedimientos formales para controlar derechos de acceso.

6. Cifrado: Sistemas y técnicas criptográficas para proteger a la información.

7. Seguridad Física y Ambiental: Perímetros y áreas protegidas para minimizar riesgos de daños a la información y operaciones de la organización

8. Seguridad de las Operaciones: Procedimientos de operaciones, actualización documentación, registro de actividad y monitorización, protección contra malware, resguardo, control del software operativo, vulnerabilidades técnicas, coordinación de la auditoría de sistemas de información.

9. Seguridad de las comunicaciones: Gestión de la seguridad de redes telemáticas; gestión de las transferencias de información.

10. Adquisición, desarrollo y mantenimiento de los sistemas de información: Controles de seguridad y validación de datos, requisitos de seguridad de los sistemas de información, seguridad en los procesos de desarrollo y soporte, datos para pruebas.

11. Relaciones con suministradores: seguridad de la información en las relaciones con los proveedores; gestión de servicios contratados.

12. Gestión de incidentes: gestión de las incidencias que afectan a la seguridad de la información, comunicación oportuna de eventos para aplicar acciones correctivas en tiempo oportuno.

13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio: Análisis de consecuencias de desastres, planes para continuidad, redundancias, pruebas pertinentes.

14. Cumplimiento: Cumplimiento de las disposiciones legales y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Situación organizacional

El Departamento de Informática desarrolla sistemas de información con estudiantes de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales CISIC, dichos aplicativos se desarrollan de forma modular de acuerdo a las necesidades de la Universidad Técnica del Norte, razón por la cual tanto analistas como programadores de planta o tesistas diseñan e implementan utilizando plataformas ORACLE 11g, servidores Linux, y otras herramientas compatibles. (Departamento Informática UTN, 2013)

Tabla 1: Matriz ºFODA Departamento Informática UTN

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Personal con conocimiento y experiencia en temas informáticos y de soporte técnico.	El avance Tecnológico proporciona un abanico de posibilidades que pueden ser aplicadas en los procesos sistemáticos.	Escasos convenios y programas de capacitación al personal de esta unidad.	Situación económica del País, escaso presupuesto para la Adquisición de equipos de cómputo y Licencias de software.
Responsabilidad en el manejo de información.	Disponibilidad de encontrar en el mercado tecnologías de punta.	Ambientes reducidos y mal ubicados para la realización de las actividades.	Exigencia de los usuarios de una atención oportuna y segura de los servicios académicos
Iniciativa del personal informático en actualizarse en las nuevas tecnologías informáticas.	Interés creciente por parte de los funcionarios a asistir a cursos informáticos.	Falta de recursos económicos para disponer de una infraestructura informática acorde a las necesidades.	Constante amenazas de virus en la red.
Personal plenamente identificado con la Institución.	Existencia de centros de especialización	Cultura organizacional orientada a la innovación de procesos a través de la aplicación de tecnologías y comunicaciones	Falta de confidencialidad con respecto a las claves de acceso, por parte del personal que labora con los sistemas de información
Infraestructura de red de datos.	Creciente demanda por servicios informáticos relacionados a consultas masivas.	Sistema no acorde con nuevas herramientas de seguridad informática.	Rechazo por parte de los funcionarios a utilizar sistemas de información desconocidos.
Proyección de una imagen positiva y eficiente a nivel institucional.	Apoyo económico por parte de las Autoridades para realizar entrevistas y viajes con otras entidades líderes en tecnología y en adquisición de tecnología de punta.	Escases de equipos de respaldo para los servicios y aplicaciones del módulo de gestión académica.	Creciente demanda por servicios informáticos relacionados a consultas masivas.
UNIPORTAL UTN.	Necesidad de proporcionar a los usuarios mecanismos de participación a través de nuestro portal Web.	Personal administrativo recurrente a no utilizar los recursos tecnológicos disponibles	Retraso en la entrega de insumos y repuestos necesarios para las actividades.

Fuente: (Universidad Técnica del Norte, 2012)

Alineación a la norma ISO/IEC 27002:2013

En el presente trabajo se sustenta en la aplicación de la norma ISO/IEC 27002:2013, se tomó como referencia los dominios con los objetivos de control y controles que se relacionan con el módulo de gestión académica. (ISO 27000, 2013)

Tabla 2: Controles de la norma ISO 27002:2013

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Directrices de la dirección en seguridad de la información	Conjunto de políticas para la seguridad dela información
		Revisión de las políticas para la seguridad de la información
ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Organización interna	Asignación de responsabilidades para la seguridad de la información
		Segregación de tareas
		Contacto con las autoridades
		Contacto de interés especial
SEGURIDAD EN LOS RECURSOS HUMANOS	Antes de la contratación	Investigación de antecedentes
		Términos y condiciones de contratación
	Durante la contratación	Responsabilidades de gestión
		Concienciación, educación y capacitación en seguridad de la información
		Proceso Disciplinario
	Cese o cambio del puesto de trabajo	Cese o cambio de puesto de trabajo
GESTIÓN DE ACTIVOS	Responsabilidades sobre los activos	Inventario de activos
		Propiedad de los activos
		Devolución de activos
CONTROL DE ACCESOS	Requisitos del negocio para el control de accesos	Política de control de accesos
		Control de acceso a las redes y asociados
	Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios
		Gestión de los derechos de acceso asignados a usuarios
		Gestión de información confidencial de autentificación de usuarios
		Revisión de los derechos de acceso de los usuarios
	Responsabilidades del usuario	Uso de la información confidencial para la autentificación
	Control de acceso a sistemas y aplicaciones	Procedimientos seguros de inicio de sesión
		Gestión de contraseñas de usuario
		Control de acceso al código fuente
CIFRADO	Controles criptográficos	Políticas de uso de los controles criptográficos
		Gestión de claves

SEGURIDAD FÍSICA Y AMBIENTAL	Áreas seguras	Perímetro de seguridad física
		Controles físicos de entrada
		Protección contra las amenazas externas y ambientales
	Seguridad de los equipos	Emplazamiento y protección de equipos
		Instalaciones de suministro
		Seguridad del cableado
		Mantenimiento de los equipos
SEGURIDAD DE LAS OPERACIONES	Responsabilidades y procedimientos de operación.	Documentación de procedimientos de operación.
		Gestión de cambios.
		Gestión de capacidades.
		Separación de entornos de desarrollo, prueba y producción.
	Protección contra código malicioso	Controles contra el código malicioso.
	Copias de seguridad	Copias de seguridad de la información
	Registro de actividad y supervisión.	Registro y gestión de eventos de actividad
		Protección de los registros de información
	Control del software en explotación.	Instalación del software en sistemas en producción
	Gestión de la vulnerabilidad técnica.	Gestión de las vulnerabilidades técnicas.
		Gestión de las vulnerabilidades técnicas.
	Consideraciones de las auditorías de los sistemas de información.	Controles de auditoría de los sistemas de información
SEGURIDAD EN LAS TELECOMUNICACIONES	Gestión de seguridad en las Redes	Controles de red.
		Mecanismos de seguridad asociados a servicios de red
		Segregación de Red
ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMACIÓN	Requisitos de seguridad de los sistemas de información.	Análisis y especificación de los requisitos de seguridad.
	Seguridad en los procesos de desarrollo y soporte	Política de desarrollo de Software.
		Procedimiento de control de cambios en los sistemas
	Datos de Prueba	Protección de los Datos utilizados en pruebas
RELACIÓN CON SUMINISTRADORES	Seguridad de la información en la relación con suministradores.	Política de Seguridad de la Información para suministradores
	Gestión de la prestación de Servicios por suministradores	Supervisión y revisión de los servicios prestados por terceros

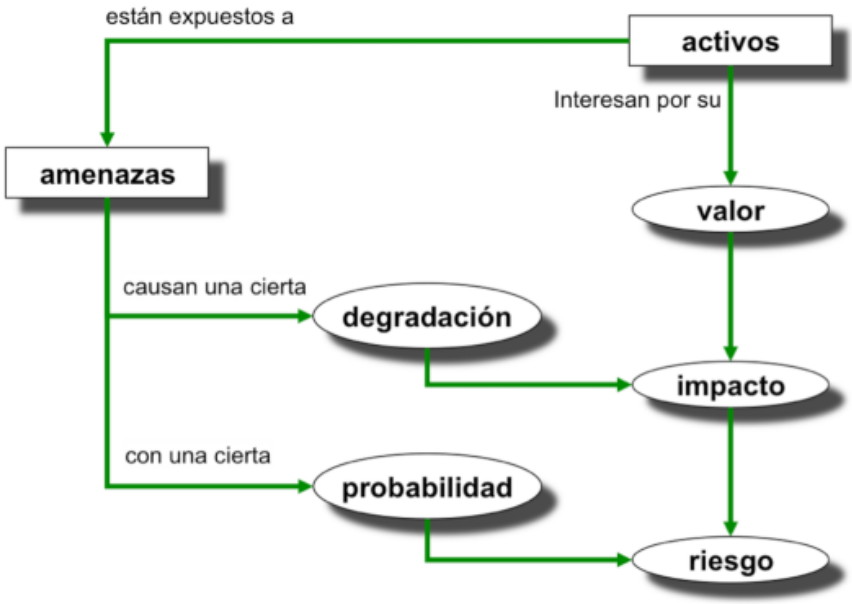
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Gestión de Incidentes de Seguridad de la información y mejoras	Responsabilidades y procedimientos
		Notificación de los eventos de seguridad de la Información.
		Respuesta a los incidentes de seguridad.
		Recopilación de evidencias
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información
	Redundancias	Disponibilidad de instalaciones para el procesamiento de la información
CUMPLIMIENTO	Cumplimiento de los requisitos legales y contractuales	Identificación de la Legislación aplicable
		Derechos de propiedad intelectual
		Protección de datos y privacidad de la información personal

Fuente: (ISO 27002 ESPAÑOL, 2013)

1.2. MAGERIT

Para determinar el estado actual de la gestión de riesgo en la seguridad de información relacionada con el módulo de gestión académica, se evaluó los activos más significativos que posee el departamento de informática de la Universidad Técnica del Norte.

Figura 2: Elementos del análisis de riesgos potenciales



Fuente: (CCN-CERT, 2013)

Para la ejecución de la metodología, la recopilación de la información se desarrolló mediante observación física, encuestas y entrevistas a los usuarios responsables del sistema de gestión académica de la Universidad Técnica del Norte.

Durante la aplicación de la metodología MAGERIT, se realizaron 5 pasos: Identificar los activos. Valoración de activos. Determinar las amenazas a las que se encuentran expuestos los activos identificados. Determinación del impacto. Determinación del riesgo. (CCN-CERT, 2013)

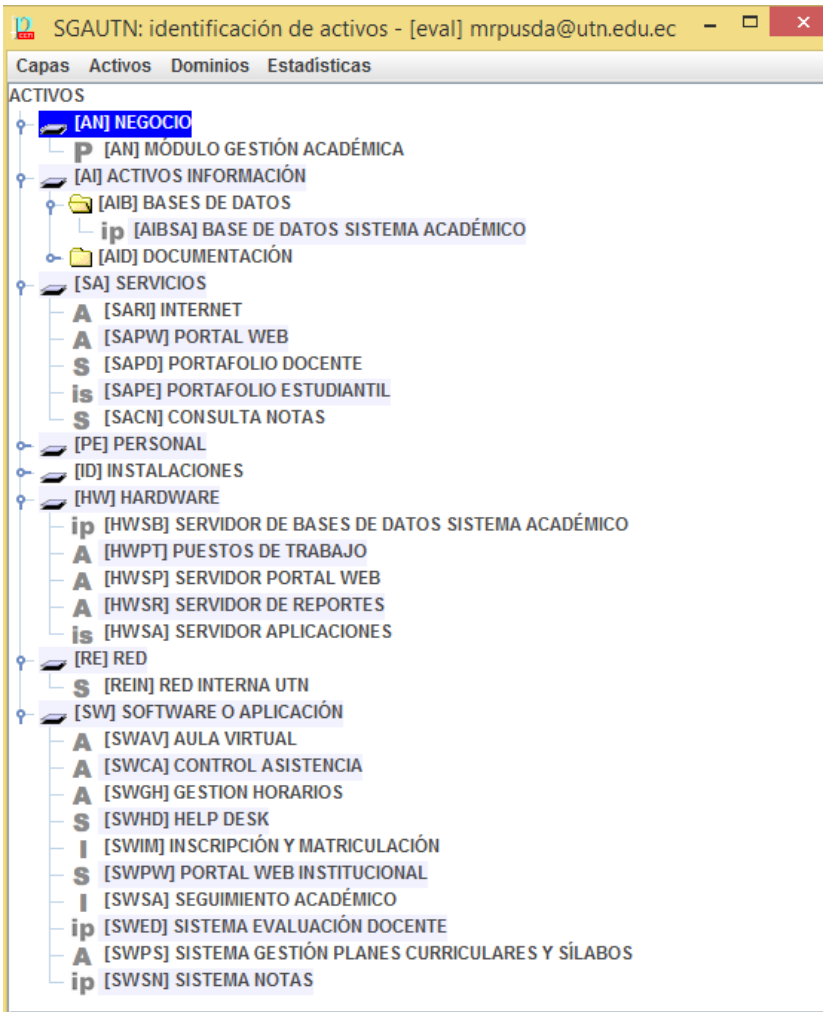
1.3. Pilar

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos". PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española. (PAE - Portal de Administración Electrónica, 2012).

Esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos, sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad: (EAR / PILAR, 2014)

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias o Salvaguardas.

Figura 3: Listado de Activos Módulo Gestión Académica



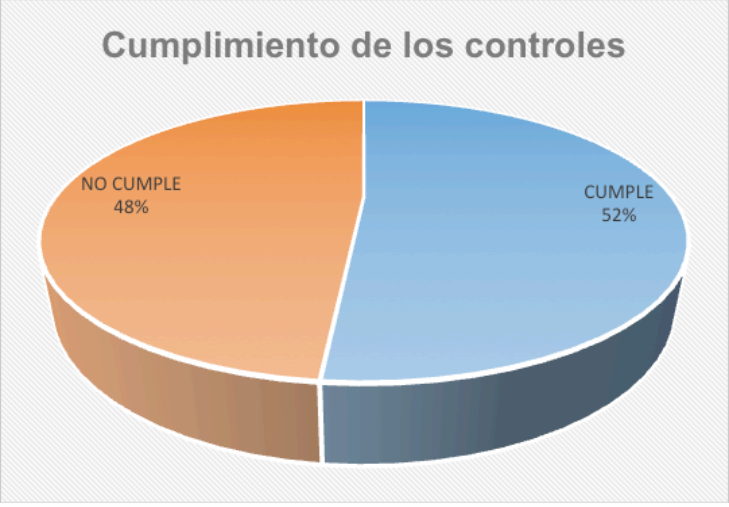
2. RESULTADOS Y DISCUSIÓN

Durante el desarrollo del proyecto se obtuvo información acerca del Módulo de Gestión Académica, utilizando entrevistas y encuestas, las herramientas e instrumentos se aplicaron a directivos de la Universidad Técnica del Norte como: director de informática, jefe de proyectos de desarrollo, analistas de sistemas, administrador de bases de datos, administrador de sistios web, administrador de red, jefe de soporte de usuarios, jefe de pruebas, secretarias, docentes y estudiantes.

En las entrevistas y encuestas se pudo diagnosticar el incumplimiento de varios de los controles recomendados por la normativa ISO/IEC 27002:2013, esto demuestra que el módulo de gestión académica tiene varias amennazas y vulnerabilidades que pueden poner en riesgo la información de toda la población estudiantil.

Para poder evaluar los resultados de la normativa ISO/IEC 27002:2013, se consideró un checklist de cumplimiento, tomando los resultados de las entrevistas y encuestas a los usuarios y actores del módulo de gestión académica. (CCN-CERT, 2013)

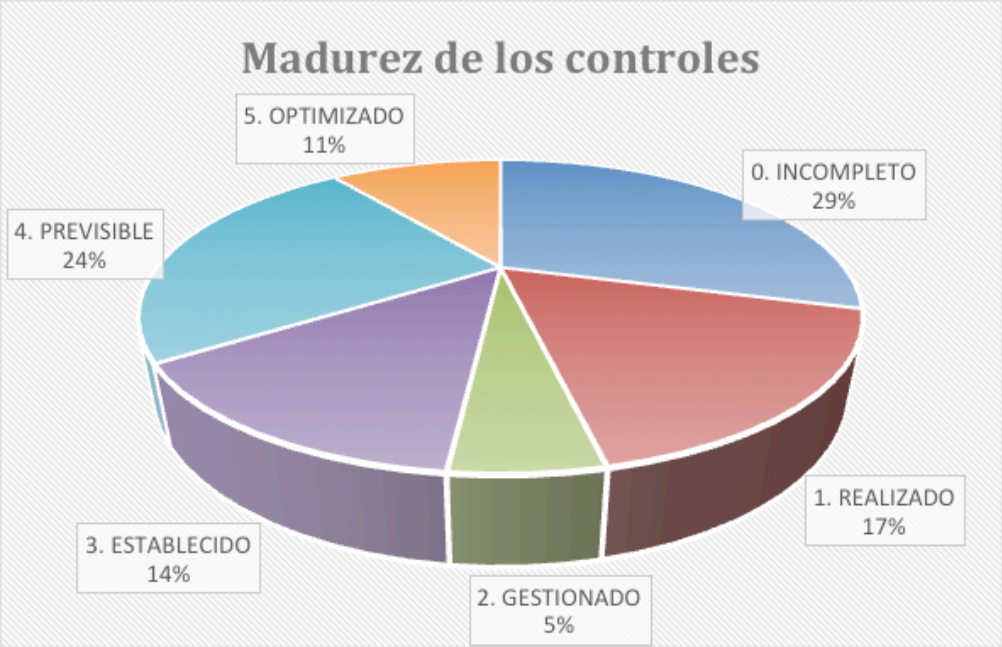
Gráfico 1: Cumplimiento de los Controles ISO/IEC 27002:2013



El gráfico 1 representa el porcentaje de cumplimiento de los controles de la normativa ISO/IEC 27002:2013 depues de haber verificado mediante un checklist, lo que evidencia que la seguridad de la información del módulo de gestión académica en todos sus aspectos de seguridad tiene que mejorar el cumplimiento de politicas y controles que garanticen la continuidad del negocio

Una vez determinado los controles relacionados con la seguridad de la información del módulo de gestión académica, se validó el nivel de madurez de los mismos, tomando como referencia el modelo de madurez de capacidad (CMM) del marco de referencia Cobit 5. (ISACA, 2012)

Gráfico 2: Madurez Controles ISO/IEC 27002:2013



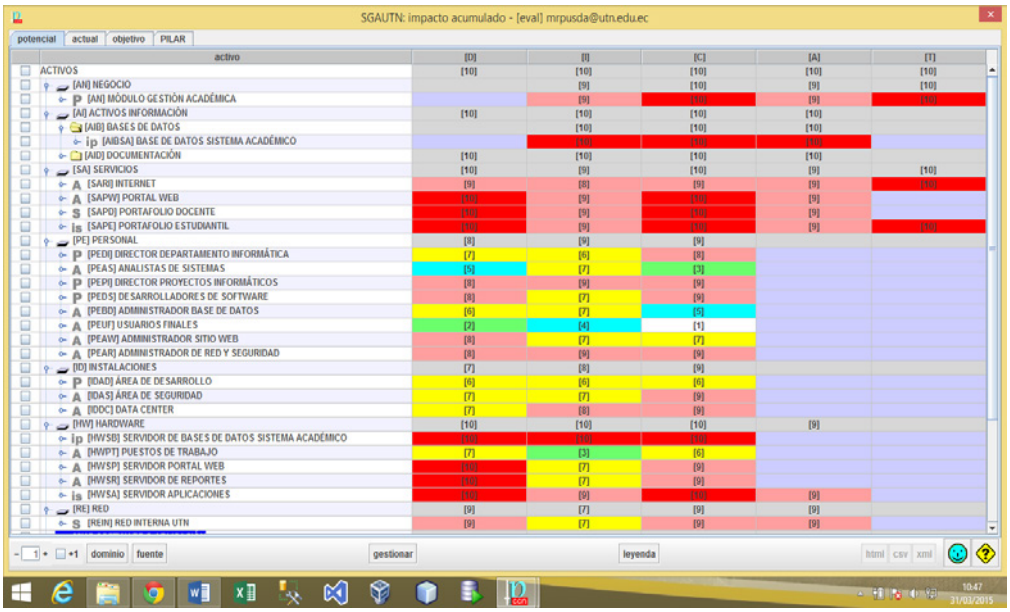
El gráfico 2 representa el porcentaje de cumplimiento de los controles de la normativa ISO/IEC 27002:2013 implementados en el módulo de gestión académica, de acuerdo a la escala recomendada por el marco de referencia Cobit 5.0, la escala tiene cinco niveles de cumplimiento determinados de la siguiente manera: Nivel 5 (Optimizado) se considera el valor máximo de cumplimiento en un rango entre 81 - 100%, Nivel 4 (Previsible) se considera el cumplimiento en un rango entre 61 – 80%, Nivel 3 (Establecido) se considera el cumplimiento en un rango entre 41 – 60%, Nivel 2 (Gestionado) se considera el cumplimiento en un rango entre 21 – 40%, Nivel 1 (Realizado) se considera el cumplimiento en un rango entre el 01 -20%, Nivel 0 (Incompleto) se considera el incumplimiento total de politica o procedimiento relacionados con seguridad de la información.

Gráfico 3: Cumplimiento de controles ISO/IEC 27002:2013

Los datos del gráfico 3 representa los 65 controles verificados en el módulo de gestión académica, lo que demuestra que son pocos los controles (Optimizado) que cumplen rigurosamente el estándar de seguridad recomendado por ISO/IEC 27002:2013 en sistemas de información, la mayoría de controles requieren de mejoras (Previsible, Establecido, Gestionado, Realizado) e incluso algunos controles (Incompleto) necesitan ser dieñados e implementados las politicas y procesos de seguridad de la información.

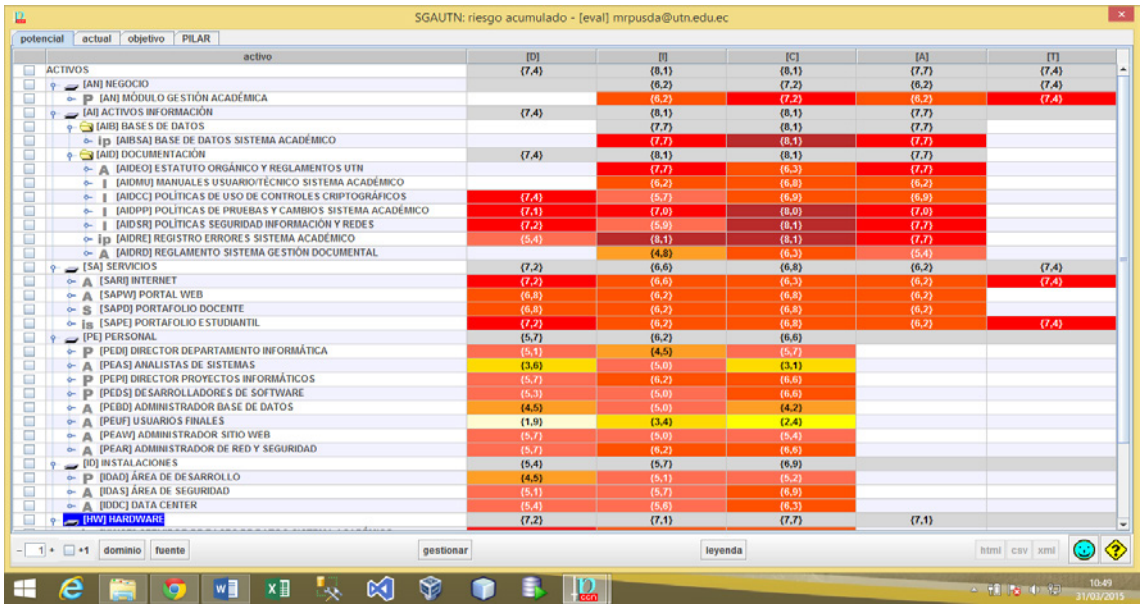
Una vez determinado el nivel de cumplimiento de los controles de ISO/IEC 27002:2013 en el módulo de gestión académica, se procede a la clasificar los activos de información y seguir el proceso recomendado por PILAR, tanto para identificación y valoración de activos, identificación de amenazas, se generan informes del impacto y riesgos. (CCN-CERT, 2013)

Figura 4: Impacto Acumulado Módulo Gestión Académica



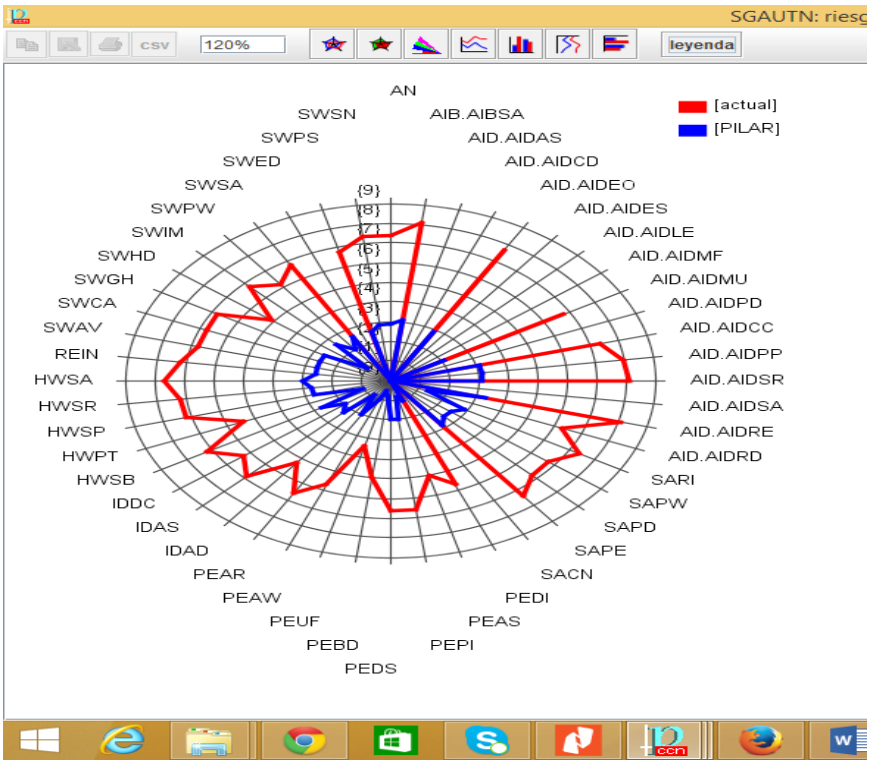
La Figura 4, representa la dependencia de los activos del módulo de gestión académica, los mismos que dependen unos de otros, la materialización de amenazas en los activos inferiores causa un daño directo sobre éstos y un daño indirecto sobre los activos superiores, afectando al rendimiento de todas las aplicaciones e infraestructura tecnológica y por ende la confidencialidad, integridad y disponibilidad de la información.

Figura 5: Riesgo Acumulado Módulo Gestión Académica



La Figura 5, representa el riesgo acumulado de todos los activos relacionados con el módulo de gestión académica, el mismo que revela el grado del daño probable de las aplicaciones e infraestructura, debido a launa amenzaza puede materializarce sobre uno o varios activos causando daños o perjuicios a la institución educativa.

Figura 6: Situación Actual Riesgo Acumulado Módulo Gestión Académica



La Figura 6, indica la situación actual del riesgo al que esta expuesto el módulo de gestión académica, la línea de color rojo es el resultado del cumplimiento de los controles implementados, esto significa que se debe realizar un adecuado tratamiento y gestión de riesgos para mitigar las amenazas y vulnerabilidades que puedan afectar el buen desempeño de los servicios que brinda el sistema acedémico integrado a la población estudiantil. La línea azul indica el nivel óptimo para reducir el riesgo cumpliendo las politicas y procesos relacionados con la seguridad de la información recomendados por ISO/IEC 27002:2013

Conclusiones

- La normativa ISO/IEC 27002:2013, desempeñan un papel importante para identificar el cumplimiento de controles que garanticen la seguridad de la información del módulo de gestión académica del sistema integrado de la Universidad Técnica del Norte.

- El análisis y gestión de riesgos son imprescindibles dentro del Departamento de Desarrollo y Transferencia Tecnológica de la Universidad Técnica del Norte, ya que se debe considerar la importancia de la información como activo institucional.

- La identificación de vulnerabilidades y amenazas del módulo de gestión académica permitió conocer las debilidades en diferentes aspectos definidos por el estándar ISO/IEC 27002:2013.

- La metodología MAGERIT permitió realizar un análisis de riesgos de la seguridad de los activos de información del Módulo de Gestión Académica del Sistema Integrado Informático Universitario.

- El análisis de riesgo aplicado, nos permitió conocer de manera global el estado actual de la seguridad informática del Área de Programación del Departamento de Desarrollo y Transferencia Tecnológica de la Universidad Técnica del Norte.

- La situación actual de cumplimiento de los controles evidencian un bajo nivel de madurez en los dominios de políticas de seguridad de la información, física y gestión.

Recomendaciones

- Crear el área de Gestión y Calidad de TIC, para que se encargue de revisar que las aplicaciones cuenten con calidad basadas en ISO 27000, como son ambientes de trabajo, desarrollo, pruebas y producción.

- El Departamento de Desarrollo y Transferencia Tecnológica de la Universidad Técnica del Norte, actualmente presenta un nivel de riesgo informático considerable que con el apoyo de las autoridades universitarias y de todo el personal administrativo es posible contrarrestar.

- Actualizar las políticas y procedimientos de la seguridad de la información acorde a las necesidades actuales del Departamento de Desarrollo y Transferencia Tecnológica de la Universidad Técnica del Norte, para mejorar la confiabilidad, integridad y disponibilidad de la información.

- Documentar todos los procedimientos operativos y de gestión de las aplicaciones que integran el módulo de gestión académica, para optimizar los procesos orientados a cumplir los objetivos institucionales

- Realizar documentos, manuales de todos los cambios del módulo de gestión académica y de la infraestructura de comunicaciones, además de controlar las versiones del Módulo de gestión académica y por ende su documentación de respaldo.

Bibliografía

• CCN-CERT. (2013). Libro I Magerit 3, Método. Madrid, España.
• CCN-CERT. (2013). Libro II Magerit 3, Catálogo de elementos. Madrid, España.
• CCN-CERT. (2013). Libro III Magerit 3, Guías de Técnicas. Madrid, España.
• Departamento Informática UTN. (2013). Manual de Funciones Departamento Informática. Ibarra, Imbabura, Ecuador.
• Departamento Informática UTN. (2013). Plan Estratégico Departamento de Informática. Ibarra, Imbabura, Ecuador.
• EAR / PILAR. (2014). EAR / PILAR, Análisis de Riesgos. Obtenido de http://www.ar-tools.com/es/tools/pilar/index.html
• Echenique, J. (2012). Auditoría en Informática. México: McGrawHill.
• ISACA. (2012). Cobit 5. Un Marco de Negocio para el gobierno y la gestión de las TI de la empresa. Madrid: ISACA.
• ISO 27000. (2013). Gestión de la Seguridad de la Información. Obtenido de http://iso27000.es/iso27002.html
• ISO 27002 ESPAÑOL. (2013). ISO 27002. Obtenido de http://www.iso27002.es/
• PAE - Portal de Administración Electrónica. (Octubre de 2012). PAE - Magerit v3 Metodología de Análisis y Gestión de riesgos de los Sistemas de Información.
• Piattini, M. (2010). Auditoría Informática. Madrid: RA-MA.
• SYBSEC S.A. (2012). Soluciones de Seguridad Informática. Obtenido de http://www.cybsec.com/ES/default.php
• UNIT - Instituto Uruguayo de Normas Técnicas. (2014). UNIT - ISO/IEC 27000. Obtenido de http://www.unit.org.uy/normalizacion/sistema/27000/
• Universidad Técnica del Norte. (2012). Plan Estratégico Institucional. Ibarra, Imbabura, Ecuador.