ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER.

"EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000"

AUTORES: IMBAQUINGO ESPARZA, DAISY ELIZABETH

PUSDÁ CHULDE, MARCO REMIGIO

DIRECTOR: ING. JORGE CARAGUAY PRÓCEL MSC.

SANGOLQUÍ MAYO 2015

CERTIFICADO

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN EVALUACIÓN Y SISTEMAS TECNOLÓGICOS

Ing. Jorge Caraguay Prócel MsC.

CERTIFICO

Que el trabajo titulado EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000, realizado por los Ing. Daisy Elizabeth Imbaquingo Esparza y Marco Remigio Pusdá Chulde, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas –ESPE.

Debido a que constituye un trabajo que aporta de forma positiva a la gestión que realiza la Universidad Técnica del Norte, contribuyendo a la mejora continua de los servicios que ofrece al desarrollo de la comunidad, me permito recomendar su publicación.

Además, se autoriza a la Ing. Daisy Elizabeth Imbaquingo Esparza y al Ing. Marco Remigio Pusdá Chulde, que entregue el presente trabajo al Mgtr. Rubén Darío Arroyo Chango, en su calidad de Director de la Carrera.
El mencionado trabajo consta de un empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf).

Sangolquí, Mayo del 2015

Ing. Jorge Caraguay Prócel MsC.
DIRECTOR

AUTORÍA DE RESPONSABILIDAD

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y SISTEMAS TECNOLÓGICOS

DAISY ELIZABETH IMBAQUINGO ESPARZA
MARCO REMIGIO PUSDÁ CHULDE

DECLARAMOS QUE

El Trabajo de investigación denominado EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000, ha sido desarrollado respetando los derechos intelectuales de terceros, conforme las citas cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Mayo 2015.

Ing. Daisy Elizabeth Imbaquingo Esparza Ing. Marco Remigio Pusdá Chulde

AUTORES

AUTORIZACIÓN

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRÍA EN EVALUACIÓN Y SISTEMAS TECNOLÓGICOS

Nosotros, Daisy Elizabeth Imbaquingo Esparza y Marco Remigio Pusdá Chulde

Autorizamos a la Universidad de las Fuerzas Armadas – ESPE, la publicación en la biblioteca virtual de la Institución del trabajo EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Mayo 2015.

Ing. Daisy Elizabeth Imbaquingo Esparza Ing. Marco Remigio Pusdá Chulde

AUTORES

DEDICATORIA

Este trabajo lo dedicamos a nuestros padres, por ese gran ejemplo de superación y valioso apoyo en todo momento.

A nuestras familias, por la colaboración y ese sacrificio continuo que nos brindaron para de esta forma seguir adelante.

A nuestras compañeras de clase con quienes trabajamos continuamente.

AGRADECIMIENTO

Nuestros agradecimientos a la Universidad de las Fuerzas Armadas ESPE, por brindarnos la posibilidad de adquirir nuevos conocimientos.

A las autoridades de la Universidad Técnica del Norte por permitirnos realizar el presente trabajo de tesis.

A los docentes que compartieron sus sabios conocimientos en el aula y a los que nos colaboraron para la culminación del presente trabajo.

Al Ing. Jorge Caraguay Prócel, por su amable colaboración, su apoyo y sus valiosas sugerencias como director de este trabajo de grado.

Al Ing. Rubén Arroyo, por su amable colaboración y apoyo constante.

Los Autores

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

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 política y procedimientos y falta de personal cualificado. Para finalizar el presente trabajo se realizó un informe de no conformidades y recomendaciones.

PALABRAS CLAVE:

- **ISO**
- **ISO/IEC 27000**
- **MAGERIT**
- **PILAR**

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. At the end of the work, a report was done which contains non-conformities and recommendations.

KEYWORDS:

- **ISO**
- **ISO / IEC 27000**
- **MAGERIT**
- **PILAR**

CAPÍTULO I

1.1 ANTECEDENTES

El Módulo de Gestión Académica, del Sistema Informático Integrado Universitario (SIIU) de la Universidad Técnica del Norte, se ha convertido por su alta usabilidad en uno de los más importantes por la información crítica generada dinámicamente en la institución, por tal razón está expuesto a riesgos y vulnerabilidades de tipo físico y lógico, en consecuencia amerita investigar y proponer alternativas que permitan resolver situaciones de posibles riesgos, que serán resultado de un estudio detallado y estructurado utilizando técnicas de evaluación y control.

Analizar cómo se está administrando los sistemas de información y los controles implantados, para en base al estudio implementar un correcto modelo de control y gobierno de TI, para obtener seguridad, confiabilidad, escalabilidad, reducir tiempos de operación y optimización de recursos en todos los ámbitos, que permitan continuidad de las operaciones en caso de suscitarse cualquier tipo de problema o incidente. Se utilizará el Marco de Referencia ISO 27000, que se basa en el uso de los controles dedicados a especificar requerimientos necesarios para establecer, implantar, mantener y mejorar un sistema de seguridad de la información.

1.2 JUSTIFICACIÓN E IMPORTANCIA

1.2.1 Estado del arte nivel mundial y local

Considerando la gestión de sistemas de Información tanto en lo estratégico como en lo operativo, los módulos integrantes cumplen un rol protagónico como ejes principales de la gestión de información, la misma que se genera de todos y cada uno de los procesos informáticos, convirtiéndose de esta forma en un requerimiento esencial para cualquier organización, en especial en las Instituciones Educativas cuyo proceso crítico está relacionado con la Gestión Académica al servicio de los estudiantes.

Según Sinisterra (2011), la auditoría se inició hace varios siglos atrás con los egipcios, con el objetivo de rendir cuentas y de poder salvaguardar la economía a través de la delegación de un integrante con formación en escritura y números para que realizara actividades como la organización de datos y cifras que permitirán una evaluación de la situación.

Según Tamayo (2011), con el pasar del tiempo siguen apareciendo nuevas actividades en la humanidad, una de ellas es la automatización de procesos, lo que ha generado en el mundo de la informática nuevos problemas y paradigmas que han sido seriamente cuestionados y causa de múltiples investigaciones a nivel mundial, para de esta forma determinar el cumplimiento de objetivos para los que fueron desarrollados e implementados y también por la calidad de servicios que la organización proporciona, razón por esta que se hace esencial que se evalúe cada uno de los procesos que se relacionan a la institución en especial cuando es la razón de ser de la empresa, ya que estos influyen directamente con la actividad del negocio, convirtiéndose de esta forma en la estructura fundamental donde fluye la información crítica institucional.

Por eso es necesario que los Sistemas de Información de las instituciones proporcionen el valor y la eficiencia que exigen tanto el negocio como los usuarios. Para confirmarlo, es recomendable realizar un proceso de evaluación y diagnóstico de la Seguridad de la Información. (Ibermática, 2012). Importante señalar que la transformación social, económica, política y funcional del Ecuador pretende estar alineada al Plan Nacional del Buen Vivir.

Al hablar de sistemas de información nos referimos a Seguridad en Bases de Datos, que es un tema de continua actualidad ya que en los últimos años ha adquirido un gran auge el estudio de bases teóricas e implementaciones prácticas, para asegurar la confidencialidad e integridad de la información, incluyendo algunos métodos con el fin de mantener la autenticidad de los datos. (Echenique, 2012)

El Departamento de Informática de la Universidad Técnica del Norte, se beneficiará porque la evaluación de riesgos y amenazas permitirá encontrar las debilidades en el módulo de gestión académica, posteriormente se realizará las respectivas recomendaciones basadas en los estándares ISO 27001, ISO 27002 las mismas que podrían hacer rectificaciones posteriores a las políticas y controles de seguridad críticos existentes.

Actualmente existen diversas metodologías de Auditoría de Sistemas, cada una con diferentes actividades o fases pero con objetivos similares, los mismos que son:

- El análisis de la eficiencia de los SI y la TI.
- La verificación del cumplimiento de la Normativa General de la Organización.
- La verificación de los Planes, Programas y Presupuestos de los Sistemas Informáticos.
- La revisión de la eficaz gestión de los recursos materiales y humanos informáticos.
- La revisión y verificación de Controles Técnicos Generales y Específicos de Operatividad

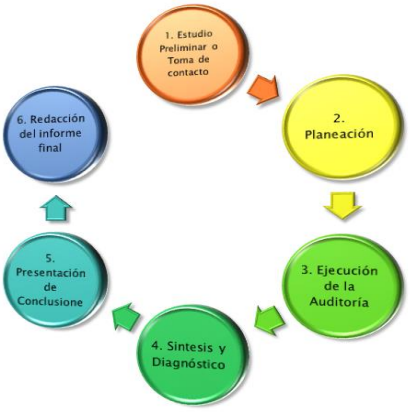


Figura 1.1: Fases de una auditoria de sistemas

Fuente: (ISO ESPAÑOL, 2014)

1.3 PLANTEAMIENTO DEL PROBLEMA

En el Departamento de Informática 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 adquirido.

Toda amenaza que pueda ser identificada contra el correcto funcionamiento del módulo de gestión académica y la consecución de sus objetivos, debe ser prioritario la realización de un análisis minucioso en todas sus fases. Para cada una de las amenazas se debe contemplar los posibles controles con el objetivo de mitigar los riesgos disminuyendo la probabilidad mínima de su realización.

Los controles son importantes medidas que permiten dar seguimiento a las políticas, normas y procedimientos para verificar, evaluar y tratar de garantizar el correcto funcionamiento del módulo de gestión académica en los diferentes ámbitos de responsabilidad.

Como actividad inicial se desarrolla el diagnóstico de la situación actual del módulo de gestión académica, con el fin de evaluar la consistencia de la información generada; la eficiencia, efectividad de las aplicaciones y servicios, y el cumplimiento políticas, procedimientos de seguridad de la información.

El paso siguiente es, verificar el nivel de cumplimiento de los controles de la normativa de seguridad de la información según el estándar ISO 27002:2013 para el módulo de gestión académica en la universidad.

Posteriormente se realiza la detección de vulnerabilidades y amenazas del módulo de gestión académica, utilizando herramientas de software libre, lo que permite determinar con certeza ciertos riesgos técnicos existentes.

Para finalizar se realiza el informe del cumplimiento de los controles del estándar ISO 27002:2013, detección de vulnerabilidades, amenazas y las recomendaciones que permitan mejorar la gestión de la seguridad de la información del módulo de gestión académica de la Universidad Técnica del Norte

1.4 FORMULACIÓN DEL PROBLEMA

¿Qué factores están influyendo para que el Departamento de Informática de la Universidad Técnica del Norte, no hayan tomado la decisión de realizar una evaluación de amenazas y vulnerabilidades al módulo de gestión académica para garantizar la seguridad de la información?

¿Cómo afecta, el no implementar políticas y procedimientos de manera adecuada a las aplicaciones que son parte del módulo de gestión académica, desarrolladas en el Departamento de Informática de la Universidad Técnica del Norte?

¿Cómo establecer una estrategia para implementar políticas y procedimientos de manera eficiente utilizando controles de ISO 27002:2013, que garanticen la seguridad de la información del módulo de gestión académica de la Universidad Técnica del Norte?

1.5 OBJETIVO GENERAL

Realizar una Evaluación de Amenazas y Vulnerabilidades del Módulo de Gestión Académica - Sistema Informático Integrado Universitario de la Universidad Técnica del Norte aplicando ISO 27000, con el fin de determinar el cumplimiento de políticas y controles que garanticen la seguridad de la información del Sistema Académico

1.6 OBJETIVOS ESPECÍFICOS

- Evaluar la situación actual de seguridad de la información del módulo de gestión académica de la Universidad Técnica del Norte

- Aplicar marco referencial ISO 27002:2013 para determinar el cumplimiento de políticas y controles de seguridad del módulo de gestión académica de la Universidad Técnica del Norte

- Determinar los riesgos del módulo de gestión académica en el departamento de Informática de la Universidad Técnica del Norte aplicando la Metodología Magerit.

- Documentar las recomendaciones que permitan asegurar una mayor integridad, confidencialidad y confiabilidad de la información, en base a un análisis y aplicación de metodologías, al módulo de gestión académica

1.7 ALCANCE

El proyecto de tesis "Evaluación de Amenazas y Vulnerabilidades del Módulo de Gestión Académica - Sistema Informático Integrado Universitario de la Universidad Técnica del Norte, aplicando ISO 27000", realizará la revisión de los riesgos y vulnerabilidades de la seguridad de la información revisando la implementación de políticas, procedimientos y controles que garanticen la seguridad informática.

De acuerdo a lo enunciado anteriormente, se procederá inicialmente con la recolección, agrupación y evaluación de evidencias para determinar la manera en la que se encuentran diseñados e implementados los controles de seguridad de la información del módulo de gestión académica en la Universidad Técnica del Norte, lo que nos dará una visión actual del Sistema Integrado Informático Universitario, para luego proceder a realizar las pruebas de cumplimiento de los controles, posteriormente procederemos a definir los riesgos que conlleva el ineficaz cumplimiento de estos controles o su falta de implementación, finalmente emitir las recomendaciones que permitan mejorar el desempeño de los servicios que el sistema académico ofrece a la comunidad universitaria

Este proyecto de tesis se ejecutará en el Departamento de Informática de la Universidad Técnica del Norte, con una duración de 27 semanas al final de las cuales se obtendrá un informe final en el que consten las condiciones encontradas y las respectivas recomendaciones de mejora para que puedan ser aplicadas según el criterio de las autoridades universitarias

CAPÍTULO II.- FUNDAMENTACIÓN TEÓRICA

2.1 MARCO TEÓRICO

2.1.1 Conceptos de auditoría y seguridad de la información

2.1.1.1 Auditoria

Hernández (2010), sostiene que la auditoría es un proceso necesario para las organizaciones con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. En donde, la alta dirección espera que de estos procesos de auditoría surjan recomendaciones necesarias para la mejora continua de las funciones, para que se lleven a cabo de manera oportuna y satisfactoria, las políticas, controles y procedimientos definidos con el objeto de que cada individuo o función opere de modo productivo en sus actividades diarias.

Según la Norma ANSI N45.2.10.1973 (2012), manifiesta: "Actividad para determinar por medio de la investigación, la adecuación de y la adhesión a, los procedimientos establecidos, instrucciones, especificaciones, códigos y estándares, u otros requisitos aplicables así como la eficacia de su implantación".

La Auditoría de Sistemas, es un proceso de revisión de la manera en la que se están administrando actualmente los sistemas y los controles implantados en los mismos, basado en un criterio o modelo de control y gobierno de TI establecido (COBIT, ITIL, ISO), recolección de evidencias significativas y la emisión de una opinión independiente acerca de los controles evaluados. (Tamayo, 2011)

La Auditoría como cualquier otra disciplina toma diferentes características de acuerdo al campo de acción y a las personas, tanto una auditoria interna como una auditoria externa debe mantenerse fuera de cualquier contenido político, y política general de la empresa u organización. (Siniesterra, 2011)

La función de un auditor se desempeña por pedido o política dela empresa dependiendo de sus razones, para ello se cuenta con algunos tipos de auditorías:

- Auditoria de Cumplimiento
- Auditoria Operativa
- Auditoria Informática de sistemas
- Auditoria a los planes de desarrollo empresarial
- Auditoria Administrativa
- Auditoría Financiera
- Auditoria de Gestión
- Auditoria de Gestión Ambiental
- Auditoria de Gestión y resultados
- Auditoría Integral

2.1.1.2 Seguridad Informática

Según Jeimy J. Cano, Ph.D., CFE (2014) : Seguridad Informática, esta disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

2.1.1.3 Análisis y Gestión de Riesgos

"El Análisis y Gestión de Riesgos son procedimientos formales para encontrar los riesgos que existen en un Sistema de Información y mediante un estudio responsable, recomienda medidas apropiadas que deberían acogerse para controlarlos." (Echenique, 2012), además se podrá saber el estado real de seguridad del módulo de gestión académica de la Universidad Técnica del Norte.

El Análisis de Riesgos busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. (Piattini, 2010)

2.1.2 ISO 27000

2.1.2.1 ¿Qué es la norma ISO 27001?

Según ISO ESPAÑOL (2014), es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (Plan-Do-Check-Act; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

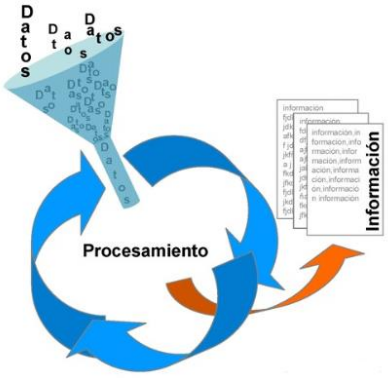


Figura 2.1: Esquema de un sistema de gestión de seguridad información

Fuente: (ISO ESPAÑOL, 2014)

"Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001". (ISO ESPAÑOL, 2014)

2.1.2.2 ¿Cuál es el origen de ISO 27001?

Su origen está en la norma de BSI (British Standards Institution) BS7799-Parte 2, norma que fue publicada por primera vez en 1998 y ya era un estándar certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005. (ISO, 2012)

2.1.2.3 ¿Qué es la serie ISO 27000?

ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En 2005 incluyó en ella la primera de la serie (ISO 27001). En próximos años está prevista la incorporación de nuevas normas que supongan un apoyo para las organizaciones que implanten y certifiquen un SGSI según ISO 27001. (ISO ESPAÑOL, 2014)

Entre otras, serán 27000 (términos y definiciones), 27002 (objetivos de control y controles), 27003 (guía de implantación de un SGSI), 27004 (métricas y técnicas de medida de la efectividad de un SGSI), 27005 (guía para la gestión del riesgo de seguridad de la información) y 27006 (proceso de acreditación de entidades de certificación y el registro de SGSIs). (ISO ESPAÑOL, 2014)

2.1.2.4 ¿Qué aporta la ISO 27001 a la seguridad de la información de una empresa?

"Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua." (ISO ESPAÑOL, 2014)

Según Echenique (2012) manifiesta: ISO 27001 ayuda a la empresa a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un coste más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc.

Ochoa y Cervantes (2012), afirman: “La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.”

Según ISO 27001 (2012), Seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas implicados en su tratamiento.

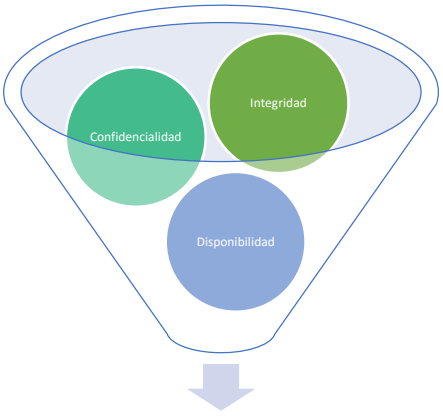


Figura 2.2: Seguridad de la Información

Integridad: “Significa que el sistema no debe modificar ni corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados sin que se haya producido ninguna modificación, adición o borrado.” (www.unl.edu.ar, 2010)

Confidencialidad: “La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información almacenada en él” (www.unl.edu.ar, 2010)

Disponibilidad: “Significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de falla” (www.unl.edu.ar, 2010)

Análisis de Riegos: “Significa que, en primer lugar es necesario identificar los riesgos que afectan a la Organización, y en segundo lugar, es necesario establecer medidas de seguridad o controles para reducir o mitigar estos riesgos.” (Piattini, 2010)

Dentro de la Gestión de riesgos podemos diferenciar dos etapas: Análisis y Controles. Para desarrollar todo el proceso de análisis y tratamiento de los riesgos, es imprescindible establecer una Metodología, la cual definirá los pasos que se tienen que seguir para llevar a cabo la Gestión de Riesgos.

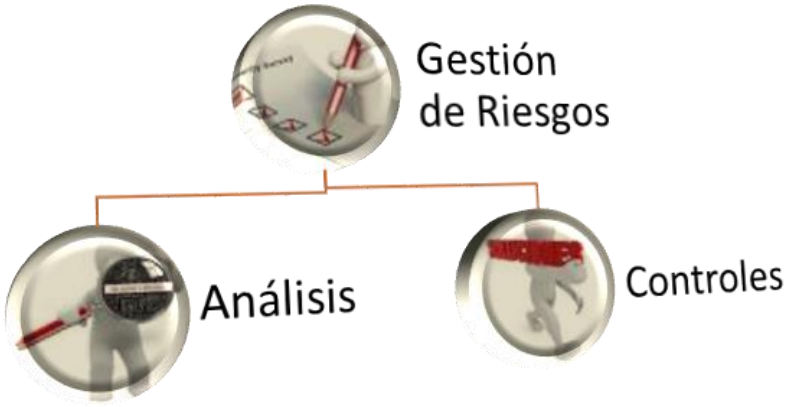


Figura 2.3: Gestión de Riesgos

Para poder Gestionar Riesgos en el Área de informática es indispensable contar con el área de seguridad el mismo que debe realizar las siguientes actividades:

Figura 2.4: Plan Integral de Seguridad

Fuente: (ISO ESPAÑOL, 2014)

Plan Integral de Seguridad: “Se detallan lineamientos de la planeación, el diseño e implantación de un modelo de seguridad cuyo principal objetivo es proteger la información y los activos de la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos.” (Hernández, 2010)

Políticas de Seguridad: “Requisitos definidos por los responsables de un sistema, que indica en términos generales, que está y que no está permitido en el área de seguridad durante la operación del sistema”. (Piattini, 2010)

La RFC 1244 define Política de Seguridad como: "Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán” (Holbrook., 1991)

Inventario de Activos Informáticos: Se debe realizar un listado detallado de los activos de información así como su localización, se consideran como activos: Impresoras, dispositivos de almacenamiento (discos duros externos, memorias flash, aplicaciones, ordenadores, servidores, personas, etc.). (Jeimy J. Cano, Ph.D., CFE, 2014).

Auditorías: “Es necesario que en las organizaciones se realice un aseguramiento independiente de la administración en relación a la efectividad de los objetivos de la seguridad de la información.” (Piattini, 2010)

2.1.2.5 ANTECEDENTES DEL ESTADO DEL ARTE

2.1.3 Familia de normas ISO/IEC 27000

2.1.4 Introducción

Normas ISO 27000: Familia de estándares de ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporciona un marco para la gestión de la seguridad. Es el conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI. (ISO, 2012). Las normas se clasifican en:

- Normas base: 20001, 20002
- Normas complementarias: 20003, 20004, 20005

2.1.4.1 ISO/IEC 27001

Norma que especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de la organización. Especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de las mismas. (ISO, 2012). Especifica los requisitos a cumplir para:

- Implantar un SGSI certificable conforme a las normas 27000
- Define cómo es el SGSI, cómo se gestiona y cuáles son las responsabilidades de los participantes.
- Sigue un modelo PDCA (Plan-Do-Check-Act)
- Puntos clave: Gestión de riesgos + Mejora continua

2.1.4.2 ISO/IEC 27002:2013

Conjunto de recomendaciones sobre qué medidas tomar en las empresas para asegurar los Sistemas de Información. Código de buenas prácticas para la gestión de la seguridad, (ISO, 2012).

Los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que se aplican en la gestión de riesgos.

Figura 2.5: Contenidos de la norma ISO 27002:2013

Fuente: (UNIT- Instituto Uruguayo de Normas Técnicas, 2015)

Objetivos: Definir los aspectos prácticos/operativos de la implantación del SGSI en cada área o sección.

- Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento.
- Realizar la libre difusión de información en español en base a las investigaciones, conocimientos y búsquedas de los editores de la web.
- Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen (empresas grandes, Pymes, organismos públicos, estudiantes, entre otros.
- Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar informaciones, opiniones, experiencias o conocimientos, e impulsar la colaboración en actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información.

Características: La normativa presenta las siguientes:

- Recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización

- Describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar)
- Antes ISO 17799, basado en estándar BS 7799 (en España norma UNE-ISO 17799)

Áreas/secciones sobre las que actuar:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

Controles: "Mecanismos para asegurar los distintos objetivos de control (guía de buenas prácticas)" (ISO ESPAÑOL, 2014). Para cada control se incluye una guía para su implantación

2.1.4.3 ISO/IEC 27003

Guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan-Do-Check-Act) y de los requerimientos de sus diferentes fases (en desarrollo, pendiente de publicación)

2.1.4.4 ISO/IEC 27004

Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados (en desarrollo, pendiente de publicación). Permite la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

2.1.4.5 ISO/IEC 27005

Gestión de riesgos de seguridad de la información (recomendaciones, métodos y técnicas para evaluación de riesgos de seguridad)

2.1.4.6 ISO/IEC 27006

Requisitos a cumplir por las organizaciones encargadas de emitir certificaciones. ISO/IEC 27001, requisitos para la acreditación de las entidades de auditoria y certificación

2.1.4.7 ISO/IEC 27007

Guía de actuación para auditar los SGSI conforme a las normas 27000

2.1.5 Magerit v3

2.1.5.1 Introducción

MAGERIT, es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. (CCN-CERT, 2012)

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. (International Classification for Standards (ICS), 2012)

MAGERIT es de interés para todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT permite saber cuánto valor está en juego y ayuda a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que evita la improvisación, ni la arbitrariedad del analista. (CCN-CERT, 2013)

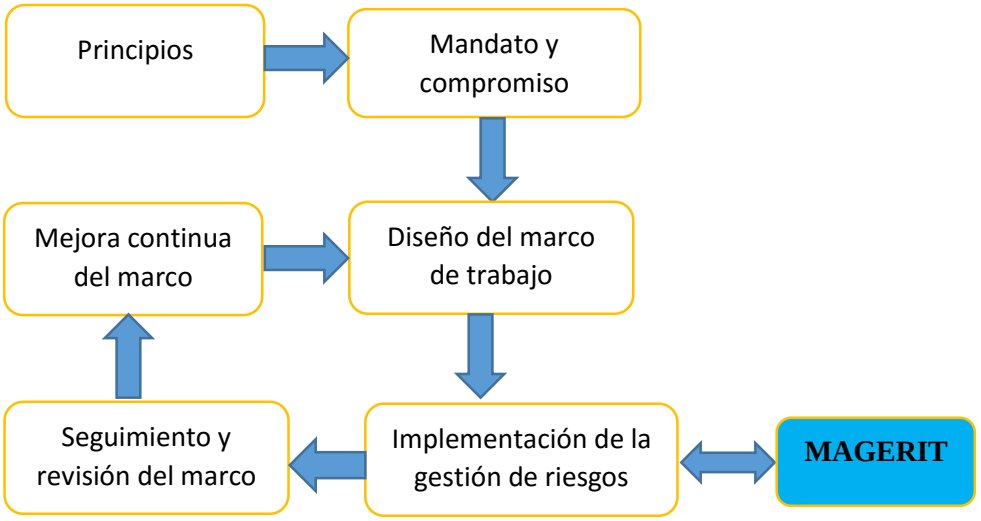


Figura 2.6: Marco de trabajo para la gestión de riesgos

2.1.5.2 Características

- Mantiene en gran medida la estructura de la versión 2
- Actualizada para un mejor alineamiento con la normativa ISO
- Integración dentro del marco organizacional de la gestión de riesgos dirigido desde los órganos de gobierno
- Eliminación de partes poco importantes o poco utilizadas, reducción del texto
- Mejora la normalización de las actividades

2.1.5.3 Objetivos

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

2.1.5.4 Organización de las guías

MAGERIT versión 3 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas". (CERT GUBERNAMENTAL ESPAÑOL, 2014)

CAPÍTULO III.- MEMORIA TÉCNICA METODOLÓGICA

3.1 DIAGNÓSTICO

3.1.1 Análisis de la situación actual

Hoy en día la amenaza más importante contra la información académica de la Universidad Técnica del Norte, ya sea por accesos indebidos o no autorizados a la información institucional usuarios internos o externos de la misma. Adicionalmente se suman los ataques de virus informáticos que son ocasionados intencionalmente o por desconocimiento de los usuarios.

Lo importante es que las universidades realicen una evaluación de riesgos, para determinar la importancia que tienen los mismos. El resultado del análisis establecerá si se está exponiendo la información internamente o externamente. La clave está en que existan políticas de Seguridad de la Información y que sean puestas en práctica para que estén concientizados de la importancia de la información.

Luego del desarrollo de las políticas de Seguridad de la Información es necesaria una difusión a todos los usuarios del sistema académico que intervienen en la manipulación de la información, por cualquier medio disponible, con el fin de concientizar a los empleados.

El Departamento de Informática se 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 diseñan e implementan utilizando plataforma ORACLE 11g, servidores Linux, y otras herramientas compatibles.

El Departamento de Informática no cuenta con documentación de Auditorias Informáticas que sirvan de base para el presente trabajo, por lo que este será el primer documento de recomendación con que cuenta la Institución. Análisis FODA del Departamento de Informática de la UTN

Tabla 3.1 Análisis FODA-UTN.

Análisis FODA-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 y
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
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 responsable de 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
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: (Departamento Informática UTN, 2013)

3.1.2 Estructura organizacional

3.1.2.1 Organigrama Estructural UTN

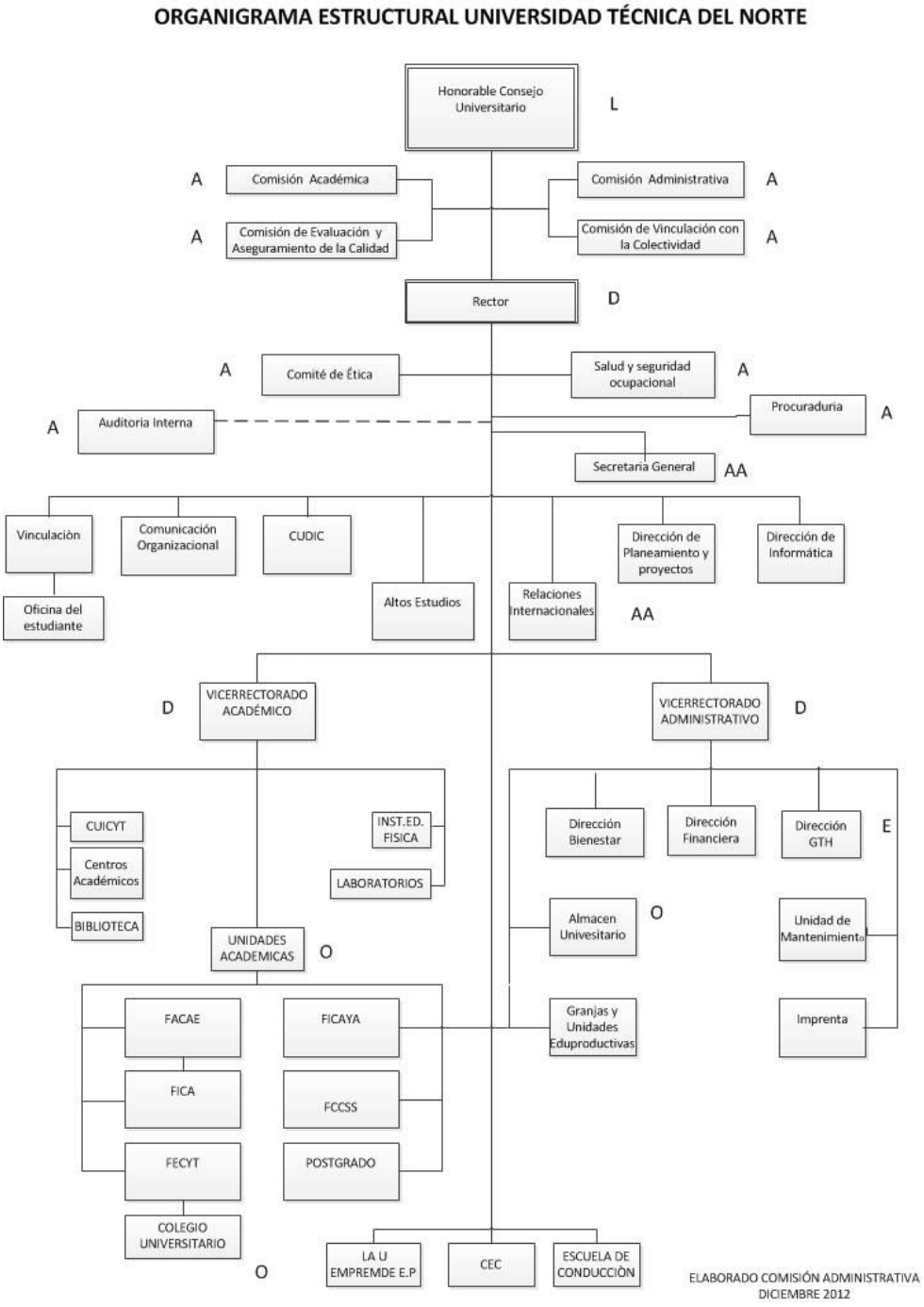


Figura 3.1: Organigrama Estructural UTN

Fuente: (Universidad Técnica del Norte, 2012)

3.1.2.2 Organigrama Departamento de Informática

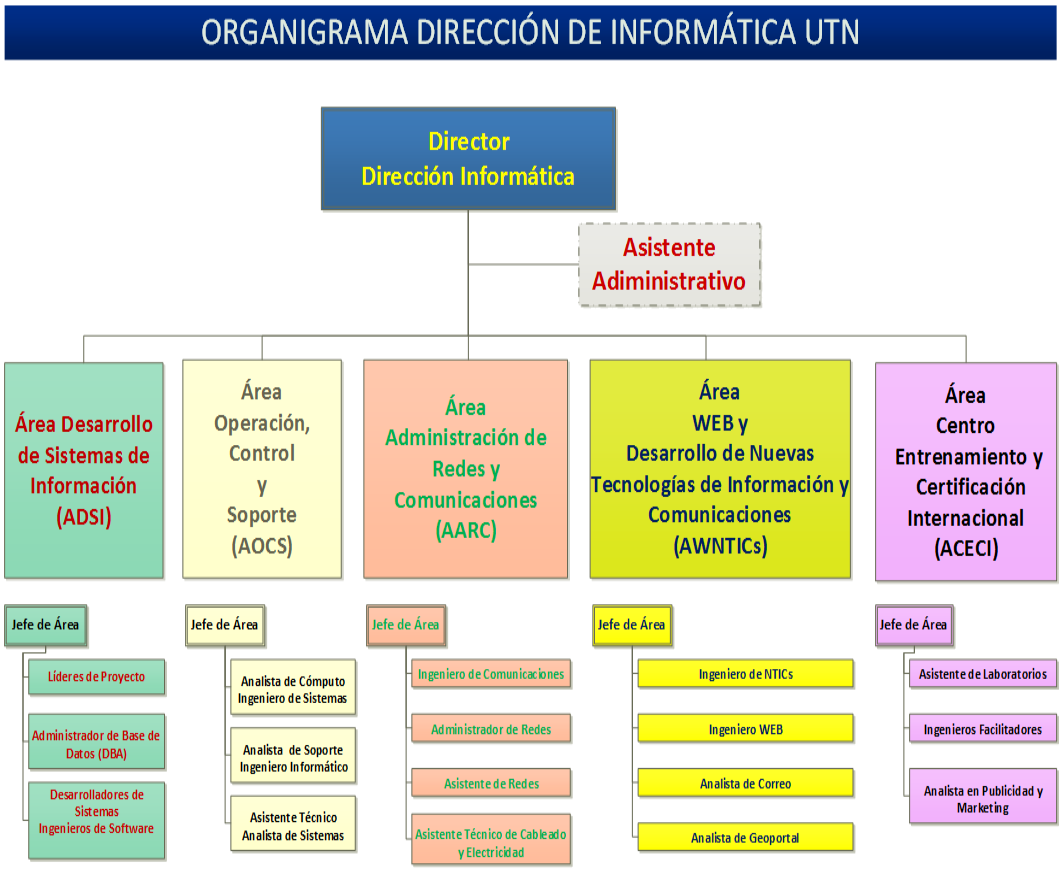


Figura 3.2 Organigrama Departamento de Informática – UTN

Fuente: (Departamento Informática UTN, 2013)

3.1.2.3 Roles y Responsabilidades y funciones del personal de TICS

Tabla 3.2

Roles y Funciones Personal TIC.

Puesto	Responsabilidades y Funciones
Jefe de Proyecto	El jefe de proyecto asigna los recursos, gestiona las prioridades, coordina las interacciones con los clientes y usuarios, y mantiene al equipo del proyecto enfocado en los objetivos institucionales. El jefe de proyecto también establece un conjunto de prácticas que aseguran la integridad y calidad de los artefactos del proyecto. Además, el jefe de proyecto se encargará de supervisar el establecimiento de la arquitectura del sistema optimizando los procesos institucionales minimizando sus tiempos y costos, brindando acceso a información integrada, confiable, precisa y oportuna. Impulsar y desarrollar proyectos de Tecnología de Información y Comunicación -TIC, que requiera la Universidad Técnica del Norte para su buen funcionamiento, para así brindar a la colectividad buen servicio optimizando tiempo y gastos innecesarios.
Analista de Sistemas	Captura, especificación y validación de requisitos, interactuando con el cliente y los usuarios mediante entrevistas. Elaboración del Modelo de Análisis y Diseño. Colaboración en la elaboración de las pruebas funcionales y el modelo de datos.
Programador	Construcción de prototipos. Colaboración en la elaboración de las pruebas funcionales, modelo de datos y en las validaciones con el usuario
Ingeniero de Software	Gestión de requisitos, gestión de configuración y cambios, elaboración del modelo de datos, preparación de las pruebas funcionales, elaboración de la documentación. Elaborar modelos de implementación y despliegue.
Administrador de la Red	Impulsar y desarrollar proyectos de Tecnología de Información y Comunicación -TIC, que requiera la Universidad Técnica del Norte para su buen funcionamiento, brindando a la colectividad buen servicio optimizando tiempo y gastos innecesarios. Personal de redes con certificaciones internacionales. Proponer la adquisición de paquetes de software, licencias y hardware, que permitan dar solución satisfactoria, a las necesidades tecnológicas. Tener una red monitoreada las 24 horas del día y operativa al 100%. Disponer de equipos para el monitoreo permanente de la red de la universidad.
Webmaster	Fortalecer la gestión de investigación. Implementación de nuevas tecnologías para la administración del GeoPortal y el manejo de NTIC´s en entornos virtuales. Participación en lo referente al soporte y soluciones informáticas de los diferentes planes y proyectos de las diferentes áreas de la institución que buscan mejorar las condiciones de sus procesos.

CONTINÚA ⟶

Ingeniero de Hardware	Implementar políticas de operación y control informático. Gestionar la adquisición de los insumos de software y hardware especializado, que permitan dar solución satisfactoria a la necesidad institucional. Programar planes de mantenimientos periódicos de los equipos informáticos de la UTN. Establecer políticas de reciclaje de insumos y materiales. Formular un plan de contingencia, que asegure la protección del hardware y la información contenida, ante la presencia de algún fenómeno natural o provocado. Capacitar al personal Docente y Administrativo de la Institución en la aplicación de reglas y normas de acceso restringido a los sistemas. Adquirir el servicio de mantenimiento correctivo de equipos informáticos de la institución. Manejo del Catálogo Electrónico de equipos informáticos del Sistema Nacional de Compras Púbicas. Administrar contratos de Servicio de Mantenimiento Preventivo y correctivo de la Institución. Administrar contratos de servicio de mantenimiento correctivo de Proyectores digitales. Soporte técnico en sitio.

Fuente: (Departamento Informática UTN, 2013)

3.1.2.4 Misión

A la Dirección de Desarrollo tecnológico e Informático de la Universidad Técnica del Norte, le corresponde administrar los servicios de informática, computación y comunicaciones, sin perjuicio de las demás funciones que se le recomiende. Ser el ente regulador de las políticas y normativas de carácter institucional; que deben ser llevadas a cabo con rigor, manteniendo el alto espíritu de calidad en todos los funcionarios, con el fin de lograr las expectativas encomendadas al departamento. (Departamento Informática UTN, 2013)

3.1.2.5 Visión

Establecer el rumbo estratégico del departamento y ejercer el liderazgo a nivel institucional, regional y nacional en el campo de la informática, computación y comunicaciones. (Departamento Informática UTN, 2013)

3.2 METODOLOGÍA DE LA INVESTIGACIÓN

3.2.1 Población y Muestra

Para calcular el tamaño adecuado de la muestra utilizamos el método del muestreo, el mismo que nos permitirá establecer un número de encuestados para determinar los servicios y seguridades del Sistema Académico de la Universidad Técnica del Norte.

El tamaño está determinado en gran medida por tres factores:

- Proporción estimada de la variable considerada
- Nivel deseado de fiabilidad; y
- Margen de error aceptable.

El tamaño de la muestra para un diseño de encuesta basado en una muestra aleatoria simple, puede calcularse mediante la siguiente fórmula. Fórmula:

$$\mathbf{n} = \frac{\mathbf{t^2 \times p(1-p)}}{\mathbf{m^2}}$$

Descripción:
n=tamaño de la muestra requerido

t= nivel de fiabilidad de 95% (valor estándar de 1,96)

p= prevalencia estimada en la zona del proyecto

m = margen de error de 5% (valor estándar de 0,05)

Para ello segmentamos la población: docentes, personal administrativo y estudiantes, la información con la que se tabularon los datos es la que el Departamento de Informática entregó con fecha diciembre 2014.

Tabla 3.3

Usuarios Sistema Académico UTN.

Usuarios	Número	Porcentaje
Estudiantes	7770	86.90%
Docentes	770	8.61%
Personal Administrativo	401	4.49%
	8682	100%

Fuente: (Departamento Informática UTN, 2013)

Aplicando dicha fórmula encontramos los siguientes datos:

$$n = \frac{(1.96)^2\,(0.25)(8941)}{(0.05)^2(8941-1)+(1.96)^2(0.25)}$$

$$n = 368$$

Estudiantes

Número de estudiantes encuestados= **320**

Docentes

Número de docentes encuestados= **32**

Personal Administrativo

Número de personal encuestados= **16**

3.2.2 Metodología de Investigación

Existen algunas metodologías de Auditorías de Sistemas y todas dependen de lo que se pretenda revisar o analizar, pero como estándar analizaremos las cuatro fases básicas de un proceso de revisión:

- Estudio preliminar
- Revisión y evaluación de controles y seguridades
- Examen detallado de áreas críticas
- Comunicación de resultados

3.2.2.1 Tipos de Investigación

Para realizar la evaluación de amenazas y vulnerabilidades de seguridad de la información necesitamos conocer la infraestructura tecnológica de la Universidad Técnica del Norte se ha utilizado dos tipos de investigación ellas son:

Descriptiva: Podremos decir que este proyecto es de investigación descriptiva porque necesitamos trabajar con las actividades, procedimientos y características fundamentales que se tienen actualmente en la Universidad Técnica del Norte para poder comprobar los riesgos relacionados con la seguridad de la información del sistema de gestión académica

Mixta: El presente trabajo se utiliza la investigación mixta porque las políticas que existan en la Universidad Técnica del Norte y el Departamento de Informática, relacionadas con la seguridad de la información serán en base a encuestas a los usuarios del sistema académico utilizando Check list, permitirán revisar los procedimientos actuales y todo esto para verificar que políticas de seguridad utilizadas en la universidad.

Transversal: Es de investigación transversal porque la recolección de información nos ayudan a realizar la evaluación técnica del sistema de gestión académica, la misma que se desarrollará en un tiempo definido.

3.2.2.2 Métodos de Investigación

El método científico: Uno de los métodos de investigación que llevaremos a cabo es el científico ya que el proyecto seguirá los lineamientos de la norma ISO/IEC 27002:2013

El método deductivo: Realizaremos método deductivo por lo que la norma ISO/IEC 27002:2013 plantea una guía de controles a ser aplicada en todo tipo de organización:

El método inductivo: Finalmente se realizar el método inductivo, por el cual nos basaremos de datos particulares (lo investigado) para determinar las amenazas y vulnerabilidades que tiene el sistema de gestión académica.

3.2.2.3 Fuentes y técnicas de recolección de información

Para la obtención de la información nos regiremos a las siguientes técnicas:

Check list: Para recoger la información relevante, se utilizó un Check List referente a los controles de gestión y operación planeados o usados en el Sistema de Gestión Académica. Este Check list nos ayudará a dar seguimiento cada control de la norma ISO/IEC27002:2013 y verificar su aplicabilidad.

Encuestas: Las encuestas se realizaron al director del departamento de informática, personal operativo del departamento de informática, personal administrativo, docentes, estudiantes la cual nos permitirán recoger información útil.

Visitas locales: Esta técnica nos permite observar y recolectar la información sobre la seguridad física y operacional del sistema de gestión académica. La visita local podría proporcionar la oportunidad de evaluar el ambiente físico en el cual el sistema de información se desarrolla y se implementa

Revisión de documentación: Otra de las técnicas que realizaremos es la revisión de documentación como por ejemplo:

- Documentación de políticas generales
- Documentación legislativa
- Documentación de directrices
- Documentación del sistema de información: Guía de usuario del sistema, Manual administrativo del sistema
- Manual del diseño del sistema
- Manual de requerimientos.
- Documentación relacionada con la seguridad: Último informe de auditoría
- Informe de evaluación de riesgos
- Resultados de pruebas del sistema
- Plan de seguridad del sistema

3.3 PLAN DE AUDITORIA

Para de desarrollo de la Auditoría del módulo de Gestión Académica del Sistema Integrado Informático Universitario de la Universidad Técnica del Norte, seguiremos cada una de las fases de un Plan de Auditoria de la Calidad.

3.3.1 Sujeto de la auditoria:

Universidad Técnica del Norte, Departamento de Informática, Sistema Integrado informático Universitario - Módulo de Gestión Académica

3.3.2 Objetivo de la Auditoria

Realizar una Evaluación de Amenazas y Vulnerabilidades del Módulo de Gestión Académica - Sistema Informático Integrado Universitario de la Universidad Técnica del Norte aplicando ISO 27000, con el fin de determinar políticas y controles adecuados para garantizar la seguridad de la información del Sistema Académico.

3.3.3 Objetivos Específicos

- Evaluar el diseño y prueba del Módulo de Gestión Académica del Sistema Integrado Informático Universitario Informático Universitario de la Universidad Técnica del Norte.
- Evaluar los procedimientos de control de operación

3.3.4 Alcance de la auditoría

Evaluación Técnica del Módulo de Gestión Académica del Sistema Integrado Informático Universitario de la Universidad Técnica del Norte, el tiempo que se evaluará este aplicativo va a ser aproximadamente 30 días laborables. Al final de dicha evaluación se realizará un informe de auditoría con recomendaciones que ayuden a mejorar la seguridad de la información del sistema académico.

3.3.5 Relación de funcionarios o personal a cargo del área a examinar

Tabla 3.4

Personal Departamento Informática UTN.

NOMBRES Y APELLIDOS	PUESTO	PERIODO DE GESTIÓN DEL	AL
Ing. Juan Carlos García	Director del Departamento de Informática	Viernes, 20 Octubre, 1995	Actualmente
Ing. Evelyn Enríquez	Analista de Sistemas	Sábado, 01 Septiembre, 2007	Actualmente
Ing. Luis Aguilar	Analista de Sistemas	Sábado, 01 Septiembre, 2007	Actualmente
Ing. Vinicio Guerra	Administrador de la Red	Domingo, 01 Junio, 2014	Actualmente
Ing. Javier Carlosama	Analista de Sistemas	Sábado, 01 Septiembre, 2007	Actualmente
Ing. Alex Guevara	Webmaster	Sábado, 01 Septiembre, 2007	Actualmente

Fuente: (Departamento Informática UTN, 2013)

3.3.6 Sistema Auditar Módulo de Gestión Académica

Nro	Modulo	Descripción	Prioridad
1	Gestión Académica	Inscripción y matriculación (Registro e información de aspirantes que recibirán los cursos de preparación académica, Proceso de matriculación en las diferentes Unidades Académicas: facultades, institutos o centros, Equiparación y convalidación de asignaturas) , gestión curricular y expediente (Calendarios académicos, Apertura y cierre de ciclos académicos (años, semestres, etc.), Parámetros y requisitos de eventos y actividades académicas, Historiales académicos de estudiantes, Fichas socioeconómicas de estudiantes), gestión de mallas curriculares y horarios (Mantenimiento físico de edificios de unidades académicas: facultades, institutos, escuelas, especialidades y unidades de apoyo, académico: laboratorios, granjas, talleres, etc. Parámetros y requisitos de mallas, curriculares y pensum académico, planes curriculares y sílabos, distributivo docente, Control de horarios), gestión de evaluación académica, asistencia e información gerencial. Matrículas e inscripciones vía internet, pruebas de admisión, notas vía internet y seguimiento a egresados y graduados.	1

Figura 3.3: Servicios Módulo Gestión Académica.

Fuente: (Departamento Informática UTN, 2013)

3.3.7 Cronograma de Trabajo

Tabla 3.5

Programa Auditoría.

PROGRAMA DE AUDITORIA			
EMPRESA	UNIVERSIDAD TÉCNICA DEL NORTE- DEPARTAMENTO DE INFORMÁTICA	**FECHA:**	**HOJA N.-**
FASE	ACTIVIDAD	HORAS ESTIMADAS	RESPONSABLES
I	**VISITA PRELIMINAR**	8	Lic. Samia Bedón
	Solicitud de Manuales y Documentaciones		
	Elaboración de cuestionarios		Ing. Evelyn Enríquez
	Recopilación de la información organizacional: estructura orgánica, recursos humanos		
II	**DESARROLLO DE LA AUDITORIA**	32	Ing. Juan Carlos García
	Aplicación de cuestionario al personal		
	Entrevista Director de Informática		Ing. Evelyn Enríquez
	Entrevista Analista a cargo del Módulo de Gestión Académica Análisis de claves de acceso, control, seguridad, confiabilidad y respaldos		Ing. Luis Aguilar
	Evaluación de la estructura orgánica, puestos, funciones y responsabilidades		Ing. Alex Guevara
	Evaluación de Módulo de Gestión Académica: relevamiento de hardware y software, evaluación del diseño lógico y del desarrollo		Ing. Vinicio Guerra
	Evaluación del proceso de datos y de los equipos de cómputo: seguridad de los datos, control de operación, seguridad física y procedimiento de respaldo		Ing. Javier Carlosama
III	**REVISIÓN Y PRE-INFORME**	16	Ing. Juan Carlos García- Director Informática UTN
	Revisión de los papeles de trabajo		
	Determinación del diagnóstico e Implicaciones		
	Elaboración de carta al Rector de la Universidad Técnica del Norte Elaboración del Borrador		
IV	**INFORME**	4	Dr. Miguel Naranjo - RECTOR UTN
	Elaboración y presentación del Informe		

3.3.8 Diagrama de GANT

ACTIVIDADES

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
Elaboración de cuestionarios	2 días	lun 02/02/15	mar 03/02/15		
Recopilación de la información organizacional: estructura orgánica, recursos humanos	5 días	mié 04/02/15	mar 10/02/15	1	
Aplicación de cuestionario al personal	3 días	mié 11/02/15	vie 13/02/15	2	
Entrevista Director de Informática	1 día	mié 18/02/15	mié 18/02/15	3	
Entrevista Analista a cargo del Módulo de Gestión Académica	1 día	jue 19/02/15	jue 19/02/15	4	
Análisis de claves de acceso, control, seguridad, confiabilidad y respaldos	2 días	vie 20/02/15	lun 23/02/15	2;3;4;5	
Evaluación de la estructura orgánica, puestos, funciones y responsabilidades	2 días	mar 24/02/15	mié 25/02/15	6	
Evaluación de Módulo de Gestión Académica: relevamiento de hardware y software, evaluación del diseño lógico y del desarrollo	2 días	jue 26/02/15	vie 27/02/15	6;7	
Evaluación del proceso de datos y de los equipos de computo: seguridad de los datos, control de operación, seguridad física y procedimiento de respaldo	3 días	lun 02/03/15	mié 04/03/15	8	
Revisión de los papeles de trabajo	3 días	jue 05/03/15	lun 09/03/15	7;8;9	
Determinación del diagnóstico e Implicaciones	2 días	mar 10/03/15	mié 11/03/15	10	
Elaboración de carta al Rector de la Universidad Técnica del Norte	1 día	jue 12/03/15	jue 12/03/15	11	
Elaboración del Borrador	3 días	vie 13/03/15	mar 17/03/15	12;10	
Elaboración y presentación del Informe	2 días	mié 18/03/15	jue 19/03/15	13	

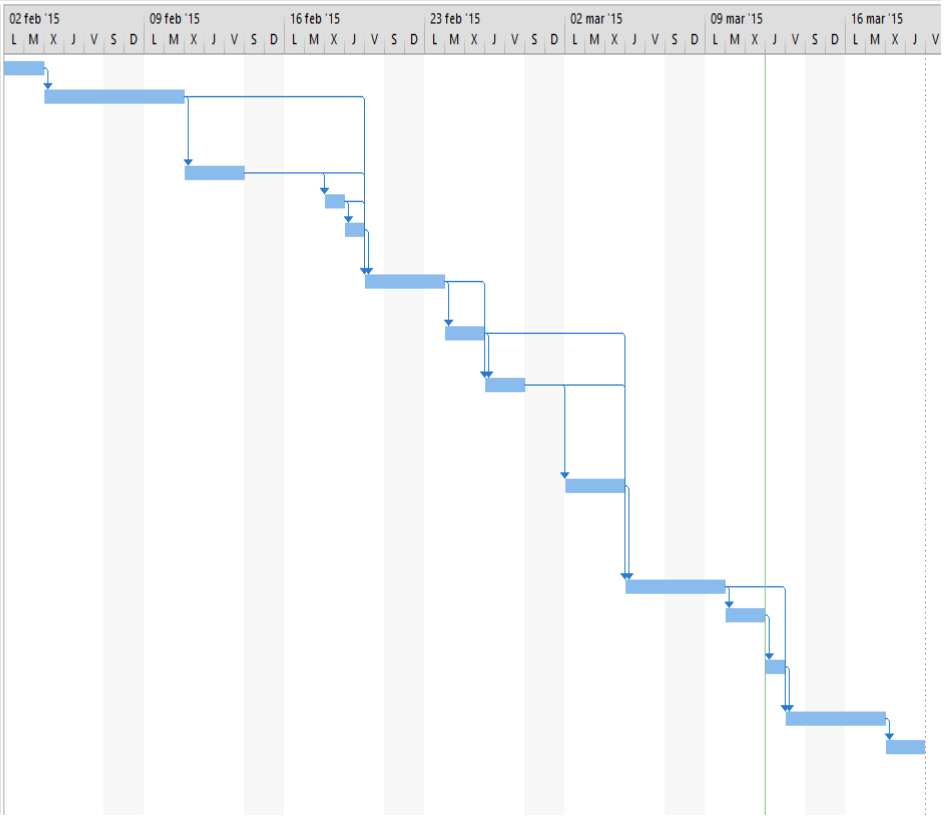


Figura 3.4: Cronograma Plan Auditoría.

3.3.9 Documentos a solicitar

- Políticas, normas, procedimientos
- Plan estratégico del Departamento de Informática
- Contratos
- Organigrama y manual de funciones
- Manual de Usuario y técnico del Módulo de Gestión Académica
- Registros
- Entrevistas
- Archivos
- Requerimientos de Usuarios
- Comunicaciones electrónicas (Quipux)
- Características de técnicos de infraestructura
- Configuraciones Firewall
- Diagrama de Red

3.3.10 Recopilación de Datos

Dentro de esta etapa se pudo obtener información acerca del Módulo de Gestión Académica, por lo que se utilizó herramientas clave para poder recabar información que sea de utilidad para el presente trabajo.

En el desarrollo de esta Auditoría, se cuenta con herramientas como la entrevista y la encuesta que es aplicada al Director de Informática de la universidad Técnica del Norte, basándonos en el orgánico funcional del departamento; en el caso del Jefe Proyectos de Desarrollo no está actualmente dirigido por ningún funcionario por lo que se aplica la encuesta a una Analista de informática quien cuenta con más experiencia y años trabajando en la Institución, administrando el Módulo de Gestión Académica, todos ellos basados en los dominios.

En dicha entrevista se pudo evidenciar que los analistas y programadores no cuentan con ambientes de prueba separados del área de desarrollo

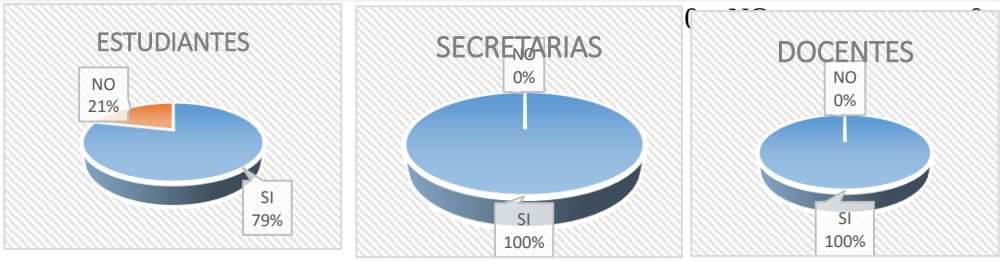
La encuesta que se desarrolló a toda la comunidad universitaria ósea docentes, personal administrativo y estudiantes quienes se encuentran enlazados directamente con el módulo de gestión académica de la Universidad.

3.3.10.1 Análisis de las encuestas

Para el desarrollo de la presente tesis se realizó una encuesta a los usuarios finales del Módulo de Gestión Académica del Sistema Integrado Informático Universitario de la Universidad Técnica del Norte, con la finalidad de realizar un diagnóstico de la calidad del servicio.

1. ¿Conoce el funcionamiento del Sistema de Gestión Académica de la Universidad Técnica del Norte?

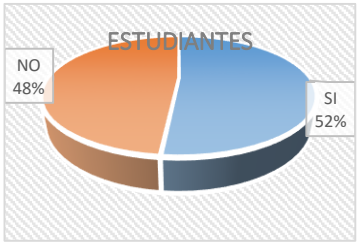
ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	252	SI	16	SI	32

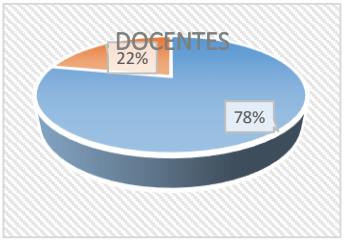


Análisis de Resultados: De acuerdo a los datos obtenidos, se puede determinar que todos los docentes y secretarias académicas conocen el funcionamiento del Sistema Académico, a excepción de los estudiantes que en un 21% no está bien informados acerca de su funcionamiento. En base a esto se puede decir que la mayoría de usuarios si conoce el funcionamiento del Sistema de Gestión Académica

2. ¿Conoce los servicios que brinda el sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	165	SI	16	SI	25
NO	155	NO	0	NO	7

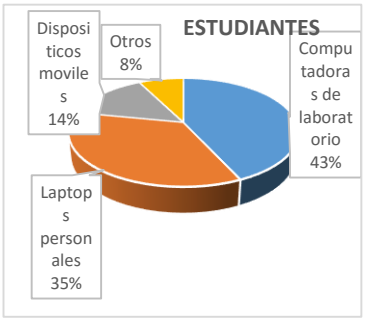


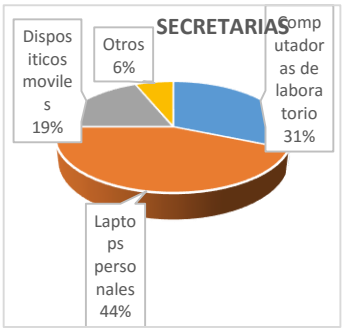


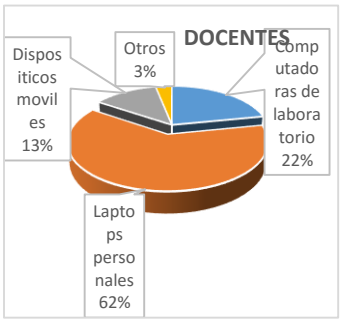
Análisis de Resultados: Acorde a los datos registrados podemos determinar que la mayoría docentes y secretarias de carrera conocen los servicios que brinda el Módulo de Gestión Académica, mientras que los estudiantes todavía desconocen de los servicios que brinda dicho sistema en un 48%.

3. ¿Qué tipo de dispositivos utiliza los servicios del sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Computadoras de laboratorio	138	Computadoras de laboratorio	5	Computadoras de laboratorio	7
Laptops personales	112	Laptops personales	7	Laptops personales	20
Dispositivos móviles	46	Dispositivos móviles	3	Dispositivos móviles	4
Otros	24	Otros	1	Otros	1



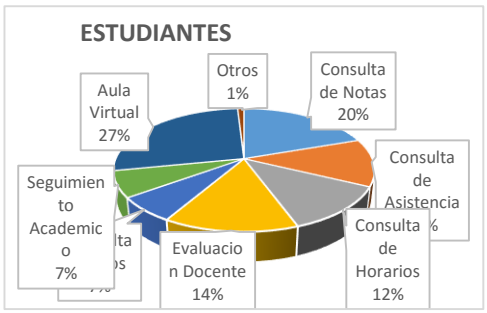


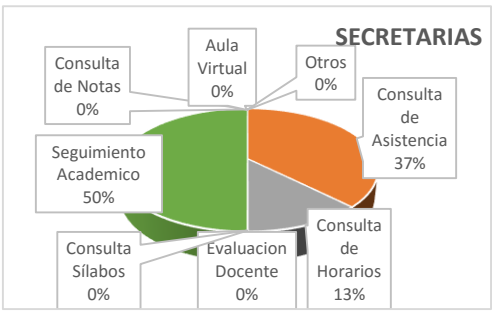


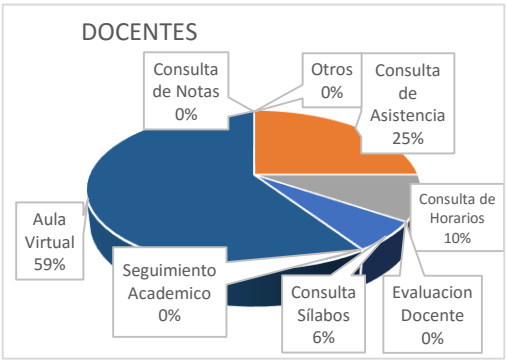
Análisis de resultados: De acuerdo a los datos recopilados pudimos evidenciar que en la mayoría de casos para acceder al Sistema de Gestión Académico lo realizan desde las computadoras de la Universidad Técnica del Norte, ya sea desde los Laboratorios de Informática de cada Facultad y en el caso de secretarias de la que a cada una de ellas se les ha designado y los estudiantes en gran porcentaje hacen uso de los recursos de la universidad en un 43%, al mismo tiempo observamos que las computadoras portátiles en los tres campos estudiantes, docentes y secretarias está llegando a un gran porcentaje en caso de estudiantes 35%, en las secretarias 44% y en el caso de docentes ellos tienen el 62% es decir que cada docente ya posee y hace uso del sistema desde sus computadoras personales, mientras q dispositivos móviles está creciendo su demanda.

4.- ¿Qué servicios utiliza del sistema de Gestión Académico?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Consulta de Notas	63	Consulta de Notas	0	Consulta de Notas	0
Consulta de Asistencia	40	Consulta de Asistencia	6	Consulta de Asistencia	8
Consulta de Horarios	39	Consulta de Horarios	2	Consulta de Horarios	3
Evaluación Docente	45	Evaluación Docente	0	Evaluación Docente	0
Consulta Sílabos	21	Consulta Sílabos	0	Consulta Sílabos	2
Seguimiento Académico	22	Seguimiento Académico	8	Seguimiento Académico	0
Aula Virtual	87	Aula Virtual	0	Aula Virtual	19
Otros	3	Otros	0	Otros	0







Análisis de resultados: Según los datos obtenidos en las encuestas podemos observar que hay una creciente demanda por parte de los estudiantes de los servicios que ofrece el Módulo de Gestión Académica con mayor porcentaje 27% el uso del Aula Virtual, con el 20% está la consulta de Notas, con el 14% está la evaluación docente y con el mismo 12% están las consultas tanto de horarios como de asistencias, mientras que tanto el seguimiento académico como la consulta de sílabos está con el 7% y apenas una 1% utilizan otro servicio. En los resultados de las encuestas realizadas a las secretarias de carrera el 50% utiliza el servicio del seguimiento académico, con el 37% se realiza consulta de asistencias, y con el 13% consulta de horarios. Mientras que los docentes en su gran mayoría con el 59% utilizan el Aula Virtual, el 25% realiza consulta de asistencias, el 10% consulta de horarios mientras que el 6% realiza consulta de sílabos.

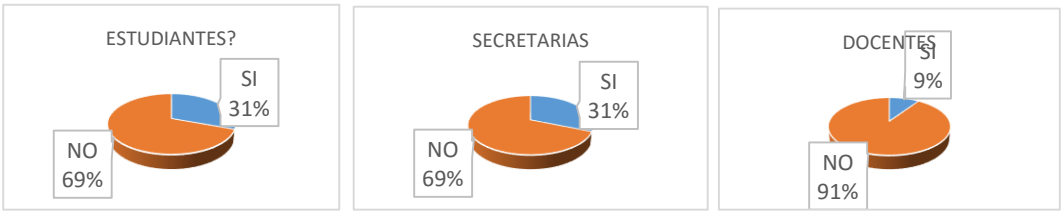
5.- ¿Cree Ud. que existe control de acceso a los servicios del sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	197	SI	16	SI	32
NO	123	NO	0	NO	0

Análisis de resultados: De los resultados obtenidos en el caso de los estudiantes el 62% cree que si existe un control para el acceso al sistema de gestión mientras que el 38% piensa lo contrario. En lo que tiene que ver a secretarias de carreras y docentes el 100% cree que si existe un control de acceso.

6.- ¿Las contraseñas empleadas para el acceso al sistema de Gestión Académica y sus servicios cuentan con requerimientos de seguridad?

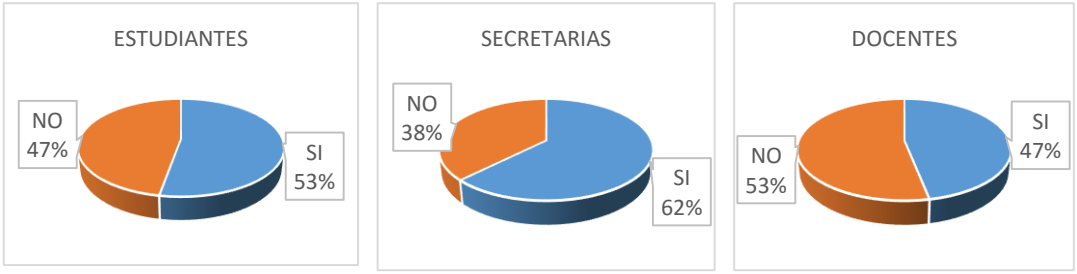
ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	98	SI	5	SI	3
NO	222	NO	11	NO	29



Análisis de resultados: Con los datos obtenidos pudimos verificar que el sistema de gestión académica cuenta con un control pero las contraseñas empleadas para el acceso al sistema no cuentan con los requerimientos de seguridad necesario en los casos de estudiantes y secretarias el 69% cree que no, mientras que el 31% cree que no. Mientras que el caso de docentes el 91% cree que el sistema no cuenta con requerimientos de seguridad.

7.- ¿El sistema de Gestión Académica tiene una política de bloqueo de computadores o sesiones después de un tiempo determinado?

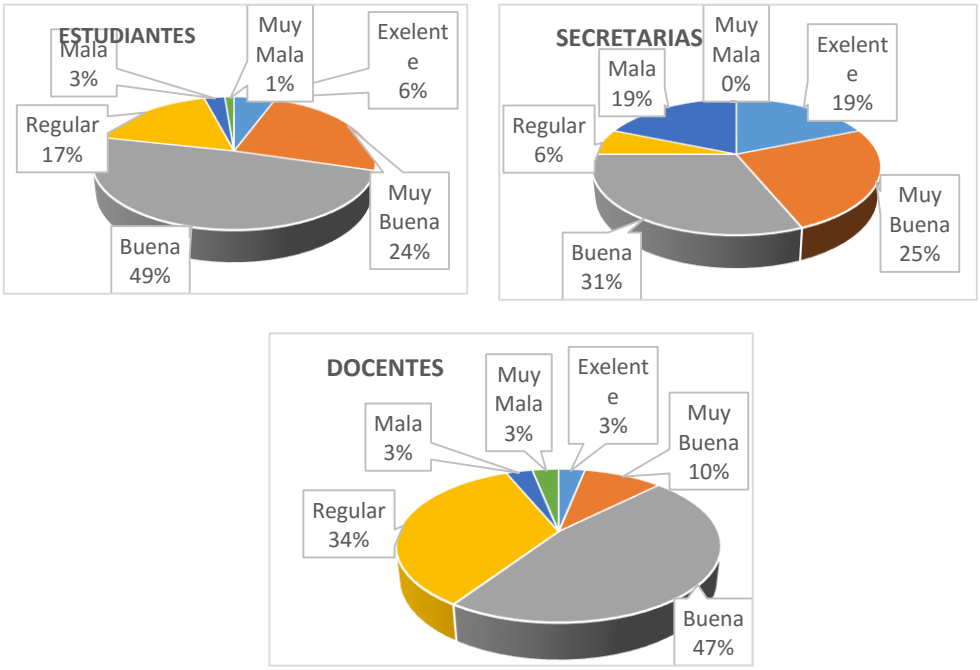
ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	169	SI	10	SI	15
NO	151	NO	6	NO	17



Análisis de resultados: De los resultados obtenidos en esta pregunta se puede identificar que en los dos estamentos estudiantes con el 53%, secretarias 62% creen que si existe una política de bloqueo de sesiones al usar el sistema de gestión académica tanto el 47 como el 38% cree que no respectivamente, en el caso de los docentes el 53% cree que no existe un bloqueo de sesiones y un 47% cree que sí.

8.- ¿Cuál es el nivel facilidad de uso del sistema Académico?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Excelente	18	Excelente	3	Excelente	1
Muy Buena	77	Muy Buena	4	Muy Buena	3
Buena	156	Buena	5	Buena	15
Regular	56	Regular	1	Regular	11
Mala	9	Mala	3	Mala	1
Muy Mala	4	Muy Mala	0	Muy Mala	1

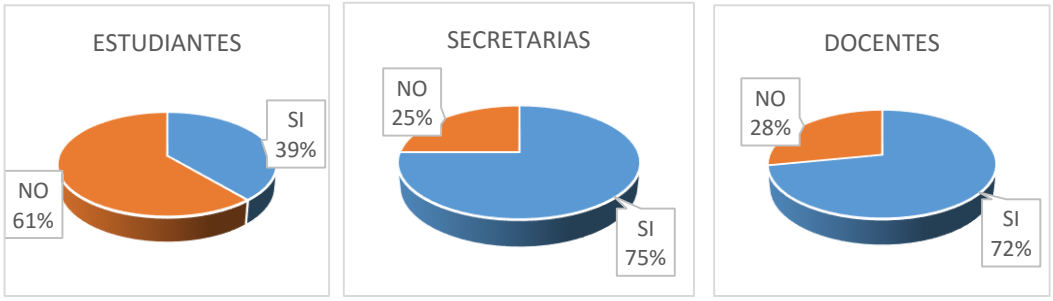


Análisis de resultados: De los datos registrados en lo que tiene que ver a estudiantes el mayor porcentaje es 49% donde indican que el nivel de facilidad para utilizar el sistema académico es bueno el 24% muy bueno el 17% Regular, el 6% excelente, el 3% mala, 1% muy mala. Al respecto los docentes mostraron los siguientes resultados 3% Excelente, 10% Muy buena, el 47% Buena quienes son mayoría, el 34% regular, 3% mala y muy mala.

De los resultados obtenidos de las secretarias de carrera tenemos los siguientes datos el 31% cree que es buena la facilidad de uso, el 25% muy buena el 19% mala, mientras que otro 19% cree que es excelente, el 6% regular.

9.- ¿Ha tenido inconvenientes en la utilización de los servicios del Sistema de Gestión Académica?

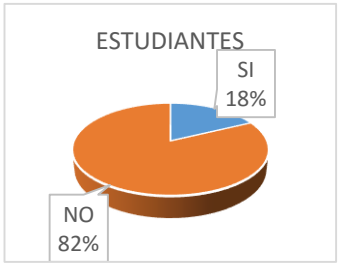
ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	124	SI	12	SI	23
NO	196	NO	4	NO	9

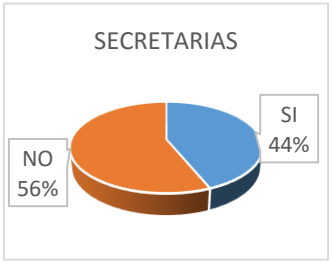


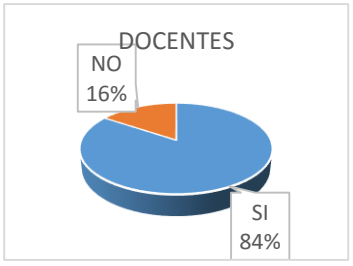
Análisis de resultados: De los resultados obtenidos en la presente encuentra encontramos que los estudiantes la mayoría con el 61% no han tenido inconveniente en la utilización del sistema académico mientas que el 39% dice que sí. Mientras que las secretarias de carreras muestran una mayoría del 75% y dicen que no tienen inconvenientes, frente a un 25% que dice que sí. En los docentes se manejan casi los mismo porcentajes es decir su mayoría el 72% no tiene inconvenientes mientas que el 28% dice que sí.

10.- ¿Ha tenido inconvenientes con la información obtenida de los servicios del sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	57	SI	7	SI	27
NO	263	NO	9	NO	5



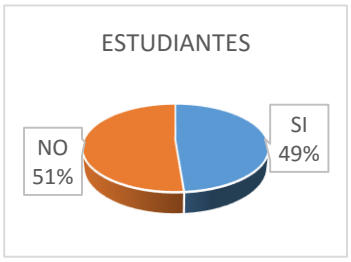


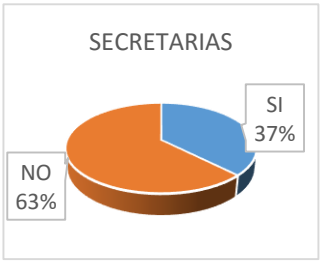


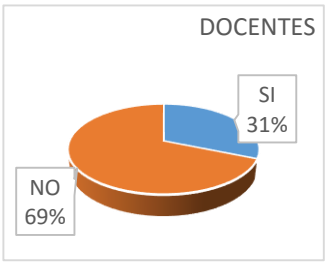
Análisis de resultados: Según los datos obtenidos acerca de inconvenientes con la información dela sistema académico los estudiantes respondieron en su gran mayoría con el 82% que no, solo un 15% respondió que s. Mientras que las secretarias el 56% respondió que sí y un 44 respondió que sí. En lo que respecta a docentes el 84% respondió que no y el 16% que sí. De donde podemos observar que la mayoría en las tres dependencias dice que NO.

11.- ¿Existe un responsable del Sistema de Gestión Académica que brinde atención cuando lo necesite?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	156	SI	6	SI	10
NO	164	NO	10	NO	22



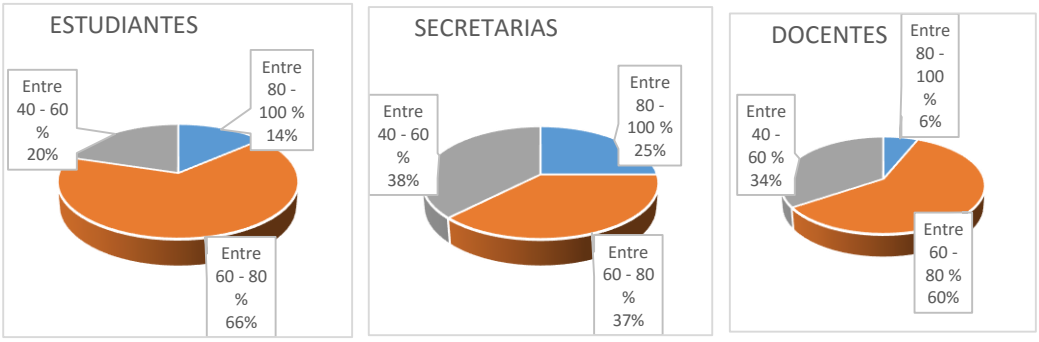




Análisis de resultados: De los datos obtenidos sobre si existe un responsable que le brinde atención cuando necesita acerca del sistema académico los estudiantes respondieron que NO el 51% un 49% dijo lo contrario, en las secretarias de carrera se manifestó que NO el 63% y el 37% dijo lo contrario, en la dependencia de los docentes la mayoría con el 69% respondió que NO y el 31% dijo lo contrario.

12. ¿En qué porcentaje se considera usted que el sistema de Gestión Académica satisface sus necesidades?

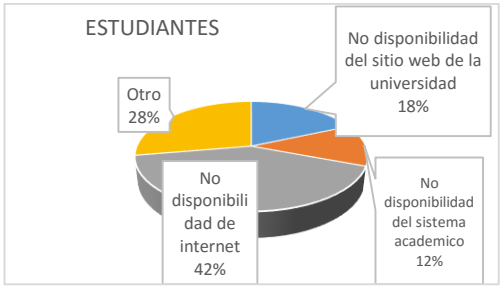
ESTUDIANTES		SECRETARIAS		DOCENTES	
Entre 80 - 100 %	44	Entre 80 - 100 %	4	Entre 80 - 100 %	2
Entre 60 - 80 %	211	Entre 60 - 80 %	6	Entre 60 - 80 %	19
Entre 40 - 60 %	65	Entre 40 - 60 %	6	Entre 40 - 60 %	11

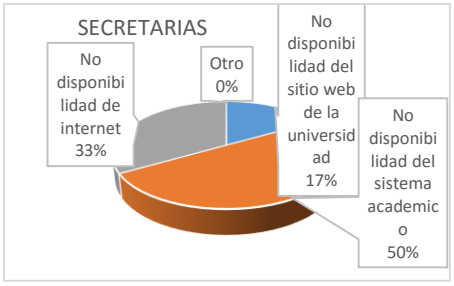


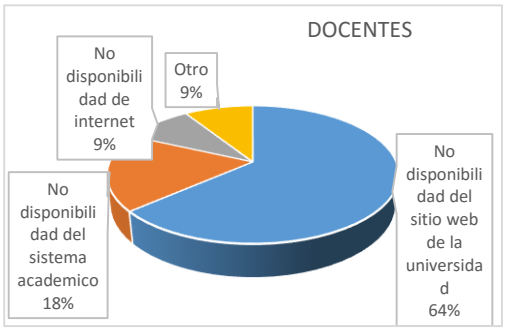
Análisis de resultados: De los resultados obtenidos en cuestión de estudiantes la encuesta arrojo estos resultados con respecto a si el Sistema satisface las necesidades donde respondiendo con mayoría con el 66% que si entre el 60 y 80, mientas que un 20% dijo que entre un 40 a 60, y un 14% entre 80-100. En lo que respecta a secretarias de carreras no se encontró una mayoría ya que el 38% cree que el sistema satisface las necesidades entre 40-60, el 37% entre 60-80 mientras que el 25% piensa que satisface entre el 80 a 100. En docentes tenemos una mayoría del 60% quienes opinan que satisfacen del 60 al 80, el 34% entre el 40 al 60 y solo un 6% entre el 80 a 100%.

13.- Si su respuesta a la pregunta anterior es inferior al 60%, indique el motivo principal.

ESTUDIANTES		SECRETARIAS		DOCENTES	
No disponibilidad del sitio web de la universidad	12	No disponibilidad del sitio web de la universidad	1	No disponibilidad del sitio web de la universidad	7
No disponibilidad del sistema académico	8	No disponibilidad del sistema académico	3	No disponibilidad del sistema académico	2
No disponibilidad de internet	27	No disponibilidad de internet	2	No disponibilidad de internet	1
Otro	18	Otro	0	Otro	1



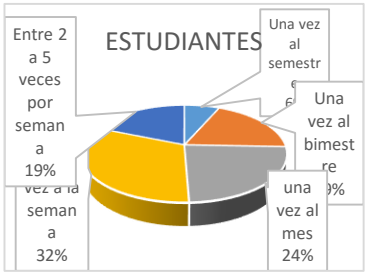


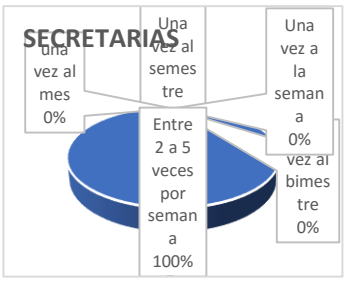


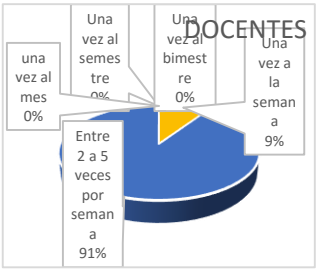
Análisis de resultados: De los datos recogidos en la pregunta anterior se pide que respondan si la respuesta fue inferior al 60% para saber el motivo de porque no se encuentran satisfechos con el sistema, en donde contestaron de la siguiente manera: estudiantes el 42% dijo que no había disponibilidad de internet, 18% no había disponibilidad del sitio web, el 12% no había disponibilidad del sistema académico, y el 28% otro. Mientras que las Secretarias de carrera respondieron de la siguiente forma 50% dijo que no había disponibilidad del sistema, el 33% a la no disponibilidad de internet, el 17% no disponibilidad del sitio web. En lo que respecta a docentes la mayoría un 64% dijo que no había disponibilidad del sitio web, el 18% no había disponibilidad del sistema académico, un 9% no disponibilidad de internet y solo un 9% otro.

14.- ¿Con que frecuencia utiliza los servicios del Sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Una vez al semestre	21	Una vez al semestre	0	Una vez al semestre	0
Una vez al bimestre	61	Una vez al bimestre	0	Una vez al bimestre	0
una vez al mes	76	una vez al mes	0	una vez al mes	0
Una vez a la semana	102	Una vez a la semana	0	Una vez a la semana	3
Entre 2 a 5 veces por semana	60	Entre 2 a 5 veces por semana	16	Entre 2 a 5 veces por semana	29



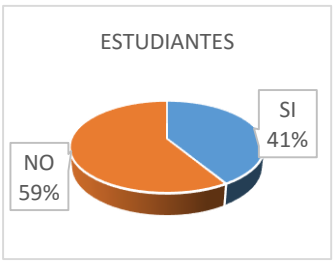


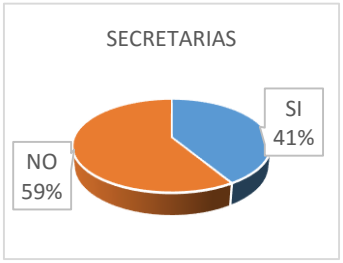


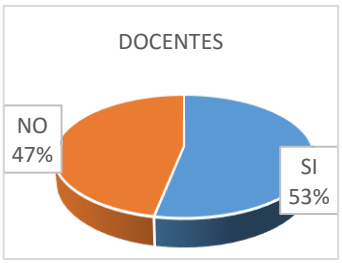
Análisis de resultados: De los datos recopilados acerca de la frecuencia de uso del sistema de gestión académica los estudiantes supieron manifestarse así: 32% lo utiliza una vez a la semana, el 24% una vez al mes, un 19% entre 2 a 5 veces por semana, con el mismo porcentaje del 19% hay estudiantes que utilizan una vez al bimestre, y un 6% lo utiliza una vez al semestre. En lo que respecta a secretarias de carrera el 100% respondió entre 2 a 5 veces por semana. Algo parecido sucedió con los docentes donde la mayoría con el 91% respondieron igual que las secretarias de carrera es decir que utilizan de 2 a 5 veces por semana y con un 9% una vez a la semana por lo que se deduce que tanto secretarias como docentes usan activamente el módulo de gestión académica.

15.- ¿Tiene la suficiente confianza como para presentar su queja sobre fallas en el sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	133	SI	11	SI	17
NO	189	NO	5	NO	15



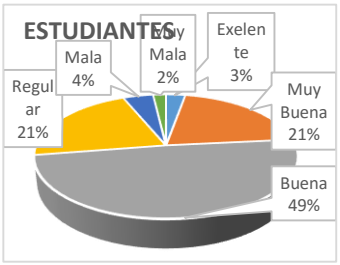


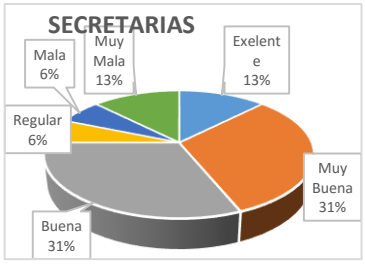


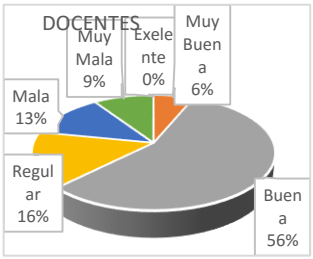
Análisis de resultados: De los datos recogidos en la encuesta sobre si tienen confianza para presentar su queja sobre fallas del sistema académico los estudiantes respondieron con el 59% que NO y el restante un 41% respondió que sí. Caso similar o igual se dio en las secretarias de facultad. De igual forma respondieron los docentes pero en un porcentaje menor el 47% dijo que NO, mientras que el 53% respondió que SI.

16.- ¿Cuál es la efectividad de los técnicos para resolver los problemas del sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Excelente	9	Excelente	2	Excelente	0
Muy Buena	66	Muy Buena	5	Muy Buena	2
Buena	157	Buena	5	Buena	18
Regular	68	Regular	1	Regular	5
Mala	14	Mala	1	Mala	4
Muy Mala	6	Muy Mala	2	Muy Mala	3



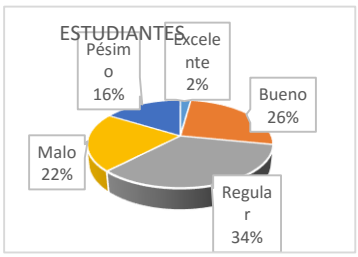


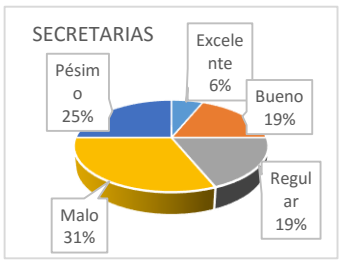


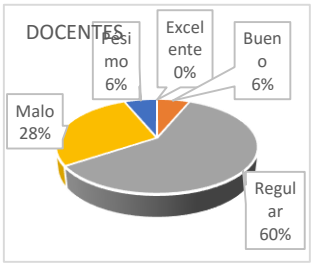
ANÁLISIS DE RESULTADOS: De acuerdo a los datos recogidos en lo que tiene que ver a la eficiencia para resolver problemas del sistema, los estudiantes respondieron así: el 49% piensa que es buena, el 21% muy buena, igual que Regular que está con el mismo porcentaje de 21%, el 4% dijo que era mala, el 3% excelente, un 2% muy mala. Mientras que las secretarias de carrera en un 31% dijeron que era buena, en igual porcentaje Muy buena, con el 13% excelente, igual con otro 13%muy mala, entre Regular y Mala tenemos el 6%. En lo que tiene que ver a docentes en cambio tenemos un 56% que cree que es buena con una mayoría, un 16% regular, un 9% muy mala y otro 6% muy buena.

17.- ¿Cómo califica el servicio de Internet en el campus universitario para utilizar los servicios del sistema de Gestión Académica?

ESTUDIANTES		SECRETARIAS		DOCENTES	
Excelente	7	Excelente	1	Excelente	0
Bueno	83	Bueno	3	Bueno	2
Regular	109	Regular	3	Regular	19
Malo	69	Malo	5	Malo	9
Pésimo	52	Pésimo	4	Pésimo	2



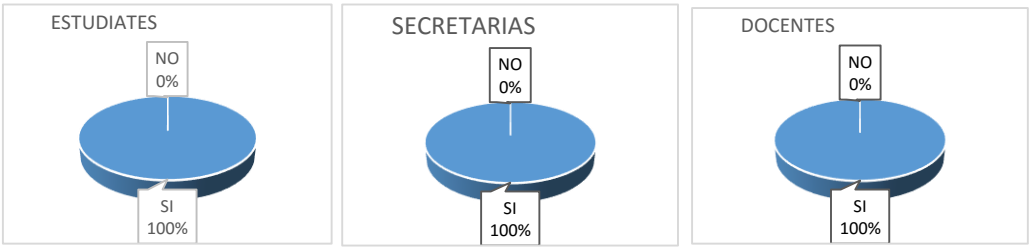




ANÁLISIS DE RESULTADOS: de acuerdo a los datos registrados de la encuesta con respecto al servicio de Internet en el campus universitario para la utilización del sistema de Gestión académica en lo que respecta a estudiantes el 34% cree que es regular, 26% dicen que es bueno, el 22% Malo, el 16% pésimo y el 2% excelente. Mientras las secretarias de facultad respondieron con el 31% que el servicio de internet es malo, el 25% respondieron que era pésimo, el 19% bueno otro 19% regular y un 6% cree que es excelente.

18.- ¿Considera que los servicios del sistema de Gestión Académica debe estar disponible a cualquier hora y para cualquier usuario?

ESTUDIANTES		SECRETARIAS		DOCENTES	
SI	302	SI	16	SI	32
NO	18	NO	0	NO	0



ANÁLISIS DE RESULTADOS: De acuerdo a los datos obtenidos acerca de que si consideran que los servicios de gestión Académica deben estar disponibles a cualquier hora en los tres estamentos de la universidad técnica del norte tanto estudiantes, secretarias y docentes con un 100%.

3.4 TÉCNICAS DE EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

3.4.1 Aplicación Normas ISO 27002:2013

3.4.1.1 Desarrollo de Políticas de Seguridad de la Información

El desarrollo de las políticas de Seguridad de la Información realizada en el departamento de sistemas de la Universidad Técnica del Norte, proviene de la recopilación de información, hallazgos y análisis de la situación actual del departamento basándonos en los controles de la ISO 27002:2013 correspondientes a los catorce dominios de la norma:

- Política de seguridad (1)
- Aspectos organizativos de la seguridad de la información (2)
- Seguridad ligada a los recursos humanos (2)
- Gestión de activos (3)
- Control de acceso (4)
- Cifrado (1)
- Seguridad física y ambiental (2)
- Seguridad en la operatividad (7)
- Seguridad en las telecomunicaciones (2)
- Adquisición, desarrollo y mantenimiento de sistemas de información(3)

- Relaciones con suministradores (2)
- Gestión de incidentes en la seguridad de la información (1)
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio (2)
- Cumplimiento (2)

3.4.2 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información (Magerit)

3.4.2.1 Gestión de riesgos

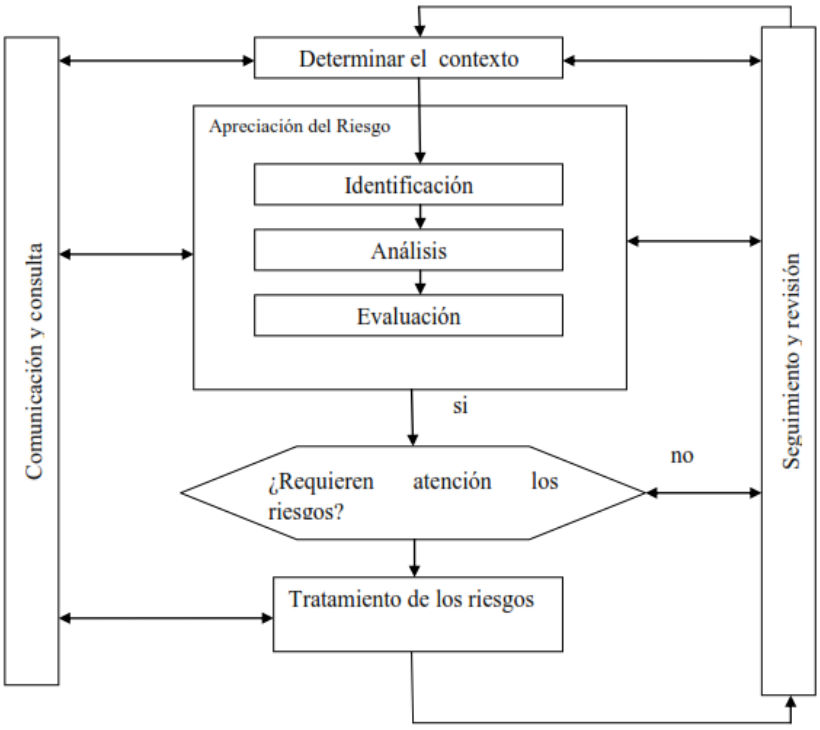


Figura 3.5: Proceso de gestión de riesgos

Fuente: (CCN-CERT, 2013)

Determinación del contexto: Lleva a una determinación de los parámetros y condicionantes externos e internos que permiten delimitar una política que se seguirá para gestionar los riesgos.

Identificación de los riesgos: Busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa.

Análisis de riesgos: Busca calificar los riesgos identificados, bien cuantificando sus consecuencias ya sean cuantitativamente o cualitativamente. De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

Evaluación de los riesgos: Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de que riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

Tratamiento de los riesgos: Recopila las actividades encaminadas a modificar la situación de riesgo.

Comunicación y consulta: Lo que se desea alcanzar un equilibrio entre la seguridad y productividad.

Seguimiento y revisión: Al finalizar el Análisis de Riesgos los resultados obtenidos del proyecto de tesis, es recomendable, poner en práctica lo recomendado para evitar incidentes dentro del entorno de la Universidad Técnica del Norte.

3.4.2.2 Análisis de riesgos

En la actualidad toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo, a un dominio o a toda su organización. Mediante del Análisis de Riesgos se deberán alcanzar los siguientes objetivos:

- Determinar los activos más significativos que posee el departamento de informática de la Universidad Técnica del Norte y la relación directa con el módulo de gestión académica
- Establecer las amenazas a las que están expuestos cada activo.
- Escoger salvaguardas apropiadas para los activos.
- Estimar el impacto si se materializara alguna amenaza.

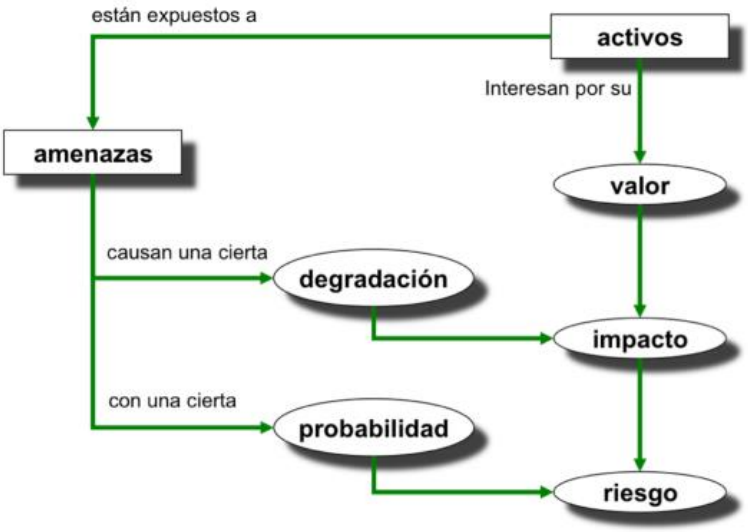


Figura 3.6: Elementos del análisis de riesgos potenciales

Fuente: (CCN-CERT, 2013)

Para la ejecución de esta fase, la recolección 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.

Mediante el análisis de riesgos se puede saber cuánto vale y como están protegidos los activos evaluándolos de manera metódica para obtener conclusiones con fundamento.

3.4.3 Procedimiento Informático Lógico para el análisis de riesgos (Pilar)

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" (EAR / PILAR, 2014), es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología Magerit.

Esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- 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.

Este software permite hacer un Análisis de Riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema. (CCN-CERT, 2012). PILAR puede hacer análisis cuantitativo y cualitativo.

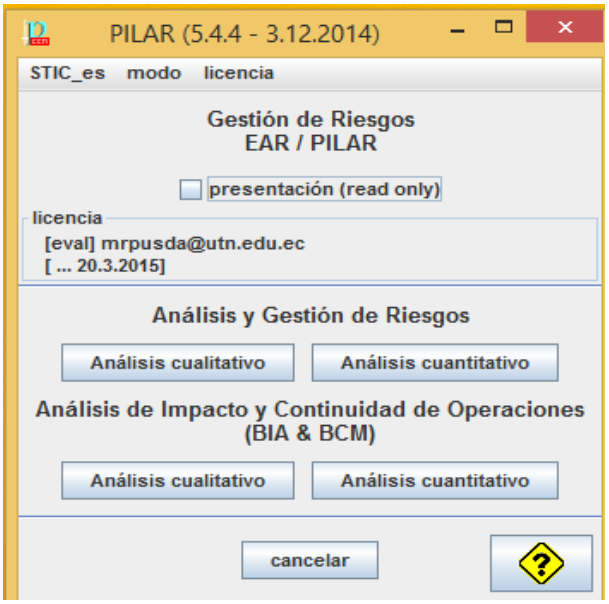


Figura 3.7: Pantalla Principal Pilar

Fuente: (EAR / PILAR, 2014)

3.4.3.1 Determinación de Activos

Listado de activos clasificados por su función con el Módulo de Gestión Académica

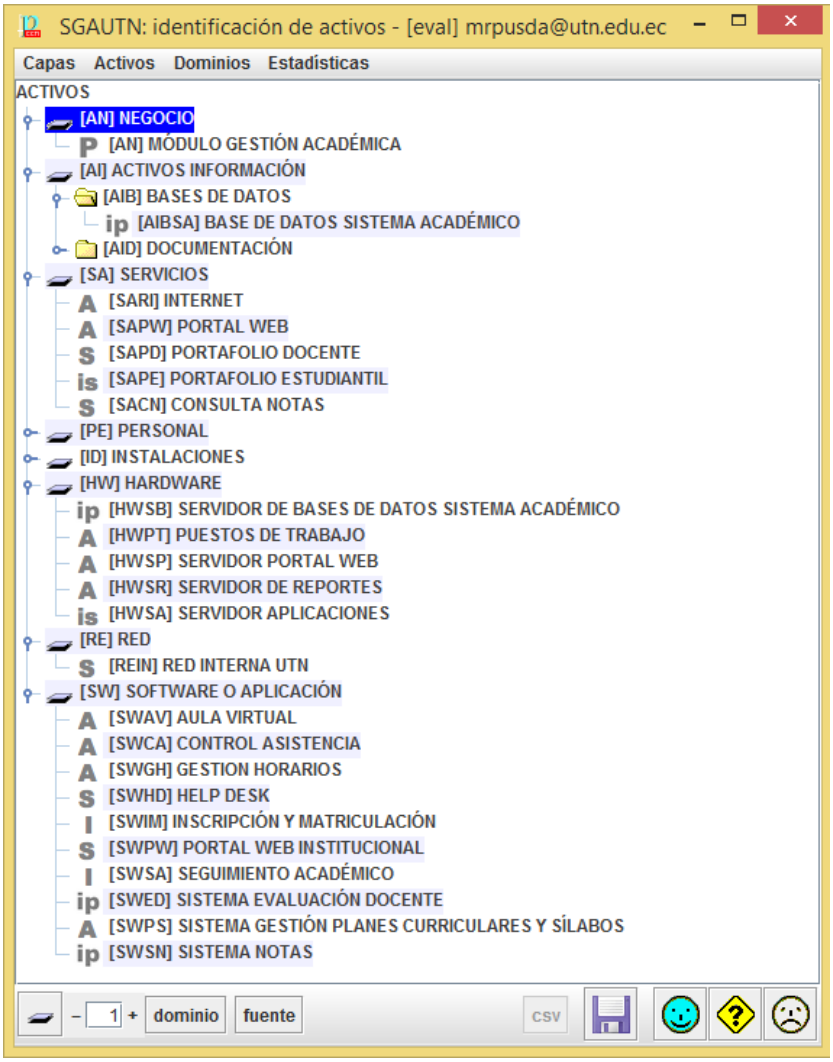


Figura 3.8: Listado de Activos Módulo Gestión Académica

3.4.3.2 Dependencias entre Activos

Relaciones entre activos principales del Módulo de Gestión Académica

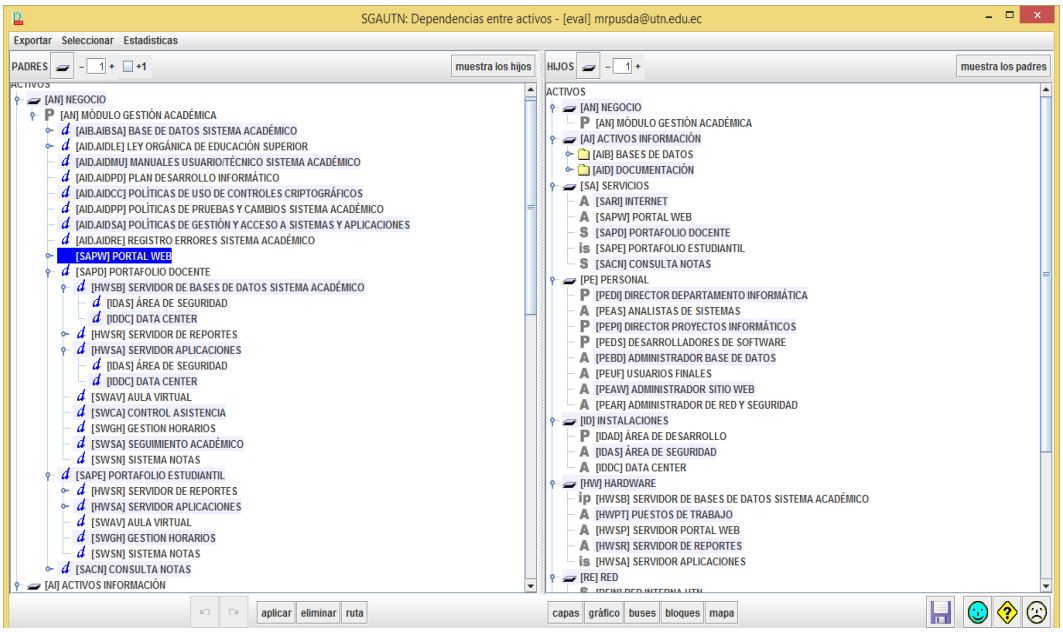


Figura 3.9: Dependencias Activos Módulo Gestión Académica

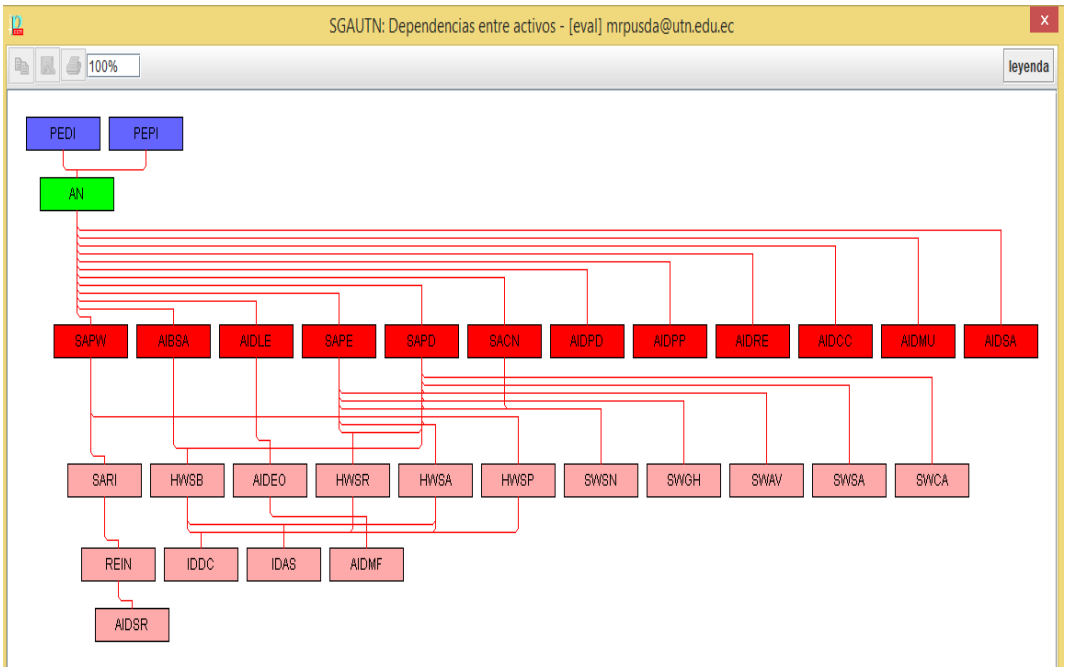


Figura 3.10: Mapa Dependencias Activos Módulo Gestión Académica

3.4.3.3 Valoración de Activos

Criterios de valoración entre activos del Módulo de Gestión Académica

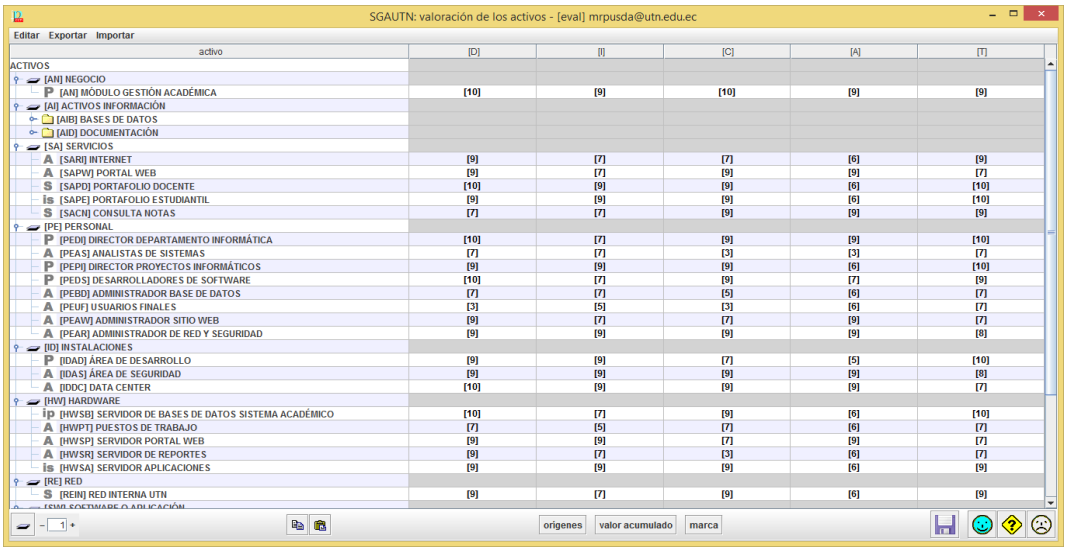


Figura 3.11: Valoración Activos Módulo Gestión Académica

3.4.3.4 Identificación de Amenazas

Recomendaciones de Pilar asociadas a cada uno de los Activos del Módulo de Gestión Académica

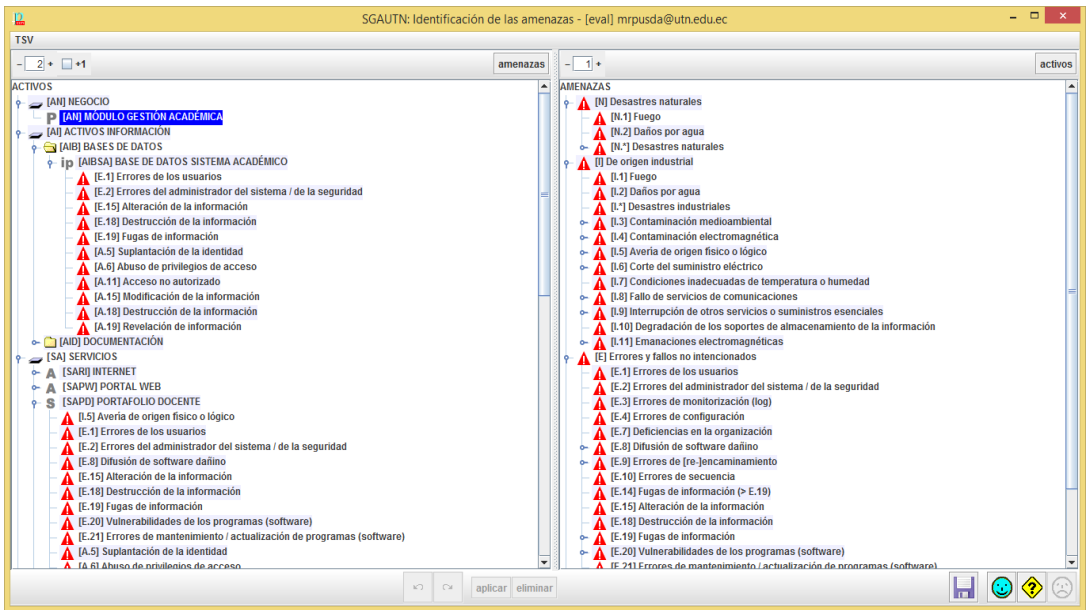


Figura 3.12: Amenazas Módulo Gestión Académica

3.4.3.5 Valoración de Amenazas

Porcentajes de valoración recomendados por Pilar para los Activos del Módulo de Gestión Académica

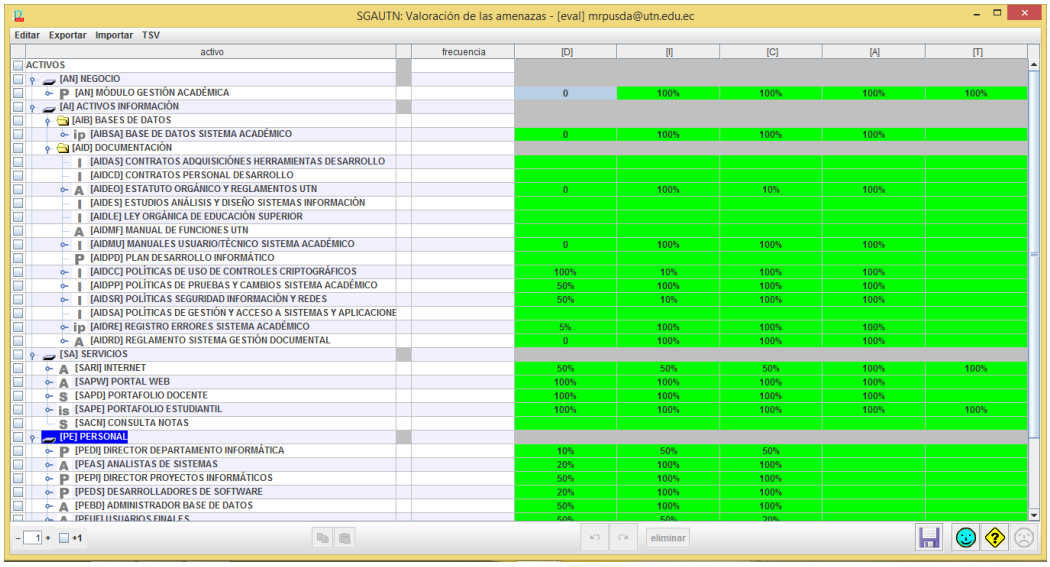


Figura 3.13: Valoración Amenazas Módulo Gestión Académica

3.4.3.6 Impacto Acumulado

Impacto evaluado en los Activos del Módulo de Gestión Académica

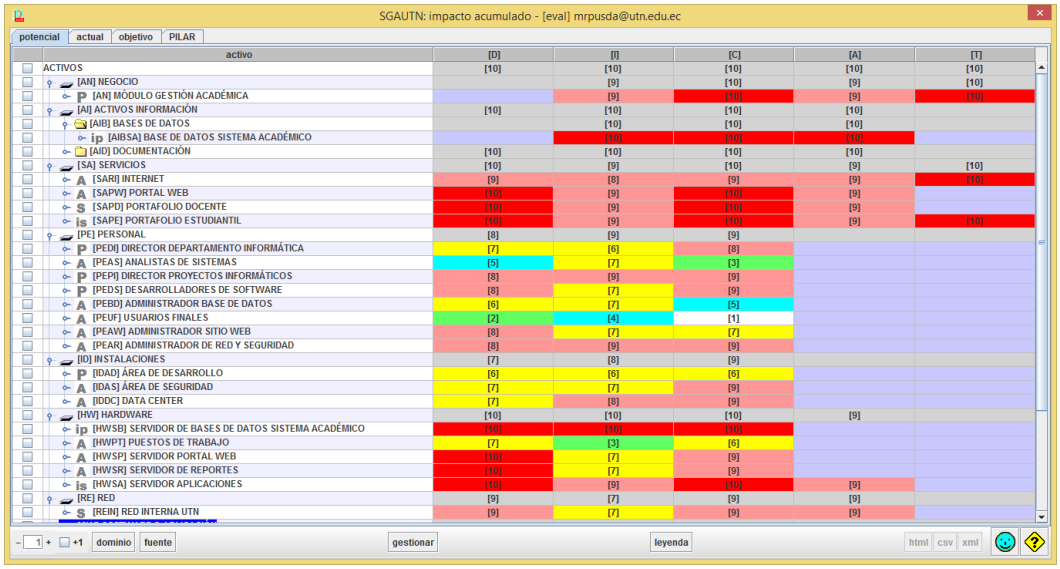


Figura 3.14: Impacto Acumulado Módulo Gestión Académica

3.4.3.7 Riesgo Acumulado

Riesgo Acumulado en los Activos del Módulo de Gestión Académica

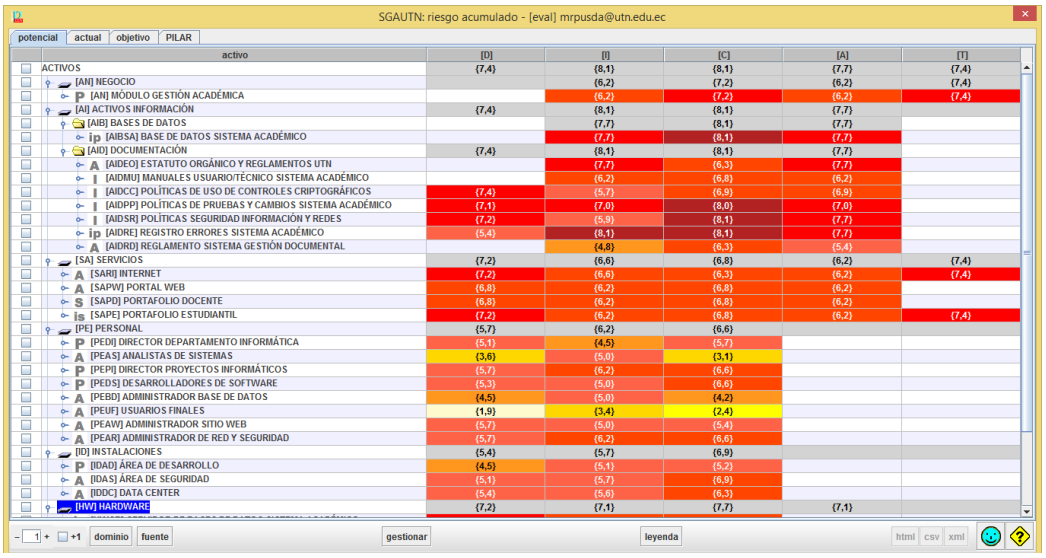


Figura 3.15: Riesgo Acumulado Módulo Gestión Académica

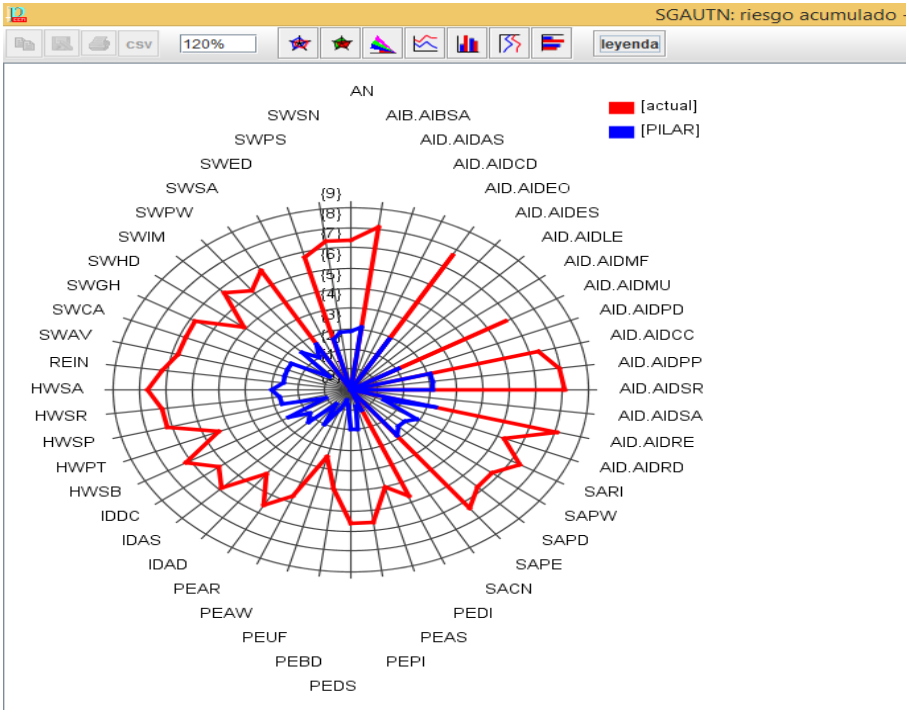


Figura 3.16: Situación Actual Riesgo Acumulado Módulo Gestión Académica

CAPÍTULO IV.- RESULTADOS

4.1 INFORME DE RESULTADOS

4.1.1 Introducción

Durante el desarrollo de este trabajo es el momento de evaluar el cumplimiento de la empresa en materia de seguridad de la información del módulo de gestión académica de la Universidad Técnica del Norte. La ISO/IEC 27002:2013 nos proporcionará un marco de control del estado de la seguridad. Durante el desarrollo de este trabajo se han llevado a cabo la identificación de la situación actual para identificar las vulnerabilidades y amenazas para identificar las deficiencias y las oportunidades de mejora.

4.1.2 Evaluación de cumplimiento

Este apartado incluye la evaluación del cumplimiento de los controles que contiene la norma ISO/IEC 27002:2013, tomados en cuenta para el módulo de gestión académica y la identificación del estado de madurez basándonos en el estándar de Cobit 5.0. Esta información mostrará las evidencias del cumplimiento de la norma

Tabla 4.1

Verificación de Cumplimiento Controles ISO 27002:2013.

DOMINIO	OBJETIVOS DE CONTROL	CONTROLES	OBSERVACIÓN	MADUREZ	CUMPLE
Políticas de Seguridad de la información	Directrices de la dirección en seguridad de la información	Conjunto de políticas para la seguridad dela información	• Existen tesis de grado que incluyen políticas y procedimientos • En el plan de desarrollo informático de la UTN 2013 -2017 se detalla tanto políticas como procedimientos aprobados por la Dirección del Departamento de Informática pero sin aprobación del HCU	Previsible	SÍ
		Revisión de las políticas para la seguridad de la información	• No existen procedimientos para la revisión de las políticas de seguridad de la información	Incompleto	NO
Organización de seguridad de la información	Organización interna	Asignación de responsabilidades para la seguridad de la información	• Todo el personal del Área de desarrollo realiza varias actividades sin dar cumplimiento al manual de funciones	Incompleto	NO
		Segregación de tareas	• Las tareas se asignan de acuerdo a la planificación y se evidencia en el Sistema Integrado Informático Universitario en el módulo de gestión por procesos	Optimizado	SI
		Contacto con las autoridades	• Las comunicaciones con las autoridades se realizan a través de la plataforma Quipux previamente autorizadas por el CIO	Previsible	SÍ

CONTINÚA →

		Contacto de interés especial	• Existen relaciones con proveedores nacionales e internacionales aunque ninguno de especial relevancia en cuestiones de seguridad de la información	Incompleto	NO
Seguridad en los recursos humanos	Antes de la contratación	Investigación de antecedentes	• Antes de realizar las contrataciones se solicita la respectivas hojas de vida, con todos los documentos habilitantes	Previsible	SI
		Términos y condiciones de contratación	• Existe documentos de llamamiento a concurso, no existe un documento descriptivo de las funciones y responsabilidades tanto para el desarrollo del módulo de gestión académica como para la seguridad de la información	Realizado	NO
	Durante la contratación	Responsabilidades de gestión	• En el manual de funciones existe la definición de responsabilidades	Previsible	SÍ
		Concienciación, educación y capacitación en seguridad de la información	• No se realiza estas actividades relacionadas con la seguridad de la información. • Existe un protocolo (no documentado) de capacitación de forma general a los nuevos empleados	Incompleto	NO
		Proceso Disciplinario	• No existe un proceso disciplinario formal y claro para los empleados que hayan provocado violaciones a la seguridad de la información	Incompleto	NO
	Cese o cambio del puesto de trabajo	Cese o cambio de puesto de trabajo	• No existe documentación relacionada con los cambios del personal.	Incompleto	NO

CONTINÚA 

Gestión de activos	Responsabilidades sobre los activos	Inventario de activos	• Existe sistematizado el inventario de equipos, servidores y dispositivos de toda la universidad en el módulo de activos fijos	Optimizado	SÍ
		Propiedad de los activos	• No existe registro de propietarios, existe responsables de los activos en el módulo de activos fijos y un manual de responsabilidades	Establecido	SÍ
		Devolución de activos	• No existe documentado procedimiento para las devoluciones, las mismas se registran de forma genérica en el módulo de activos fijos	Establecido	SÍ
Control de accesos	Requisitos del negocio para el control de accesos	Política de control de accesos	• No existen documentadas políticas de control de acceso al módulo de gestión académica, se considera una tesis de grado sobre sistema de gestión de seguridad	Realizado	NO
		Control de acceso a las redes y asociados	• No existe documentado las políticas sobre control de acceso a las redes, existe un monitoreo permanente de la red	Realizado	NO
	Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios	• No existe documentado los procedimientos, se utiliza el módulo de auditoría, la actualización y revisión es permanente	Previsible	SÍ
		Gestión de los derechos de acceso asignados a usuarios	• Se gestiona mediante el módulo de seguridad, la administración la gestiona el administrador de Red	Realizado	NO

CONTINÚA →

	Gestión de información confidencial de autentificación de usuarios	• No existe documentación relacionada con políticas y procedimientos de confidencialidad	Incompleto	NO
	Gestión de información confidencial de autentificación de usuarios	• No existe documentación relacionada con políticas y procedimientos de confidencialidad	Incompleto	NO
	Revisión de los derechos de acceso de los usuarios	• Existe revisión de acceso de empleados que renuncian más no del resto de usuarios del módulo de gestión académica. • Se revisan los accesos en caso de error, anomalía o incidencia	Realizado	NO
Responsabilidades del usuario	Uso de la información confidencial para la autentificación	• No existe documentado, el procedimiento se lo realiza mediante la configuración directa de la base de datos	Incompleto	NO
Control de acceso a sistemas y aplicaciones	Procedimientos seguros de inicio de sesión	• No existe documentación, se trabaja mediante la configuración de la base de datos, se acepta 3 intentos antes de bloquearse el usuario	Realizado	NO
	Gestión de contraseñas de usuario	• No existe documentación, se trabaja según la configuración de la base de datos	Gestionado	NO
	Control de acceso al código fuente	• No existe documentación, la gestión se realiza de tal manera que solo los usuarios autorizados tienen acceso al código fuente, se realiza registro de cambios	Previsible	SÍ

CONTINÚA

Cifrado	Controles criptográficos	Políticas de uso de los controles criptográficos	• No existe una política formal sobre el uso de controles criptográficos en el módulo de gestión académica • Existe documentado en el sistema de gestión de procesos	Gestionado	NO
		Gestión de claves	• No existe política formal de gestión y uso de claves que permitan generar y almacenar certificados de seguridad • El módulo de gestión académica tiene implementado la gestión de claves directamente desde la base de datos en base a su configuración	Realizado	NO
Seguridad física y ambiental	Áreas seguras	Perímetro de seguridad física	• Existe señalización ética del departamento de informática y el área de desarrollo. No se cuenta con señalamiento de rutas de evacuación	Establecido	SÍ
		Controles físicos de entrada	• Existe control biométrico y reportes de entrada y salida	Establecido	SÍ
		Protección contra las amenazas externas y ambientales	• No existe documentación de políticas y procedimientos	Incompleto	NO
	Seguridad de los equipos	Emplazamiento y protección de equipos	• No existe diagrama de instalaciones. no existe políticas de seguridad respecto al uso de alimentos, líquidos o cualquier sustancia que dañe los equipos.se tiene delimitado las áreas de trabajo	Incompleto	NO
		Instalaciones de suministro	• No existen diagramas de las instalaciones de suministro. Las instalaciones del departamento de informática están protegidas ante fallos. no existe un sistema de suministro redundante que asegure el funcionamiento y la continuidad operativa	Realizado	NO

CONTINÚA →

Seguridad de las operaciones		Seguridad del cableado.	• El cableado eléctrico y de comunicaciones está protegido ante daños y el acceso es restringido solo a personal autorizado	Previsible	SÍ
		Mantenimiento de los equipos.	• Se tiene adquirido herramientas para mantenimiento de equipos, los servidores y dispositivos del Datacenter tienen un mantenimiento adecuado, existe contratos con proveedores externos para reparación en caso de fallas	Previsible	SÍ
	Responsabilidades y procedimientos de operación	Documentación de procedimientos de operación.	• Se toma como referencia dos tesis de pregrado realizadas. La mayoría de procedimientos de operaciones no están debidamente documentados y adaptados a las realidades de la Universidad	Establecido	SÍ
		Gestión de cambios.	• No existe documentación del proceso. Se lleva un control de cambios previamente autorizado. Se utiliza la plataforma Quipux para solicitar cambios requeridos por los usuarios	Establecido	SÍ
		Gestión de capacidades.	• Las funciones y tareas del personal del departamento de informática son asignadas de tal manera que se evite modificaciones no autorizadas	Establecido	SÍ
		Separación de entornos de desarrollo, prueba y producción.	• Las áreas de desarrollo y producción están debidamente separadas. No existe área ni procedimientos para la una área de pruebas, las mismas se realizan en cada uno de los ambientes de desarrollo de cada programador	Gestionado	SÍ
	Protección contra código malicioso	Controles contra el código malicioso.	• Todos los equipos del departamento de informática y área de desarrollo tienen instalado herramienta Eset-EndPoint corporativo. • Se cuenta con firewall para accesos a internet. • Los controles no están documentados.	Previsible	SÍ

CONTINÚA →

	Copias de seguridad.	Copias de seguridad de la información.	• Las copias de seguridad se realizan mediante tareas programadas a diario. • Los respaldos físicos se realizan periódicamente cada semestre. • No existe documentación de los procesos de copias de seguridad	Previsible	SÍ
	Registro de actividad y supervisión.	Registro y gestión de eventos de actividad.	• El departamento de informática desarrolló un Help Desk pero no está instalado para producción. No existe documentado procesos de gestión de eventos	Incompleto	NO
		Protección de los registros de información.	• Los registros de seguridad de los sistemas se protegen de forma adecuada de los accesos no autorizadas y de manipulaciones indebidas. No se revisan de forma frecuente.	Previsible	SI
	Control del software en explotación.	Instalación del software en sistemas en producción.	• Software utilizado para producción del módulo de gestión académica cuenta con las debidas licencias.	Optimizado	SI
	Gestión de la vulnerabilidad técnica.	Gestión de las vulnerabilidades técnicas.	• No existe procedimiento ni documentación para la gestión de vulnerabilidades. En caso de daños en hardware no cuentan con equipos y dispositivos backup.	Incompleto	NO
		Restricciones en la instalación de software.	• No existe procedimientos para sancionar al personal que instale software no permitido	Incompleto	NO
	Consideraciones de las auditorías de los sistemas de información.	Controles de auditoría de los sistemas de información.	• El control de auditoría del módulo de gestión académica se gestiona a través del sistema de auditoría. La documentación del proceso esta detallada en una tesis de grado	Previsible	SÍ

CONTINÚA →

Seguridad en las Telecomunicaciones	Gestión de seguridad en las Redes	Controles de red.	• Existe control por medio de portal cautivo para estudiantes, docentes y personal administrativo con filtrado MAC. • Ancho de banda segmentado. • Cuentan con firewall de red y sus configuraciones pero no cuentan con la documentación soporte	Previsible	SI
		Mecanismos de seguridad asociados a servicios de red	• Cuentan con mecanismos de seguridad controlados por Cisco ASA. • Cuentan con el procedimiento de forma empírica pero no se encuentra documentado.	Previsible	SI
		Segregación de Red	• La red se encuentra segmentada en diferentes vlans y cuentan con configuraciones detalladas en la guía de configuración.	Optimizado	SI
Adquisición desarrollo y mantenimiento de sistemas de información	Requisitos de seguridad de los sistemas de información.	Análisis y especificación de los requisitos de seguridad.	• El proceso se encuentra documentado en el manual de procedimientos del área de desarrollo. • Este documento está aprobado por la dirección de Informática, pero no por el HCU.	Previsible	SI
	Seguridad en los procesos de desarrollo y soporte.	Política de desarrollo de Software.	• Para el desarrollo del módulo de gestión académica se utiliza la metodología RUP, debidamente documentada	Optimizado	SI
		Procedimiento de control de cambios en los sistemas	• Los procedimientos de control de cambios se realizan en el módulo de Planificación del Sistema Integrado Informático Universitario • No existe documentado los procesos para el control de cambios.	Previsible	SI
	Datos de Prueba	Protección de los Datos utilizados en pruebas	• Los datos de prueba se realizan en cada ambiente de trabajo de los desarrolladores. • No existe documentación de los procedimientos de los datos de prueba antes de entrar en producción	Incompleto	NO

CONTINÚA →

Relación con suministradores	Seguridad de la información en la relación con suministradores.	Política de Seguridad de la Información para suministradores.	• Existen convenios con suministradores externos pero no existen procesos ni documentación	Establecido	NO
	Gestión de la prestación de Servicios por suministradores	Supervisión y revisión de los servicios prestados por terceros	• Existen contratos con proveedores externos que reposan en procuraduría • El proceso de contratación consta en el servicio e contratación pública. • Existe convenios con empresas relacionadas con temas educativos con respecto a licencias y actualización de software	Optimizado	SI
Gestión de incidentes en la seguridad de la información	Gestión de Incidentes de Seguridad de la información y mejoras	Responsabilidades y procedimientos	• Cuenta con software Help Desk pero no está en producción • No cuentan con procedimientos para el reporte incidentes.	Incompleto	NO
		Notificación de los eventos de seguridad de la Información.	• No se verifican los eventos ni hay un control de incidentes. Se utiliza Quipux para registro de incidentes. • No se cuenta con respuesta sobre evidencia de errores del sistema. • No existe recopilación de errores por cada aplicación que son parte del módulo de gestión académica.	Realizado	NO
		Respuesta a los incidentes de seguridad.	• La respuesta a incidentes se realiza con los registros de Quipux debidamente autorizados por la dirección de informática, no existe documentación del proceso para la respuesta a los incidentes	Establecido	SI
		Recopilación de evidencias	• En caso de incidentes de seguridad el área de desarrollo realiza la recopilación de evidencias mediante la plataforma Quipux.	Realizado	NO

CONTINÚA →

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.	• El departamento de informática y el área de desarrollo cuenta con una planificación de continuidad a baja escala, sin analizar grandes catástrofes, daños y sin incluir la seguridad de la información • La gestión de Continuidad lo realizan de manera empírica, no cuentan con documentación • El personal de backup se lleva de manera informal.	Realizado	NO
	Redundancias	Disponibilidad de instalaciones para el procesamiento de la información.	• No se cuenta con la infraestructura necesaria para brindar un servicio de Alta Disponibilidad 24-7.	Incompleto	NO
Cumplimiento	Cumplimiento de los requisitos legales y contractuales	Identificación de la Legislación aplicable	• Se aplica la Ley de Educación Superior y el Reglamento Interno de la Universidad Técnica del Norte.	Optimizado	SI
		Derechos de propiedad intelectual	• En cada una de las tesis desarrolladas en el Departamento de Informática se hace una sesión de derechos a la universidad.	Previsible	SI
		Protección de datos y privacidad de la información personal	• El departamento de informática no cuenta con ningún documento de confidencialidad de la información.	Incompleto	NO

4.1.3 Evaluación de Resultados

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

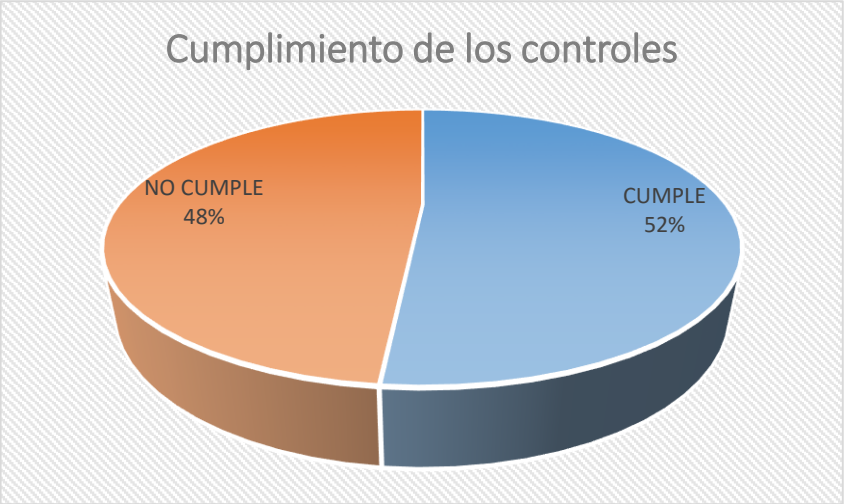


Figura 4.1: Cumplimiento de los Controles ISO/IEC 27002:2013

Una vez determinado los controles considerados importantes en 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) de Cobit 5.0

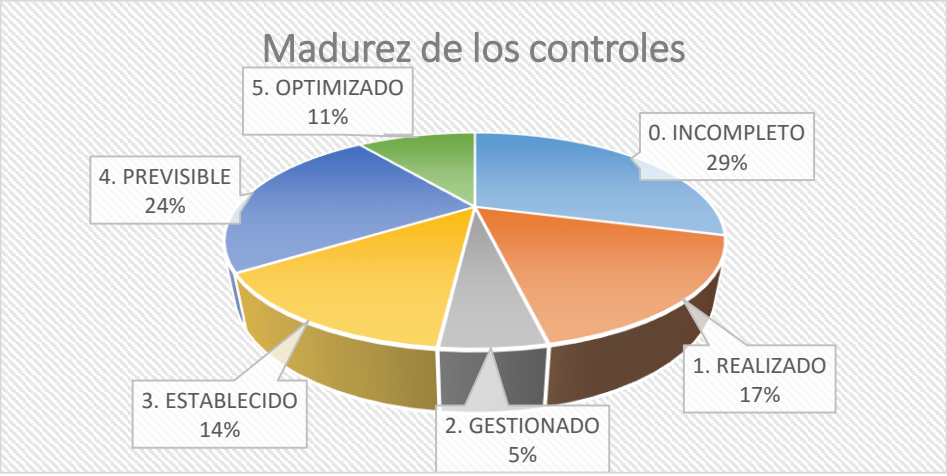


Figura 4.2: Madurez Controles ISO/IEC 27002:2013

4.1.4 Activos de Información

En la actualidad la Dirección de Desarrollo Tecnológico e informática de la Universidad Técnica del Norte, cuenta con los siguientes activos de información e infraestructura tecnológica.

4.1.5 Servidores y Equipo de Datos

- La Institución cuenta con servidores
- Un equipo de seguridad perimetral firewall un CISCO ASA
- 49 Zonas de acceso inalámbrico con potencia media integrados LAN CONTROLER
- Redes de comunicación Internet
- 88 switches de red
- 1 router principal que pertenece al ISP

4.1.6 Sistemas de Comunicación y Voz

- La Institución cuenta con una central VoIP con un total de 213 extensiones distribuidas en el campus universitario

4.1.7 Sistemas de Seguridad, Prevención y Control de Acceso

- Cámaras de seguridad
- Alarmas
- Extintores
- Lectores Biométricos

4.1.8 Equipos de Cómputo

- El Departamento de Desarrollo Tecnológico e informático cuenta con 700 equipos de cómputo.

4.1.9 Diagrama de la Red

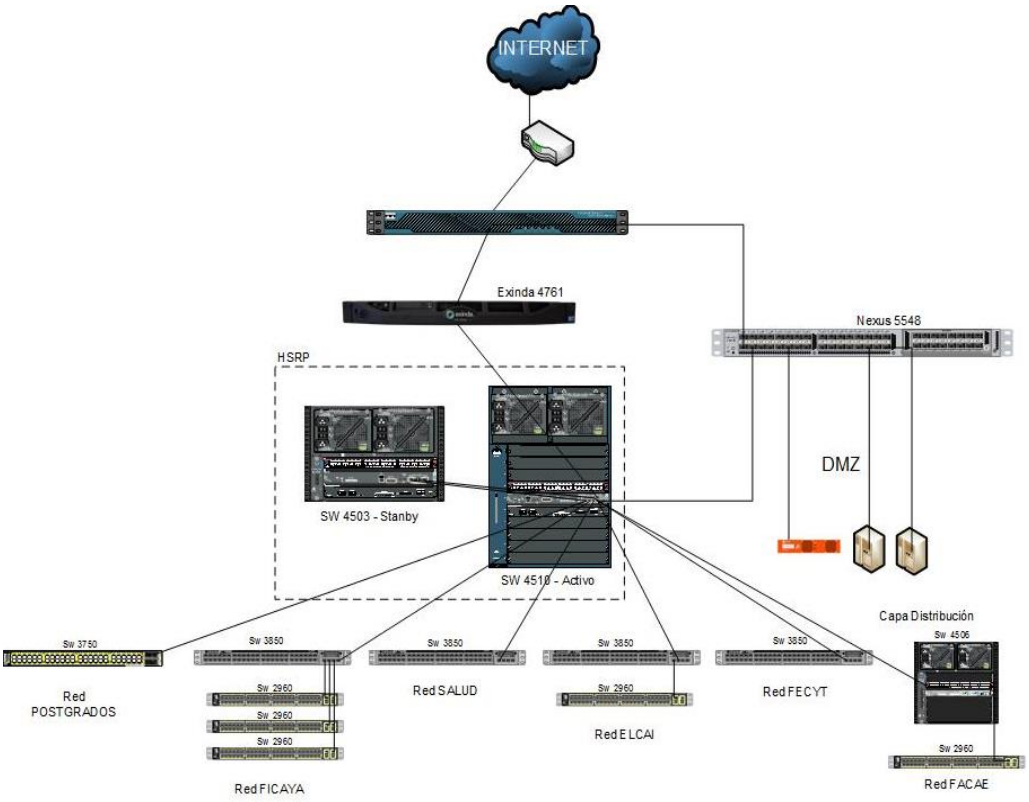


Figura 4.3: Diagrama RED UTN.

Fuente: (Departamento Informática UTN, 2013)

4.2 INFORME DE EJECUCIÓN

4.2.1 No conformidades y Observaciones

Tabla 4.2

No Conformidades y Observaciones.

CÓDIGO	CONTROLES	OBSERVACIÓN	NO CONFORMIDAD	RECOMENDACIÓN
5.1.2	Revisión de las políticas para la seguridad de la información	• No existen procedimientos para la revisión de las políticas de seguridad de la información	• La documentación que se encuentra en las tesis no se han actualizado y en algunas situaciones no se ha puesto en funcionamiento	• Designar personal que se dedique a la revisión y actualización de las políticas de seguridad de la información
6.1.1	Asignación de responsabilidades para la seguridad de la información	• Todo el personal del Área de desarrollo realiza varias actividades sin dar cumplimiento al manual de funciones	• No existe personal con dedicación completa al análisis de sistemas, los desarrolladores realizan la actividad de analistas	• Contratar o asignar personal de análisis de sistemas para el Área de desarrollo
6.1.4	Contacto de grupos de interés especial	• Existen relaciones con proveedores nacionales e internacionales aunque ninguno de especial relevancia en cuestiones de seguridad de la información	• No se evidencian contactos con grupos especializados con la seguridad de la información	• Establecer contactos con grupos relacionados con la seguridad de la información, mediante foros, boletines de noticias
7.1.2	Términos y condiciones de contratación	• Existe documentos de llamamiento a concurso, no existe un documento descriptivo de las funciones y responsabilidades tanto para el desarrollo del módulo de gestión académica como para la seguridad de la información	• Aunque el proceso de contratación está bien identificado, no existe la especificación de los términos y condiciones mediante las cuales el empleado elaborará en el Área de Programación	• Definir los términos y condiciones de contratación para las diferentes actividades del Área de Programación

CONTINÚA →

7.2.2	Concienciación, educación y capacitación en seguridad de la información	• No se realiza estas actividades relacionadas con la seguridad de la información	• No se identifican evidencias de la concienciación, educación y capacitación de los empleados respecto a la seguridad de la información	• Elaborar un plan de capacitación respecto a la seguridad de la información y generar evidencias de la implementación del mismo
7.2.3	Proceso Disciplinario	• No existe un proceso disciplinario formal y claro para los empleados que hayan provocado violaciones a la seguridad de la información	• No se evidencia el proceso disciplinario formal para los empleados relacionados con el módulo de gestión académica que hayan provocado alguna violación de seguridad de la información	• Elaborar el proceso disciplinario en caso de incumplimiento de las normas y políticas de seguridad. • Recopilar evidencias
7.3.1	Cese o cambio de puesto de trabajo	• No existe documentación relacionada con los cambios del personal del Área de Programación o personal relacionado con el módulo de gestión académica	• No se identifican evidencias de los cambios de personal del Área de Programación debidamente autorizados	• Elaborar un plan de cese o cambios de personal relacionado con el módulo de gestión académica • Recopilar evidencias debidamente autorizadas por el CIO
• **8. No se identifican no conformidades en este dominio**				
9.1.1	Política de control de accesos	• No existen documentadas políticas de control de acceso al módulo de gestión académica, se considera una tesis de grado sobre sistema de gestión de seguridad	• No se evidencia las políticas de control de acceso exclusivamente para el módulo de gestión académica, la información de la tesis de grado no es aplicad de manera formal	• Actualizar y adaptar las políticas de control de acceso exclusivamente para el módulo de gestión académica

CONTINÚA →

9.1.2	Control de acceso a las redes y asociados	• No existe documentado las políticas sobre control de acceso a las redes, existe un monitoreo permanente de la red	• No se identifican evidencias del control de acceso a las redes, para determinar si está controlado técnicamente	• Realizar un plan de acceso a las redes y asociados para tener un control técnico y eficiente
9.2.4	Gestión de información confidencial de autentificación de usuarios	• No existe documentación relacionada con políticas y procedimientos de confidencialidad	• No hay evidencias de acuerdos de confidencialidad sobre la información de los usuarios	• Realizar acuerdos de confidencialidad en donde se acepte y firme la responsabilidad el empleado y el CIO • Los acuerdos deben revisarse periódicamente
9.2.5	Revisión de los derechos de acceso de los usuarios	• Existe revisión de acceso de empleados que renuncian más no del resto de usuarios del módulo de gestión académica. • Se revisan los accesos en caso de error, anomalía o incidencia	• No hay documentación formal de revisión de derechos de acceso de usuarios por parte del administrador del módulo de gestión académica.	• Establecer un proceso formal, al menos semestral, de revisión de derechos de acceso al módulo de gestión académica
9.3.1	Uso de la información confidencial para la autentificación	• No existe documentado, el procedimiento se lo realiza mediante la configuración directa de la base de datos	• No existe una guía de recomendaciones sobre la autentificación y su confidencialidad para los usuarios del módulo de gestión académica	• Elaborar una guía de recomendaciones y socializar a todos los usuarios del módulo de gestión académica
9.4.2	Procedimientos seguros de inicio de sesión	• No existe documentación, se trabaja mediante la configuración de la base de datos, se acepta 3 intentos antes de bloquearse el usuario	• No se establecen mecanismos técnicos de inicio de sesión seguro, no se muestra un aviso de número de intentos y proceso para desbloquear usuarios	• Elaborar una guía de inicios de sesión y desbloqueo, para los usuarios del módulo de gestión académica

CONTINÚA →

9.4.3	Gestión de contraseñas de usuario	• No existe documentación, se trabaja según la configuración de la base de datos	• No existe política formal sobre la gestión de contraseñas de usuario para los usuarios del módulo de gestión académica	• Documentar una política para la gestión de contraseñas de usuarios del módulo de gestión académica • Firmar cláusulas de confidencialidad de contraseñas
10.1.1	Políticas de uso de los controles criptográficos	• No existe una política formal sobre el uso de controles criptográficos en el módulo de gestión académica • Existe documentado en el sistema de gestión de procesos	• No existe política del uso de controles criptográficos, aunque se evidencia el uso de esta tecnología en algunas aplicaciones que son parte del módulo de gestión académica	• Identificar y seleccionar una tecnología criptográfica actualizada • Establecer una política formal sobre el uso de controles criptográficos
10.1.2	Gestión de claves	• No existe política formal de gestión y uso de claves que permitan generar y almacenar certificados de seguridad • El módulo de gestión académica tiene implementado la gestión de claves directamente desde la base de datos en base a su configuración	• Como no existe política de uso de técnicas criptográficas tampoco existe una política clara y formal para la gestión de claves	• Establecer una política clara y formal para la gestión de claves del módulo de gestión académica
11.2.1	Emplazamiento y protección de equipos	• Los equipos del Área de programación están desprotegido respecto al uso de alimentos, líquidos o cualquier sustancia que dañe los mismos. • Se tiene delimitado las áreas de trabajo y los quipos están ubicados adecuadamente	• No existe política de seguridad de equipos en lo que respecta a protección de los mismos en especial al uso de alimentos o sustancias que puedan dañarlos	• Establecer una política de uso de alimentos, líquidos y sustancias que dañen equipos informáticos del Área de Desarrollo

CONTINÚA →

11.2.2	Instalaciones de suministro	• No existen diagramas de las instalaciones de suministro. • No existe un sistema de suministro redundante que asegure el funcionamiento y la continuidad operativa • Las instalaciones del departamento de informática están protegidas ante fallos leves	• No existe evidencia sobre instalaciones de protección ante fallas • No existe documentación de un sistema redundante que asegure el funcionamiento y la continuidad operativa en caso de fallas eléctricas	• Realizar una guía de las instalaciones se suministros de todos los equipos del departamento de informática y del área de programación • Realizar un plan de redundancia en caso de fallas eléctricas
12.4.1	Registro y gestión de eventos de actividad.	• El departamento de informática desarrolló un Help Desk pero no está instalado para producción. • No existe documentado procesos de gestión de eventos • Se recopila evidencias de incidentes de seguridad por medio de la plataforma Quipux	• No existe planificación de implementación del Help Desk • No existe documentación formal sobre notificaciones de incidentes • No se realizan un análisis de los incidentes para determinar el coste y como evitarlo en el futuro	• Poner en productividad la herramienta de software Help Desk para la gestión de incidencias relacionadas con el módulo de gestión académica • Comunicar a los usuarios del módulo de gestión académica el objetivo y función de la notificación de incidencias de seguridad • Establecer un procedimiento de gestión de incidentes(evaluación de costes, mejora continua) • Establecer un procedimiento de recopilación de evidencias sobre incidentes de seguridad de la información

CONTINÚA →

12.6.1	Gestión de las vulnerabilidades técnicas.	• El departamento de informática y el área de programación realiza la gestión de vulnerabilidades técnicas en cuanto a los sistemas operativos • En caso de daños en hardware no cuentan con equipos y dispositivos backup.	• No existe procedimiento ni documentación para la gestión de vulnerabilidades de las aplicaciones del módulo de gestión académica	• Establecer un procedimiento para la gestión de vulnerabilidades de todas las aplicaciones, equipos y servicios del módulo de gestión académica
12.6.2	Restricciones en la instalación de software.	• No existe procedimientos para sancionar al personal que instale software no permitido	• No existe política para el control de instalación de software en los equipos del área de desarrollo	• Establecer un proceso formal de instalación de software por parte de la dirección del Departamento de Informática
14.3.1	Protección de los Datos utilizados en pruebas	• Los datos de prueba se realizan en cada ambiente de trabajo de los desarrolladores. • No existe documentación de los procedimientos de los datos de prueba antes de entrar en producción	• Los datos de prueba se tratan de igual manera que los datos reales • No existe procedimiento para la protección de datos de pruebas	• Establecer un procedimiento para los datos de prueba, de tal manera que no estén accesibles a personal no autorizadas • Tomar medidas especiales de protección (borrado tras uso, pruebas de auditoría, entre otros)
15.1.1	Política de Seguridad de la Información para suministradores.	• Existen convenios con suministradores externos pero no existen procesos ni documentación	• No existen políticas de seguridad de la información para suministradores	• Establecer un política formal sobre la seguridad de información para suministradores

CONTINÚA 

16.1.1	Responsabilidades y procedimientos	• El departamento de informática y el área de desarrollo cuenta con un esquema informal de responsabilidades y procedimientos para la gestión de incidentes de seguridad de la información	• Cuenta con software Help Desk pero no está en producción • No cuentan con procedimientos para el reporte incidentes de seguridad de información.	• Establecer una política formal de responsabilidades y procedimientos para la gestión de incidentes de la seguridad de la información
16.1.2	Notificación de los eventos de seguridad de la Información.	• No se verifican los eventos, no hay un control de incidentes. • No se cuenta con respuesta sobre evidencias de errores del sistema. • Se utiliza Quipux para registro de incidentes.	• No existe documentación sobre gestión de incidencias • No se notifica a los usuarios sobre la importancia de la notificación de incidencias	• Establecer un procedimiento formal para la gestión y documentación de incidencias • Socializar a los usuarios sobre la importancia de la notificación de eventos de seguridad de la información
16.1.7	Recopilación de evidencias	• En caso de incidentes de seguridad el área de desarrollo realiza la recopilación de evidencias mediante la plataforma Quipux.	• No existe procedimiento alguno de recopilación de evidencias en caso de incidentes de seguridad que implique acciones legales	• Establecer un procedimiento de recopilación de evidencias. • Designar personal debidamente capacitado y experimentado en seguridad de información
17.1.1	Planificación de la continuidad de la seguridad de la información.	• El departamento de informática y el área de desarrollo cuenta con una planificación de continuidad a baja escala, sin analizar grandes catástrofes, daños y sin incluir la seguridad de la información • La gestión de Continuidad lo realizan de manera empírica, no cuentan con documentación • El personal de backup de igual forma se lleva de manera informal.	• No existe gestión de continuidad del negocio, del módulo de gestión académica, con algún tipo de plan o procedimiento	• Elaborar un proyecto de implantación de la gestión de continuidad del negocio y de la seguridad de información

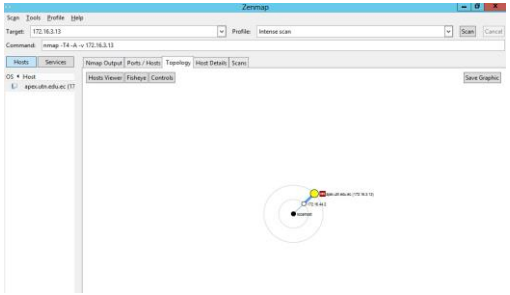
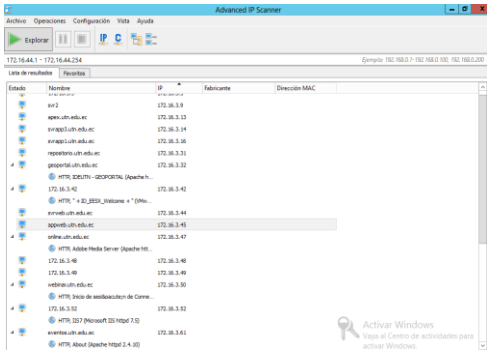
CONTINÚA 

17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	• No se cuenta con la infraestructura redundante necesaria para brindar un servicio de Alta Disponibilidad 24-7.	• No existe plan o procedimiento para asegurar el funcionamiento y la continuidad operativa del módulo de gestión académica	• Elaborar un plan de un sistema redundante para el módulo d gestión académica • Asignar recursos económicos para un sistema redundante fuera de las instalaciones de la Universidad Técnica del Norte
18.2.2	Protección de datos y privacidad de la información personal	• El departamento de informática no cuenta con ningún documento de confidencialidad de la información.	• No existe políticas de protección de datos y privacidad de la información personal	• Elaborar políticas y procedimientos sobre la protección y privacidad de la información personal

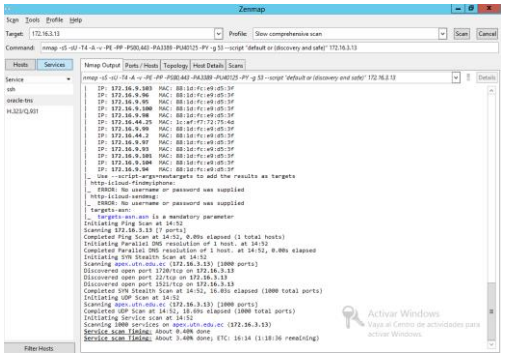
4.2.2 Evaluación de Vulnerabilidades

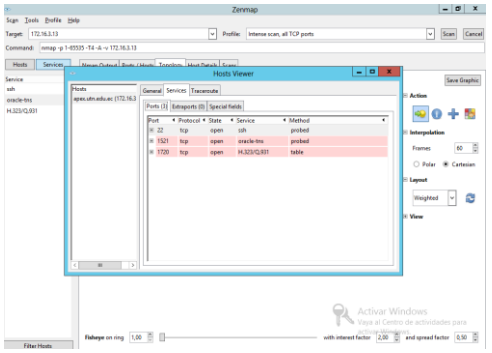
Tabla 4.3

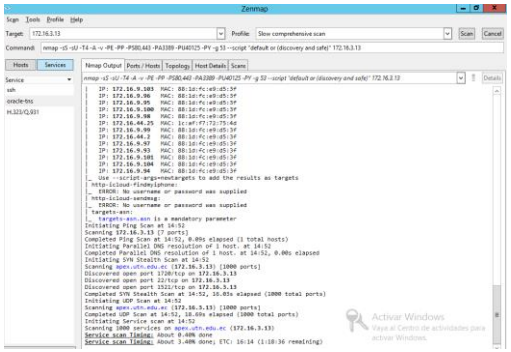
Evaluación Vulnerabilidades.

PRUEBA EFECTUADA	ACTIVO DE INFORMACIÓN	FECHA DURACIÓN	CONCLUSIONES
1.- Se realizó enumeración de puertos, ser vicios y protocolos- Identificación de direccionamiento e los segmentos 172.16.x.xx . Prueba efectuada con herramientas como zenmap en Windows. **BASE DE DATOS** 	Servidor de Base de Datos Oracle 11g Servidor de Aplicación “Sistema Informático Integrado Universitario”	10 de Marzo de 2015 direcciones privadas	El firewall de protección de perímetro es bastante restrictivo a nivel de direccionamiento público, pero fue fácil identificar los puertos abiertos en los servidores tanto de aplicación como de base de datos. Un ejemplo de ello es que se obtuvo información de todos los servicios, puertos abiertos e IP asociadas. 

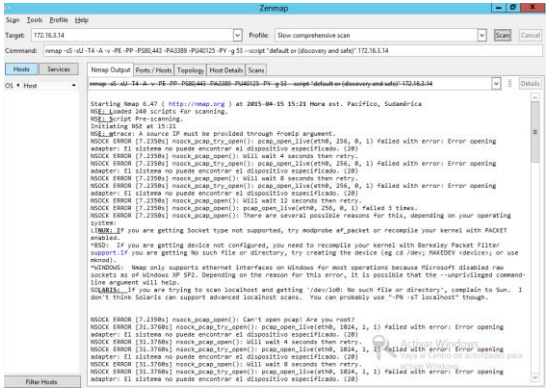
CONTINÚA



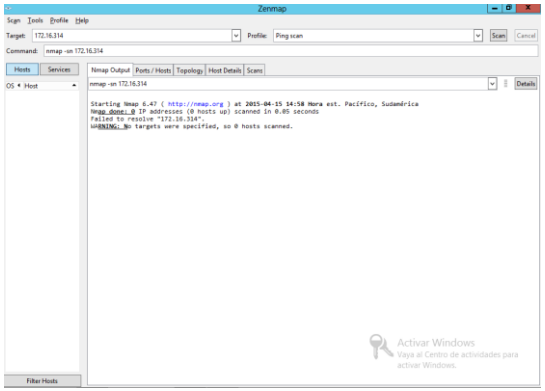




APLICACIÓN

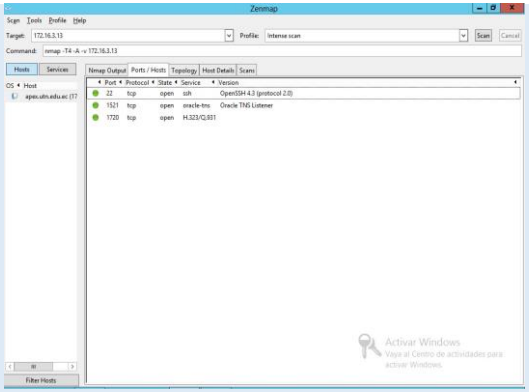


CONTINÚA

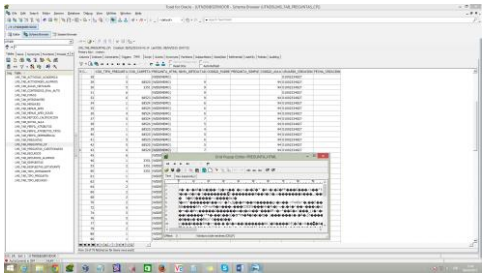


Luego de hacer las pruebas correspondientes con el software identificamos os puertos que se encuentran activos en el servidor de base de datos que es el más crítico obteniendo los siguientes	Servidor de Base de Datos Oracle 11g	De acuerdo a los dato obtenidos pudimos encontrar que se encuentra protegida por ejemplo el puerto **1520** garantiza la entrega de paquetes de datos en el mismo orden, en que fueron enviados. Pero en el detalle de la captura encontramos que se encuentra habilitado el puerto 1720, el mismo que se utiliza para audio y video

CONTINÚA →



Pruebas de contraseñas realizadas en el servidor



Se pone en prueba el funcionamiento del Sistema Integrado Informático Universitario en matrículas

Servidor de Base de Datos Oracle 11g

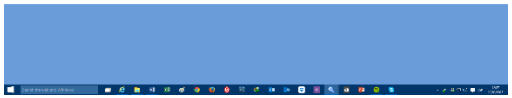
En los datos observados en el servidor de Base de Datos se pudo constatar que las contraseñas se encuentran encriptadas.

Pero no cuentan con políticas claras de creación y eliminación de usuarios.

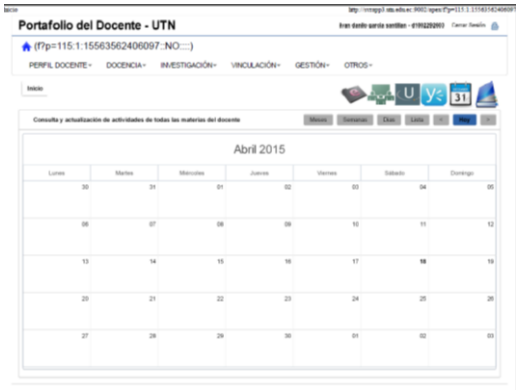
Ya que un docente a pesar de ya no estar vinculado con la Universidad hace un año sigue manteniendo su usuario y clave y puede seguir haciendo consulta de notas y demás.

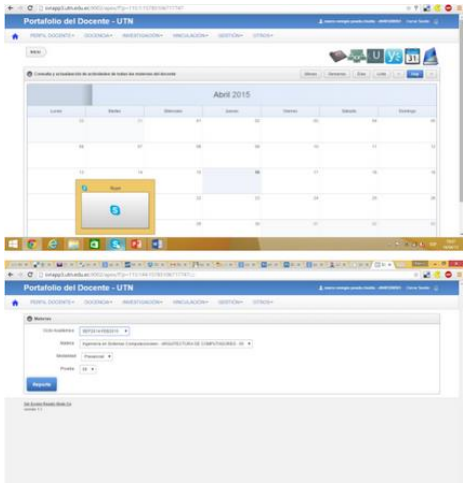
Se logró constatar que el servidor al procesar varias solicitudes de carga no responde por ende el servicio no se encuentra disponibles en el momento requerido.

CONTINÚA ⟶



Al poner en funcionamiento el sistema con una cuenta de una docente que hace 3 años renuncio, pudimos ingresar sin ninguna precaución o restricción.	Módulo de Gestión Académica	10 de Marzo se realizó la prueba pero tiene tiempo indefinido	Es decir que en el sistema no se toma en cuenta las bajas de los usuarios. Se debería revisar semestralmente la base de datos a los usuarios que se dará de alta.





4.2.3 Informe de Auditoría

Fecha del Informe: 10 / 04 / 2015

Nombre de la Entidad: Universidad Técnica Del Norte

AUDITORIA AL MÓDULO DE GESTIÓN ACADÉMICA

OBJETIVO

Verificar políticas y controles de la seguridad de información para el funcionamiento del módulo de gestión académica, utilizando la normativa ISO/IEC 27002:2013, de conformidad con las necesidades de la Universidad, que permitan a la comunidad universitaria cumplir con los objetivos institucionales

Lugar de la Auditoría: Dirección de Desarrollo Tecnológico e Informático UTN

Grupo de Trabajo de Auditoría: Ing. Daisy Imbaquingo Esparza
Ing. Marco Pusdá Chulde

Fecha de Inicio de la Auditoría: 02 / 02 / 2015

Tiempo estimado del proceso de revisión: 60 horas

Fecha de Finalización de la Auditoría: 19 / 03 / 2015

HERRAMIENTAS UTILIZADAS

- Normativa ISO 27002:2013
- Metodología de auditoría Magerit 3 y Pilar v5.5.4
- Utilitarios estándar

ALCANCE

El proyecto de tesis “Evaluación de Amenazas y Vulnerabilidades del Módulo de Gestión Académica - Sistema Informático Integrado Universitario de la Universidad Técnica del Norte, aplicando ISO 27000”, realizará la identificación de riesgos y vulnerabilidades de la seguridad de la información, constatando la implementación y aplicación formal de políticas, procedimientos y controles de la normativa ISO/IEC 27002:2013, que permitan mantener disponible y en funcionamiento eficiente todos los servicios académicos

De acuerdo a lo enunciado anteriormente, se procederá inicialmente con la recolección, agrupación y evaluación de evidencias para determinar la manera en la que se encuentran diseñados e implementados los controles de seguridad de la información del módulo de gestión académica en la Universidad Técnica del Norte, lo que nos dará una visión actual del Sistema Integrado Informático Universitario, para luego proceder a realizar las pruebas de cumplimiento de los controles, posteriormente procederemos a definir los riesgos que conlleva el ineficaz cumplimiento de estos controles o su falta de implementación, finalmente emitir las recomendaciones que permitan mejorar el desempeño de los servicios que el sistema académico ofrece a la comunidad universitaria

CAPÍTULO V.- CONCLUSIONES Y RECOMENDACIONES

5.1 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.

5.2 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. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: CERT Gubernamental Español.

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.

CERT GUBERNAMENTAL ESPAÑOL. (2014). *CCN-CERT*. Obtenido de www.ccn-cert.cni.es

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.* Mc Graw Hill.

Hernández, E. (2010). *Auditoría en informática: un enfoque metodológico y práctico.* México: Continental.

Holbrook., J. R.-P. (1991). Site Security Handbook. *RFC*, 35.

International Classification for Standards (ICS). (2012). *Quality assurance terms and definitions.*

ISO. (2012). *ISO 27001*.

ISO ESPAÑOL. (2014). *ISO 27002 en español*. Obtenido de http://www.iso27002.es/

J. Cano, J. (.-4. (s.f.).

Jeimy J. Cano, Ph.D., CFE. (2014). [ISACA] La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. *ISACA JOURNAL*.

Ochoa Ovalles, S. y Cervantes Sánchez, O. (2012). Seguridad informática. *Contribuciones a las Ciencias Sociales*.

Piattini, M. (2010). *Auditoría Informática.* Madrid: RA-MA.

Siniesterra, G. (2011). *Contabilidad Administrativa.* México: ECOE.

Tamayo, A. (2011). *AUDITORÍA DE SISTEMAS, Una visión práctica.* Bogotá: Centro de publicaciones Universidad Nacional de Colombia.

UNIT- Instituto Uruguayo de Normas Técnicas. (2015). *Normas Técnicas*. Obtenido de http://www.unit.org.uy/

Universidad Técnica del Norte. (2012). Plan Estratégico Institucional. Ibarra, Imbabura, Ecuador.

www.unl.edu.ar. (03 de Agosto de 2010). Obtenido de ttp://www.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf