UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001"

"Tesis previa la obtención del título de Ingeniera en Sistemas"

Autor:

María Gabriela Pardo Cuenca

Director:

Ing. Mario Andrés Palma Jaramillo, Mg. Sc

Loja-Ecuador

2015

CERTIFICACIÓN DEL DIRECTOR

Ing. Mario Andrés Palma Jaramillo, Mg. Sc
DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS

CERTIFICA:

Que el señorita **María Gabriela Pardo Cuenca**, egresada de la carrera de Ingeniería en Sistemas y cuyo tema de tesis versa sobre **"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001"**, ha sido monitoreado, revisado y orientado bajo mi asesoramiento, con pertinencia y con la rigurosidad científica que el trabajo de investigación debe cumplir, por lo cual autorizo su presentación y sustentación.

Loja, 30 de marzo del 2015.

Ing. Mario Andrés Palma Jaramillo, Mg. Sc
DIRECTOR DEL PROYECTO DE TESIS

AUTORÍA

Yo **MARÍA GABRIELA PARDO CUENCA**, declaro ser autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional - Biblioteca Virtual.

Autor: María Gabriela Pardo Cuenca.

Firma: 

Cédula: 1104616576

Fecha: Loja, 14 de marzo de 2015

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LA AUTORA, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **MARÍA GABRIELA PARDO CUENCA**, declaro ser la autora de la tesis titulada: **"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001",** como requisito para optar el grado de: **INGENIERA EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja a los 14 días del mes de marzp de dos mil quince.

Firma: 

Autora: María Gabriela Pardo Cuenca

Cédula: 1104616576 **Dirección:** Loja (Tebaida Alta: Chile 21-06 y España)

Teléfono: (07) 2578942 **Celular**: 0980317229

Correo Electrónico: mgpardoc@unl.edu.ec – gaby16_pc@hotmail.com

Director de Tesis: Ing. Mario Andrés Palma Jaramillo, Mg. Sc.

Tribunal de Grado: Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.
Ing. Waldemar Victorino Espinoza Tituana, Mg. Sc.
Ing. Alex Vinicio Padilla Encalada, Mg. Sc.

AGRADECIMIENTO

A mis padres, por su esfuerzo y apoyo durante mi carrera universitaria.

Al personal técnico y administrativo que labora en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, bajo la dirección del Ing. Milton Ricardo Palacios Morocho, que con su supervisión, sugerencias y apoyo permitieron el desarrollo de mi proyecto de tesis.

Al Ing. Hernán Torres Carrión que con su experiencia y asesoría me permitió enfocar el objetivo de mi proyecto, al Ing. Mario Palma Jaramillo, por su guía y supervisión en el desarrollo y culminación del proyecto.

Igualmente esteriorizo mi agradecimiento a todo el personal docente de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, por las bases científicas y éticas impartidas a lo largo de mi formación profesional.

María Gabriela Pardo Cuenca.

DEDICATORIA

El presente trabajo lo dedico a Dios y María Inmaculada, por ser la fuente de sabiduría y fortaleza en cada instante de mi vida.

A mis padres, Alonso y Olga, por su apoyo en cada etapa de mi vida, los valores y ejemplo de ciudadanía brindados en el hogar, y el amor incondicional que ha fortalecido mi espíritu en todo momento.

A mis hermanos, Eddy, Cisne y Margarita, por el apoyo y consejos dados a lo largo de mi carrera, a mi sobrina, Xilena, por ser la inspiración para lograr mis objetivos, a toda mi familia y amigos que han estado siempre presentes en el transcurso de mi preparación profesional.

María Gabriela Pardo Cuenca.

CESIÓN DE DERECHOS

María Gabriela Pardo Cuenca, autora del presente proyecto de titulación, autoriza a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales No Renovables y por consiguiente a la carrera de Ingeniería en Sistemas, hacer uso total o parcial del contenido del mismo, en lo que estimen conveniente y necesario.

a. Título

“MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001”

b. Resumen

En la actualidad, uno de los bienes más importantes para cualquier tipo de organización es la Información, por lo tanto su gestión y administración son claves para preservar su integridad, confidencialidad y disponibilidad, por lo cual debe contar con un entorno que garantice la protección de dichas características.

Partiendo de lo dicho anteriormente, se ha determinado el enfoque del presente proyecto de tesis, que busca proporcionar medidas de control para la protección de los activos de información, que son propiedad de la Universidad Nacional de Loja, gestionados desde la Unidad de Telecomunicaciones e Información.

El desarrollo de dicho proyecto, se llevó a cabo bajo las consideraciones la de Norma ISO/IEC 27001, para la planificación de un Sistema de Gestión de Seguridad de la Información, para lo cual, es de gran importancia tener en cuenta la situación actual de la Unidad de Telecomunicaciones e Información, donde, a través de entrevistas al personal técnico se pudo identificar las necesidades en cuanto a seguridad para la gestión de la información, manejada en los activos informáticos bajo responsabilidad de la UTI, con ello, se consideró la metodología MAGERIT v3 para la gestión de los riegos informáticos identificados en el análisis, permitiendo con ello determinar mecanismos de control para la mitigación de riesgos, estableciendo de esta forma los primeros pasos en la creación de cultura de seguridad de la información a nivel institucional.

Al finalizar el desarrollo del proyecto, se realizó la socialización de los resultados obtenidos con el personal de la UTI, permitiendo con ello validar la propuesta del *Manual de Políticas de Seguridad de la Información,* como solución para la mitigación de los riesgos asociados a los activos de información que son propiedad de la Universidad Nacional de Loja.

Summary

Currently the information is one of the most important goods of any organization, therefore its management and administration are the keys to preserve their integrity, confidentiality and disponibility, hence it must has an environment that guarantees the protection of those features.

From what was said above it has been determined the focus of this thesis project that tries to provide control measures for the protection of the information assets, property of the Universidad Nacional de Loja, managed by the Telecommunications and Information Unit.

The development of this project was carried out under the Standard ISO/IEC 27001 for the planning of the Information Security Management System, for which it is very important to consider the current situation the Telecommunications and Information Unit, where, through interviews for the technical staff it was posible to identify the security needs for the information management, handled on the computer assets under the responsibility of the UTI, with this, it was considered the MAGERIT v3 methodology for the computer assets indentified by the analysis, thereby allowing control mechanisms for the risk mitigation, so establishing the first steps for the creation of culture information security at institutional level.

At the end of the project was performed the socialization of the results obtained with the UTI staff, thereby allowing the proposal of a Information Security Policy Manual as the solution for the mitigation of the risks associated with the information assets that are the property of the Universidad Nacional de Loja.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

c. Introducción

En la actualidad, al hablar de la información, se debe considerar que esta es uno de los bienes más importantes dentro de cualquier tipo de organización, para mantener sus niveles de competitividad, donde se debe tener en cuenta que la gestión de la misma debe ser adecuada con el fin de preservar su integridad, confidencialidad y disponibilidad; para lo cual es pertinente contar con un entorno que garantice cumplir con estas características **[1-5]**.

Partiendo de lo mencionado, dentro de la Universidad Nacional de Loja, es importante considerar la necesidad de crear cultura de seguridad de la información, mediante la adopción de mecanismos de control, que permitan incorporar un nivel de seguridad adecuado a los activos de información, que son gestionados por la Unidad de Telecomunicaciones e Información de la Institución, ya que actualmente existe desconocimiento de los riesgos a los que está expuesta la información por parte del personal de la institución responsable de los equipos, debido a que no existen políticas o planes de seguridad orientados a sensibilizar el manejo seguro de la información.

A partir de esto, se ha propuesto el presente proyecto, el mismo que busca diseñar un modelo de gestión de seguridad de la información para la Universidad Nacional de Loja, que será gestionado por la UTI, adaptando los requerimientos de la Norma ISO/IEC 27001 a las actividades y funciones realizadas en la Unidad, para ello se establecieron cuatro fases de desarrollo, las mismas que permitieron, mediante: el análisis de la situación actual de la UTI en cuanto a seguridad de la información, valoración de los activos de información (bajo las dimensiones de: confidencialidad, disponibilidad e integridad), determinación de amenazas y vulnerabilidades asociadas a los activos de información, análisis de riesgos encontrados para los activos de información y determinación de los mecanismos de control necesarios para la mitigación de dichos riesgos a partir del *Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005*, que contiene ***133*** mecanismos de control, distribuidos en **11** secciones; esquematizar la propuesta de un *Manual de Políticas de Seguridad de la Información*, destinado a la mitigación de riesgos informáticos y creación de cultura de seguridad de la información a nivel institucional, todo ello gestionado por la Unidad de Telecomunicaciones e Información de la Institución **[5-8]**.

Cabe considerar que las políticas institucionales de seguridad de la información que se sugiere como resultado del proyecto, están basadas en los resultados del estudio y análisis de riesgos realizado en el periodo ***febrero-octubre de 2014*** con ayuda del personal responsable de cada una de las secciones de la UTI en ese mismo periodo.

d. Revisión de Literatura

1. SEGURIDAD DE LA INFORMACIÓN – CONCEPTOS BÁSICOS

1.1. Diferencia entre Seguridad Informática y Seguridad de la Información.

La Seguridad Informática hace referencia a un enfoque técnico donde se manejan **vulnerabilidades** asociadas a los equipos tecnológicos y en parte amenazas enfocadas a los ataques más no se habla de riesgos y su tratamiento, por lo tanto lo que hace la seguridad informática es proteger a los activos de acuerdo a sus vulnerabilidades y los ataques que puedan sufrir a partir de mediciones o lecturas tomadas sobre los equipos, sin considerar los riesgos a los que está sometida la organización y el impacto que pudiese ocasionar un incidente de seguridad, por lo tanto la seguridad informática se encarga de la implementación de soluciones técnicas para la protección de la información.

Partiendo de ello se despliega o se amplía lo que se denomina Seguridad de la Información ya que esta incluye la conceptualización de la seguridad informática incluyendo la responsabilidad del personal que labora en la organización, ya que sin el involucramiento del personal no puede existir un plan sustentable de seguridad de la información, donde ya se puede hablar de un análisis de riegos, aplicación de buenas prácticas y esquemas normativos.

Por lo tanto la determinación de las vulnerabilidades se realiza o se complementa con información que se puede recolectar a partir de sugerencias, opiniones, experiencias, etc., del personal a cargo del manejo de equipos y directivos de la organización, lo mismo sucede con la valoración de los activos ya que esto en muchos de los casos no está al alcance de los técnicos ya que dicho valor es el valor del negocio, donde los propietarios de los procesos de negocio son quienes pueden establecer un valor adecuado de los activos de información, derivado en valores de los **activos/recursos** que son utilizados en las diferentes actividades de la organización.

Partiendo de lo mencionado se puede decir que el concepto de **Seguridad de la Información** es una extensión de la conceptualización de **Seguridad Informática**, ya que implica una visión enmarcada en los riegos del negocio, hablando de riesgos organizacionales, operacionales y físicos en los sistemas de información **(ver figura 1) [1]**.

Figura 1: Seguridad de la Información vs. Seguridad Informática

Por lo tanto se puede decir que la seguridad de la Información es la disciplina que se encarga de proponer y diseñar normas, políticas, técnicas y métodos orientados a conseguir un sistema de información seguro y confiable enfocada en los requerimientos del negocio y valor organizacional [2], es decir que la seguridad de la información es la característica de un sistema informático que garantiza que esté libre de peligro, daño o riesgo, es decir que con esta característica un sistema sea lo más fiable posible para sus usuarios [3].

La seguridad de la información se puede definir como la protección de la confidencialidad, integridad y disponibilidad **(ver Figura 2)** de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.

Definiendo estos parámetros o dimensiones como:

Confidencialidad: Donde se busca limitar el acceso a la información, es decir que esta solo pueda ser utilizada por personas autorizadas.

Integridad: Que se refiere a la protección de información, tanto en su almacenamiento como en su forma de gestión o administración.

Disponibilidad: Lo que se busca es que la información esté disponible y completa a todo momento, para usuarios autorizados **[1-5]**.

Figura 2: Parámetros básicos de la seguridad de la Información

3.1 ¿Qué es un fallo de seguridad?

Un fallo de seguridad es cualquier incidente o evento que pone en peligro cualquiera de los parámetros con los que se valora la seguridad, considerando el crecimiento desmedido de los usuarios que manejan los sistemas de información cada vez más complejos, mediante el intercambio de información, se vuelve un reto evitar que sucedan diferentes tipos de fallos como son:

- Fallo en las comunicaciones.
- Fallos en el suministro eléctrico
- Fallos humanos de usuarios internos, usuarios externos, administradores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc., que inundan la red.
- Accesos no autorizados a los sistemas o a la información.
- Incumplimiento de una ley o reglamento.

Los fallos de seguridad son ocasionados muchas veces por la errónea percepción de que si la seguridad física está asegurada novan a existir problemas, o que con la protección únicamente de las aplicaciones y base de datos que se garantiza la seguridad, partiendo de ello se dejan desprotegidas muchas áreas de la organización o activos de información que pueden ser fácilmente dañados o destruidos ya que no se considera la seguridad física, seguridad lógica o medidas organizativas **[4,5]**.

3.2 Importancia y beneficios de la seguridad en las organizaciones

La seguridad de la información está directamente relacionada con la supervivencia del negocio, sus actividades y procesos, donde al existir pequeños fallos puede repercutir

en pérdidas para la organización, en caso de sucesos graves o catastróficos puede significar el cierre de la organizaciones con pérdidas irremplazables al hablar de información.

Partiendo de lo mencionado actualmente las organizaciones están tomando conciencia de la aplicación de controles, con cumplimiento de regulaciones legislativas donde la idea principal es la protección de la información, todo esto mediante aplicaciones de sistemas de gestión que permiten ordenar las actividades y dirigirlas al cumplimiento del objetivo que busca la organización. Lo que se pretende con un sistema de gestión para la seguridad es evitar tener que reaccionar ante hechos que podrían haber sido previstos o gestionados antes que lleguen a ser un problema, ya que evitar problemas es una manera muy barata de ahorrar costos **[4,5]**.

En cuanto a los beneficios que la seguridad de la información ofrece para las organizaciones existen muchas entre las que se puede destacar las siguientes:

- **Reducción de costes:** esto incide directamente sobre la rentabilidad económica de cualquier tipo de organización, ya que la aplicación de sistemas de gestión de seguridad, a corto plazo se observar cómo se evitan situaciones que pueden repercutir en pérdidas económicas para la organización.
- **Protección del negocio:** un sistema de seguridad busca mediante planes de contingencia evitar interrupciones en las actividades o procesos de la organización, manteniendo la disponibilidad de los activos de información, es decir garantizando la continuidad del negocio.
- **Mantener y mejorar la imagen corporativa:** Se ve reflejada directamente en la imagen de la organización ya que esta se percibe como empresa responsable, comprometida con la mejora de sus procesos, productos y servicios **[5]**.

2. ENTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 La organización ISO (Organización Internacional de Estándares).

Es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

Los miembros de esta organización, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos que

buscan soluciones en campos de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (*International Electrotechnical Commission*), la organización que a nivel mundial prepara y publica estándares en el campo de la electro tecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1).

Para una Norma Internacional sea aprobada se requiere que del 75% de los organismos internacionales que conforman la organización lo den su voto favorable **[5-8]**.

4.2 Familia de la Normas ISO 27000

Esta familia es un conjunto de estándares desarrollados por la *International Organization for Standardization e International Electrotenchnical Commission* que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización **[5,6]**.

La familia de la norma ISO 27000 es una serie de estándares comprendidos entre los rangos de numeración que van desde 27000 – 27019 y de 27030 a 27044, (ver **Anexo 1)**.

Entre las más importantes tenemos para el proyecto tenemos:

ISO 27000: Que contendrá términos y definiciones que se emplean en toda la serie, hace referencia Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario; esta recoge los términos y conceptos relacionados con la seguridad de la información, dando una visión general de la familia de estándares de esta área, una introducción a los SGSI y una descripción del ciclo de mejora continua.

Fue publicada en mayo de 2009, revisada para su segunda edición en diciembre de 2012, llegando a su tercera edición en enero de 2014.

ISO 27001: Es la norma principal que contiene los requisitos del Sistema de Gestión de Seguridad de la Información[1], fue publicada en el 2005, revisada para septiembre de 2013, se origina en la BS7799-2:2002.

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, fue publicada en el

[1] Sistema de Gestión de Seguridad de la Información (SGSI)

2007, es el nuevo nombre de ISO 17799:205. No es certificable. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

ISO 27003: Consiste en la guía de implementación de SGSI e información del modelo PDCA, y los requerimientos de sus diferentes fases. Publicada en el 2010, tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y quías de implantación.

ISO 27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

ISO 27005:2008 Diseñada para establecer las directrices para la gestión de riesgos de seguridad, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.

ISO 27007: Guía de auditoria de un SGSI, como complemento lo específico en ISO 19011.

ISO/IEC 27011: Contiene las directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizado en el Norma ISO/IEC 27002, facilitando el cumplimiento de la Norma ISO27001 para la consecución de un nivel de seguridad aceptable **[5-8]**.

4.2.1 La Norma ISO 27001

4.2.1.1 Origen

Esta norma fue publicada en el año 2007, donde se originó al redefinir a sus antecesoras como la norma **BS7799**, que se refiere al código de buenas prácticas para la gestión de la seguridad de la información, donde en su versión 2 (BS7799-1) incorpora especificaciones para los sistemas de gestión de seguridad de la información; con una revisión en el 2001 es adoptada por la norma ISO con la denominación ISO/IEC17799

A partir del 2007 la ISO 17799:2005 adopta el nombre de ISO 27002, para redefinirse finalmente en octubre de 2007 como UNE-ISO/IEC27001 **[5, 8, 9]**.

4.2.1.2 Contenido de la norma ISO/IEC 27001

La norma específica los requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización**.** Está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente.

La norma recoge los componentes de un SGSI, es decir, la parte documental del sistema: documentación mínima que debe formar parte del SGSI, como se deben gestionar y mantener, es decir: como debe ser su diseño, definir los controles de seguridad a considerar a partir de su anexo A (controles detallados en la Norma ISO/IEC 27002) **(ver Anexo 2)**, hasta la forma en la que debe realizarse la revisión y mejora del SGSI **[5,8, 9]**.

4.3 Otros Estándares y Normas para Asegurar la Información

En proceso de Gestión de Seguridad de la Información, existen diferentes estándares o normas de buenas prácticas que permiten crear modelos de aplicación para la seguridad a nivel organizacional, a continuación se hace referencia a los más conocidos y aplicados:

- **BS 7799-3 (British Standars Institution):** se publicó su tercera versión en el 2006 que se dedica a la gestión de riesgos de seguridad de la información que profundiza en los aspectos de evaluación de riegos y su tratamiento, incluyendo tomas de decisiones por parte de la Dirección. Se considera que la ISO 27001 es una evolución de esta normativa donde ya se hace referencia a la identificación, evaluación, tratamiento y gestión de riesgos de seguridad [9,10].

- **Centros de Computación/Data Center:** Hace referencia a la instalación de alta prioridad como los Data Center, donde se ven incluidas varios estándares de aplicabilidad para una gestión segura de los mismo como son:

  - ✓ **ASHRAE (American Society of Heating, Refrigeration and Air-conditioning Engineers):** responsable de la creación de directrices térmicas para entornos de procesamientos de datos **[9,11]**.

- ✓ **BICSI 002 (ANSI/BICSI002):** que recopila las mejores prácticas en la implantación como en diseño de Data Center **[9,12]**.
- ✓ **TIA 942 (Telecommunications Industry Association):** Fundada en 1988, ha desarrollado el estándar ANSI/TIA 942 que hace referencia a las mejores prácticas para infraestructura de Data Center **[9,13]**.

- **COBIT:** Fue establecido por ISACA (Information Systems Audit and Control Association) en 1988 para aclarar y orientar en cuestiones actuales y futuras relativas a la administración, seguridad y aseguramiento TI. Donde el documento más conocido es **CobiT** (Objetivos de control para tecnologías de la información y similares), donde su marca de referencia es compatible con ISO 27002 (anterior ISO 17799:2005) y COSO (Committee of Sponsoring Organizations of Treadway Commission) **[9,14,15]**.

- **COSO (Committee of Sponsoring Organizations of Treadway Commission):** que se refiere a una iniciativa del sector privado formada en 1985, con su objetivo principal de identificar los factores que causan informas financieros fraudulentos y hacer recomendaciones para reducir su incidencia; definiendo controles internos, normas y criterio contra los cuales las empresas y organizaciones pueden evaluar sus sistemas de control **[9,16]**.

- **Gestión de Servicios:**
  - ✓ **ISO/IEC 20000:** Es el primer estándar internacional certificable para la gestión de servicios TI, actualmente ha evolucionado o extendido en la norma ISO/IEC 27013, donde esta incorpora el ciclo de vida Plan-Do-Check-Act, donde su norma predecesora (BS 15000), fue inicialmente desarrollada para indicar las mejores prácticas contenidas en el marco ITIL**[9]**.
  - ✓ **ITIL ("IT Infrastructure Library):** se refiere a un conjunto de publicaciones para las mejores prácticas en la gestión de servicios TI e incluye opciones que pueden ser adoptados o adaptadas según las necesidades del proveedor de servicios. Se debe considerar que esta norma fue integrada en la serie de la norma ISO 20000 con el propósito de que los dos conjuntos de publicaciones formen parte de la misma estructura para su mejor comprensión, esta sirve de base para dicho estándar [9,17].

- **ISO 22301:** Importante para las empresas que intentar disponer de planes de continuidad de negocio que minimicen la inactividad de la organización en caso de interrupciones.

- **UNE 71502:2004:** Norma española certificable, desarrollada en base a BS7799-2:2002, que estables las especificaciones para los sistemas de gestión de seguridad de la información, especificando los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de Seguridad de la Información dentro del contexto de los riesgos identificados para la organización. Su vigencia fue corta por la aparición de la norma ISO 27001 que hizo que esta sea anulada **[9]**.

4.3.1 Tabla comparativa entre las normativas o estándares para seguridad de la información.

TABLA I. Tabla comparativa entre estándares para seguridad de la información.

NORMA	Características principales	Anal. Y gestión de Riesgos	Impacto en la organiz.	Document. de aplicabili.	Controles estándar.	Norma predecesora y/o compatible	Certificable	Observación
BS77993	- Se vincula con la toma de decisiones con la Dirección. - Orientada a la gestión de riesgos.	SI	SI	NO	NO	27001	NO	Se dedica a la gestión de riesgos (evaluación),no busca su mitigación usando salvaguardas
ASHRAE	- Creación de directrices para el entorno de DATA CENTER	NO	NO	SI	NO	---	NO	Orientada exclusivamente a la instalación de DATA CENTER. Sus recomendaciones son aceptadas a nivel internacional
BICSI002	- Cubre los factores fundamentales para la implantación y diseño de DATA CENTER	NO	NO	SI	NO	----	NO	Cuenta con 150 expertos para el desarrollo de contenidos. Dispone de formación especializada para profesionales para obtención de certificaciones como requerimiento para acreditaciones de

								profesionales a nivel individual
TIA 942	- Enfocada en las mejores prácticas para la infraestructura de DATA CENTER	NO	NO	SI	NO	---	NO	Recopila especificaciones para comunicaciones y cableado estructurado. La ausencia de una entidad o mecanismos de regulación en la emisión de certificados ha generado descrédito.
COBIT	- Orientada a clarificar cuestiones actuales y futuras en cuanto a administración, seguridad y aseguramiento de tecnologías de información	NO	SI	SI	SI	27002 y COSO	NO	Han evolucionado para tratar de adaptarse y lograr certificación en ISO 27001. Utiliza ciclo PDCA para integrarlo en procesos de negocios. Existen certificaciones individuales.
COSO	- Definición de controles internos, normas y criterios para evaluar sistemas de control	NO	SI	SI	NO	COBIT y ITIL	NO	Existe una mejora para el 2004 que introduce nuevos elementos. No se trata de un estándar específico de seguridad de la información.

ISO/IEC 20000	- Indica la mejores prácticas para la gestión de Servicios en TI	SI	NO	SI	NO	Proviene de BS1500 y evoluciona a la ISO/IEC 27013	SI	Certificable en la gestión de SERVICIOS de tecnologías de información.
ITIL	- Las mejores prácticas en la Gestión de Servicios TI, incluyendo opciones para la adaptación según las necesidades del proveedor de servicios	NO	NO	SI	SI, para el ciclo de vida de los servicios	Integrada en la ISO/IEC 20000	NO	Se integra con la ISO/IEC 2000 para que los dos conjuntos de publicaciones formen parte de la misma estructura para cuestiones de comprensión. La nueva versión fue publicada en 2007
ISO 22301	- Buenas prácticas para la gestión de continuidad de negocio	SI	SI	SI	SI	Sustituida o integrada en la ISO/IEC 27001	SI	Paso a integrarse como parte de la ISO/IEC 27001 con la norma 27031.
UNE 71502:2004	- Especifica los requisitos para establecer, implementar, documentar y evaluar un SGSI en el contexto de los riegos organizacionales.	SI	SI	SI	SI	Cortada su vigencia por la publicación de la ISO/IEC 27001	SI	Ante la publicación de la ISO/IEC 27001 fue anulada a favor de la norma internacional el 31 de diciembre de 2008 (ver Anexo 16)
ISO/IEC 27001	- Especifica los requisitos para establecer, implementar,	SI	SI	SI	SI	Compatible con COBIT,	SI	- Esta norma reemplaza a la UE 71502:2004

	documentar y evaluar un SGSI en el contexto de los riegos organizacionales, basada en un enfoque por procesos y mejora continua. - Recoge los componentes de un SGSI, en la parte documental para la gestión y mantenimiento; definición de controles de seguridad para a partir de su Anexo A, finalizando con la revisión y mejora del SGIS					COSO, ISO/IEC 20000, ITIL, ISO22301		- Se involucra con todas las secciones de la organización para el manejo de seguridad de la información. - Utiliza el modelo PDCA para mejora continua. - Engloba las mejores normativas y prácticas en cuestión de seguridad de la Información

Con el análisis de las diferentes normas internacionales destinadas a la seguridad de la información podemos decir que la norma que se adapta a cubrir con las necesidades más importantes en la gestión de la información a nivel organizacional es la norma ISO/IEC 27001, ya que esta engloba las mejores prácticas propuestas en sus normas antecesoras (BS77993, ISO/IEC 22301, ISO/IEC20000, UNE 71502:2004), así como normas que vienen a integrarse a ella (TIA,COBIT, ITIL) permitiendo de esta forma gestionar los activos de información de las diferentes secciones de la organización, mediante la mitigación de riesgos asociados a dichos activos, y la mejora continua en la seguridad de la información a nivel institucional.

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

5.1 Aspectos Generales sobre la implementación de un SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) es el concepto central sobre el que se construye ISO 27001, donde la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

La seguridad de la información, según la ISO 27001, busca la protección de la información bajo las tres dimensiones de confiabilidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada adecuadamente se debe identificar su ciclo de vida y los aspectos relevantes adoptados para garantizar las tres dimensiones, en base a este conocimiento se deben adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial **[5,6]**.

5.2 Tareas a realizar en el proceso de un SGSI

La implementación de un SGSI en una organización se enfoca en cuatro fases o etapas que conforman el denominado Ciclo Deming (2005) de mejora continua o ciclo PDCA (Plan-Do-Check-Act) **(ver figura 3 y Tabla II)**, que permite establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a la norma ISO 27001:2005, este ciclo es tradicional en los sistemas de gestión de calidad **[5,6]**.

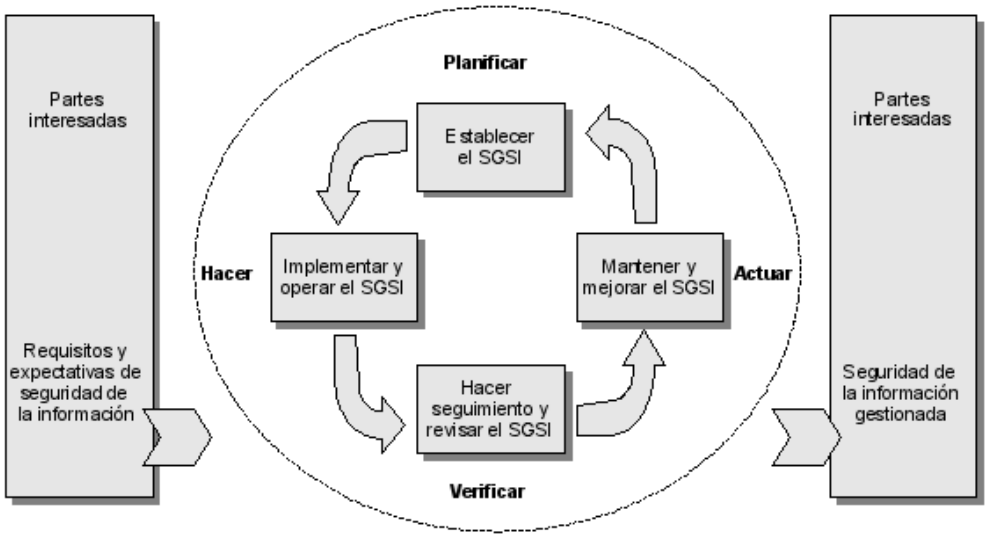


Figura 3: Ciclo Deming-PDCA

TABLA II. Descripción del proceso PDCA

FASE	DESCRIPCIÓN
PLANEAR (establecer el SGSI)	Establecer políticas, objetivos, procesos y procedimientos del SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
HACER (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
REVISAR (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
ACTUAR (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

5.2.1 Fase Plan

Al planificar un SGSI de debe definir el alcance del mismo en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Es importante que defina los límites del SGSI, es recomendable empezar por un alcance limitado **(ver Figura 4) [5,6]**.

Figura 4: Ciclo PDCA, Fase PLAN

Para ello se debe:

1. Definir una política de seguridad donde se:

Incluya el marco general y los objetivos de seguridad de la información de la organización.

- ✓ Considere requerimientos legales referentes a la seguridad de la información.
- ✓ Esté alineada con el contexto estratégico de gestión de riesgos de la organización.
- ✓ Establezcan los criterios con los que se va a evaluar el riesgo.
- ✓ Aprobación por la dirección.

2. Definir una metodología de evaluación del riesgo apropiada para el SGSI, establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles.

3. Identificar los riesgos donde se debe considerar:
    - ✓ La identificación de los activos que están dentro del alcance del SGSI y a sus responsables directos.
    - ✓ La identificación de las amenazas en relación a los activos.
    - ✓ La identificación las vulnerabilidades.
    - ✓ La identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos.

4. Analizar y evaluar los riesgos donde se debe:
    - ✓ Evaluar el impacto de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
    - ✓ Evaluar la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas y vulnerabilidades.
    - ✓ Estimar los niveles de riesgo.
    - ✓ Determinar si el riesgo es aceptable o necesita ser tratado.

5. Identificar y evaluar las distintas opciones de tratamiento de los riesgos donde se debe:
    - ✓ Aplicar controles adecuados, seleccionados en el Anexo A de la ISO 27001.
    - ✓ Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para su aceptación.
    - ✓ Evitar el riesgo, aplicando normativas.
    - ✓ Transferir el riesgo a terceros.

6. Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI, para lo cual se considera definir una declaración de aplicabilidad que incluya:
    - ✓ Los objetivos de control y controles seleccionados y su justificación de elección.
    - ✓ Los objetivos de control y controles que actualmente ya están implantados.
    - ✓ Los objetivos de control y controles del Anexo A excluidos y justificación de exclusión, donde se puede detectar posibles omisiones involuntarias **[5,6,18-23]**.

5.3 Conceptos básicos manejados en la Fase “PLAN”.

5.3.1 Activos de Información

Activos de información es todo aquello que tiene algún valor para la organización que contiene o manipula información y por lo tanto debe protegerse.

Refiriéndose a activos de información a los siguientes tipos:

- ✓ **Datos:** Toda la información, indistintamente de su formato, que se genera, recogen, gestiona o se transforma en la organización.
- ✓ **Aplicaciones:** El software utilizado en la gestión de la información.
- ✓ **Personal:** Considerando aquí, al personal de la organización que manipula los sistemas de información, personal ajeno a la organización que tiene acceso a la información o a los activos de información.
- ✓ **Servicios:** Se consideran los servicios internos que son parte de la organización y los externos que son dados por proveedores a la organización.
- ✓ **Tecnología:** Los equipos utilizados para la gestión de la información y comunicación.
- ✓ **Instalaciones:** Lugares en los que se alojan los sistemas de información.
- ✓ **Equipamiento auxiliar:** Equipos que dan soporte a los sistemas de información.

Donde es importante considerar que cada equipo debe contar con un responsable, que se debe hacer cargo de mantener la seguridad del activo.

Destacando que la valoración de un activo de información para la organización es valorado bajo las dimensiones de: disponibilidad, confidencialidad e integridad **[5,6,21-23].**

5.3.2 Conceptos básicos de un análisis de riesgos.

El análisis de riegos se refiere a la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización, donde el riesgo indica lo que le podría afectar a los activos al no estar protegidos **(ver Figura 5) [5,6,24]**.

Para ello es importante tener en cuenta los siguientes conceptos:

1. **Amenaza:** Un sistema informático puede ser protegido desde la parte lógica y física, donde las amenazas se presentan a partir de diferentes circunstancias a las que la información está expuesta, a una amenaza se la considera como

cualquier evento que puede provocar algún tipo de daño en un sistema de información **[25].** Donde las amenazas se las puede identificar bajo las siguientes categorías:

- **De origen natural:** que comprende los accidentes naturales, donde los activos de información son víctimas pasivas.
- **Del entorno (de origen industrial):** refiriéndonos a los desastres de tipo industriales como contaminación, fallos eléctricos, inundaciones, etc., donde los activos de información son víctimas pasivas.
- **Causadas por las personas de forma accidental:** referente a las personas con acceso al sistema de información que pueden causar daños no intencionados, por error o por omisión
- **Causadas por las personas de forma deliberada:** donde las personas con acceso al sistema de información causan problemas intencionados, como ataques deliberados, daños físicos, robo, etc., con ánimo de causar daños y perjuicios a la organización.

  Es importante considerar que la valoración de amenazas se basa en dos enfoques esenciales que son:

  - **Degradación:** refiriéndose a cuán perjudicado resultaría el valor del activo.
  - **Probabilidad:** refiriéndose a cuán probable o improbable es que se materialice una amenaza.

2. **Vulnerabilidad:** se refiere a la debilidad de un activo que puede ser aprovechada por una amenaza para causar daño.
3. **Impacto:** se refiere a la medida del daño sobre el activo derivado de la materialización de una amenaza, donde se debe conocer el valor del activo y la degradación del mismo.
4. **Riesgo:** se refiere a la medida del daño probable sobre un sistema, donde se debe conocer el impacto de las amenazas sobre los activos. El riesgo crece con el impacto y la probabilidad.

Es importante considerar la necesidad de analizar los riesgos a los que están sometidos los activos de información ya que mediante esto se determina o averigua cuales son los peligros a los que se enfrenta la organización en cuestión de seguridad y la importancia de estos activos, todo esto con el fin de tomar

decisiones orientadas a las medidas de seguridad que son necesarias implantarse.

Para el tratamiento de un riesgo se debe considerar las repercusiones que este tenga para la organización, por lo tanto los objetivos de control que se utilizaran estarán orientados a la mitigación de los riesgos asociados a los activos de información identificados en la organización.

Es importante considerar que en base al análisis de riegos que se realice se obtendrá el nivel de riesgo asociado al activo con el que se podrá establecer su criterio de aceptación y con ello realizar las medidas para mitigación o tratamiento de riesgos para cada caso **[5,6].**

Las medidas de mitigación para el tratamiento de riesgos se describen a continuación **(ver Figura 6):**

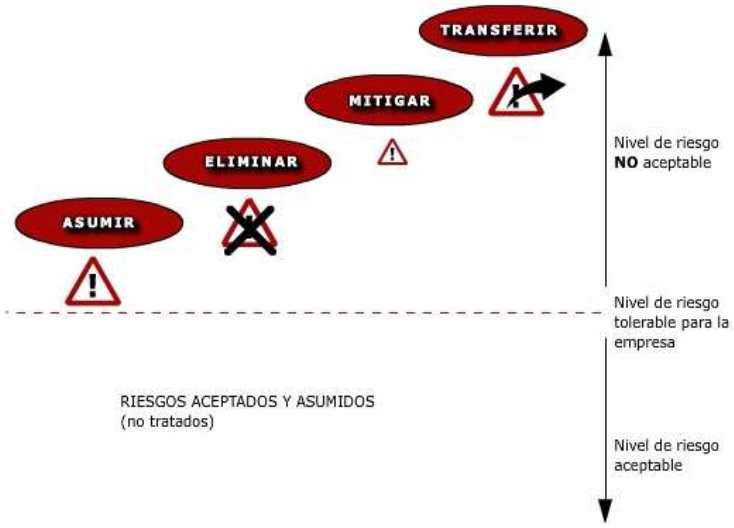


Figura 5: Tratamiento del Riesgos en un Sistema de Seguridad de la Información

Se debe considerar la importancia de la categorización de riesgos, con el fin de que estos sean tratados a tiempo, dependiendo de la importancia de los activos de acuerdo a su valoración y a la exposición de estos a diferentes amenazas o vulnerabilidades.

Con lo mencionado anteriormente se deben considerar los cuatro tipos o calificaciones de decisiones para el tratamiento de riesgos, determinándose de la siguiente manera:

- **Riesgo Transferible**: donde el riesgo se traspasa a otra organización o instancia universitaria, debido a su estado crítico que necesita de atención privilegiada o urgente. Así como este puede darse el caso de que exista algún tipo de seguro asociado a este.

- **Riesgo Mitigable**: donde el riesgo puede ser reducible con la aplicación de controles de seguridad dedicados, debido a la gravedad del mismo.
- **Riego Eliminable**: donde lo habitual es la eliminación del activo que somete a la organización a riesgos que son injustificados.
- **Riegos Asumible**: donde el riesgo asociado al activo puede ser aceptable por la organización en el sentido en que no se van a tomar acciones para reducirlo o eliminarlo **[5,6,26].**

5. **Salvaguardas:** definidas como los procedimientos o mecanismos tecnológicos que reducen o minimizan el riesgo.

El análisis de riegos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar su daño y costo para la organización **(ver figura 6) [5,6,24,25]**.

Figura 6: Esquema de gestión de riesgos

5.4 Metodología de Análisis de Riesgos.

Al hacer referencia a la metodología de análisis de riesgos para la seguridad de la información, es importante considerar que existen varias metodologías que pueden ser empleadas, las mismas que se basan en los requerimientos de la norma ISO/IEC 27001, donde todas cumplen con el mismo objetivo y su diferencia se determina en la forma de presentación de los resultados.

5.4.1 Metodología de Análisis de Riegos MAGERIT[2] – versión 3.0

Es una metodología desarrollada por el Ministerio de Administraciones Públicas español, esta metodología de análisis de riesgos describe los pasos para realizar un análisis del estado de riegos y para gestionar su mitigación. Esta detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión efectiva. Se debe considerar que esta cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas (Libro I: Método, Libro II: Catálogo de Elementos y Libro III: Guía de Técnicas).

MAGERIT persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de la organización 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 información y comunicaciones.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

Con ello es importante considerar que la metodología MAGERIT, está orientada a los criterios de valoración de activos que busca la norma ISO/IEC 27001 en su aplicación como son: *disponibilidad, Integridad y confidencialidad*, considerando que esta metodología contempla también derivadas de estos criterios como son la *autenticidad y trazabilidad,* donde se debe tener presente que estos criterios pueden ser requeridos o no dependiendo de cada caso **[5,24, 26,27]**.

5.4.1.1 Herramienta PILAR

PILAR, es el acrónimo de "*Procedimiento Informático-Lógico para el Análisis de Riesgos*" es una herramienta desarrollada bajo especificación del Centro Nacional de

[2] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología ***Magerit*** bajo la norma **ISO/IEC 27001*.***

Esta herramienta soporta todas las fases del método Magerit:

- Caracterización de los activos: identificación, clasificación, dependencia y valoración.
- Caracterización de las amenazas.
- Evaluación de las salvaguardas.

La herramienta incorpora los catálogos del "Catalogo de Elementos" permitiendo una homogeneidad en los resultados del análisis:

- Tipos de activos
- Dimensiones de valoración
- Criterios de valoración
- Catálogo de amenazas.

La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Los resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo. De esta forma es posible elaborar diferentes tipos de informes y presentaciones de los resultados.

La herramienta tiene un licenciamiento privativo que su costo varía de acuerdo al tipo o versión de la herramienta, que son tres y un módulo de personalización:

1. **uPILAR** (este tipo permite solamente el análisis de perfiles de distribución) su costo es de ***250 euros,*** considerando que si se necesita perfiles de evaluación adicionales cada uno tiene un valor de ***150 euros.***
2. **PILAR Basic** (versión sencilla para empresas pequeña y mediana) su valor enfocado al análisis de riesgos cualitativos es de ***500 euros.***
3. **PILAR** (versión completa de la herramienta) esta incluye:
    - Análisis de riesgos cualitativo.
    - Análisis de riesgos cuantitativo-
    - Análisis de impacto y continuidad de operaciones.

Tiene un costo de ***1500 euros***, agregándole a esto el valor por el soporte de base datos (SQL) que es de ***500 euros,*** por lo tanto el valor de la licencia de la herramienta en su versión completa es de ***2000 euros***

La licencia incluye:

- Garantía frente a defectos por 1 año-

- Derecho a todas las actualizaciones dentro de la misma versión.

Módulo de Personalización RMAT: el mismo que es vendido como un paquete integral que incluye:

- EVL (Perfiles de protección)
- TSV (Perfiles de amenazas)
- KB (Protección adicionales)

Todo esto con un costo de ***3000 euros.***

Es importante que para fines académicos se puede solicitar una licencia para fines educativos **[24,28]**.

5.4.2 Aspectos generales sobre otras metodologías de análisis de riesgos.

Para el trabajo con la norma ISO/IEC 27001, se han considerado otras metodologías de análisis de riegos que pueden ser utilizadas generando resultados similares, tenemos las siguientes:

OCTAVE[3]**:** Esta metodología permite recoger y analizar información de manera que se pueda diseñar una estrategia de protección o planes para mitigación de riesgos. Esta metodología se centra en los aspectos relacionados con el día a día de las empresas, donde la evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para organización.

Se divide en tres fases:

1. Construcción de perfiles de amenazas basadas en activos.
2. Identificación de vulnerabilidades en la infraestructura

[3] OCTAVE (Operationally Critical Threatm Asset, and Vulnerability Evaluation

3. Desarrollo de estrategias y planes de seguridad **[5, 28-30]**.

IT-GRUNDSCHUTZ[4]**:** Esta metodología fue desarrollada en Alemania por la Oficina Federal de la Seguridad de la Información. Esta metodología ofrece numerosas herramientas disponibles para lograr un nivel adecuado de seguridad con normas básicas requeridas para la gestión de la seguridad de la información.

Los pasos que se realizan con esta metodología son:

1. Iniciar el proceso.
2. Definir los objetivos de seguridad y el contexto de la organización.
3. Estableces la organización para la seguridad de TI.
4. Evaluación de los requisitos de protección.
5. Modelado
6. Comprobación de la seguridad de TI.
7. Planificación e implantación.
8. Mantenimiento, seguimiento y mejora del proceso **[5,31]**.

Métodos ISF[5] **para la evaluación y gestión de riesgos**: Se refiere a un conjunto de principios y objetivos para la seguridad de la información asociando buenas prácticas. Es estándar cubre la gestión de la seguridad a nivel corporativo, las aplicaciones críticas del negocio, las instalaciones de los sistemas de información, las redes y desarrollo de sistemas.

Este estándar contiene:

- SARA, que es otra metodología para analizar el riesgo en sistemas
- FIRM, que es una metodología para el seguimiento y control del riesgo.
- SPRINT, que es una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas no críticos **[5]**.

EBIOS[6]**:** es una metodología francesa para análisis y gestión de riesgos de seguridad de información la misma que consta de cinco fases para completar su ciclo de trabajo:

- **Fase 1:** Análisis del contexto

[4] Manual de protección básica de TI
[5] ISF (Information Security Forum).
[6] EBIOS (EXPRESSION DES BESOINS ET INDENTIFICATION DES OJECTIFS DE SÉCIRITÉ

- **Fase 2 y 3:** Análisis de las necesidades de seguridad y de las amenazas.
- **Fase 4 y 5:** Resolución del conflicto, donde se establecen los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

Esta metodología se enfoca a gestores del riesgo de TI **[5]**.

4. Generalidades de la Universidad Nacional de Loja

La Universidad Nacional de Loja es una Institución de Educación Superior, laica, autónoma, de derecho pública, con personería jurídica y sin fines de lucro, que ofrece formación en los niveles: técnico y tecnológico superior, de tercer y cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno con calidad, pertinencia y equidad para el desarrollo sustentable de la región y del país **[37]**.

6.1 Misión y Visión

Misión

Es misión de la Universidad Nacional de Loja: la formación académica y profesional, con sólidas bases científicas y técnicas, pertinencia social y valores; la generación y aplicación de conocimientos científicos, tecnológicos y técnicos, que aporten al desarrollo integral del entorno y al avance de la ciencia; el fortalecimiento del pensamiento, la promoción, desarrollo y difusión de los saberes y culturas; y, la prestación de servicios especializados.

Visión

La Universidad Nacional de Loja tiene como visión, consolidarse como una Comunidad Educativa, con excelencia académica, humanista y democrática, líder en el desarrollo de la cultura, la ciencia y la tecnología **[37]**.

6.2 Objetivos Estratégicos

1. Formar talento humano de calidad, con sólidas bases científicas, técnicas y humanistas, que respondan a las necesidades del desarrollo local, regional y nacional, en el marco de los lineamientos de Sistema de Educación Superior y de un permanente proceso de evaluación.

2. Generar conocimientos científicos, innovar tecnologías y potenciar los conocimientos tradicionales, que enriquezcan los procesos de formación y coadyuven a resolver los principales problemas del desarrollo regional y nacional.

3. Constituir a la Universidad Nacional de Loja, en espacio académico y de interacción social, que produzca pensamientos y propuestas para el desarrollo de la región; que promocione y difunda nuestras culturas y que oferte a la colectividad servicios especializados de calidad **[37]**.

6.3 Unidad de Telecomunicaciones e Información

6.3.1 Misión

Administrar tecnología de información y proveer servicios informáticos y de comunicaciones para el proceso de datos y acceso de información, así como investigar e implementar tecnología de punta que garanticen la disponibilidad, integridad y confiabilidad de la información **[37]**.

6.3.2 Atribuciones y Responsabilidades.

- Participar en la elaboración de estudios y diseños de redes.
- Coordinar actividades relacionadas con el mejoramiento de la infraestructura técnica de la Universidad: Redes de portadores, servicios de óptima calidad.
- Coordinar actividades con áreas relacionadas en el mejoramiento de la tecnología y capacitación: Ingeniería en Electrónica y Telecomunicaciones, Ingeniería de Sistemas.
- Actualizar licencias y permisos de operación, tanto de redes de telecomunicaciones como redes informáticas.
- Coordinar y supervisar todos los requerimientos de Software y Conectividad, así como las necesidades de Video Conferencia y Teleducación de la MED.
- Coordinar y supervisar los proyectos TIC's (TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN), en especial de TELEMEDICINA y TELEDUCACIÓN, TELEMETRÍA y VIDEO CONFERENCIAS.
- Realizar la planificación de redes de telecomunicaciones con sus respectivos componentes, memorias técnicas, diseños, detalles constructivos, especificaciones técnicas de cada uno de los proyectos.
- Elaborar estudios de perfeccionamiento del software y redes que brindan servicios de telecomunicaciones e información a la ciudad universitaria, para

el ordenamiento e integración, mediante propuestas de conectividad en sus diferentes modalidades: fibra óptica, micro-onda, satelital.

- Planificar y controlar la instalación y el adecuado funcionamiento de los servicios de Internet.
- Elaborar proyectos de expansión de servicios hacia zonas de interés de la Universidad que requieren conectividad: internet, telefonía, telemetría, video conferencia, etc.
- Realizar términos referenciales y pliegos de consultoría para la contratación de estudios de telecomunicaciones y electrónicos.
- Planificación, diseño, implementación y monitoreo para la optimización de los servicios de gestión académica.
- Capacitar a los usuarios en el manejo tanto de software adquirido como del software desarrollado por la sección.
- Establecer las políticas de seguridad y respaldo de los sistemas informáticos de la institución.
- Planificación y distribución adecuada de los diferentes anchos de banda para los servicios de Internet e intranet.
- Proveer de soporte técnico a todas las redes de equipos electrónicos que operan en la Universidad, esto es: sistemas de computación, equipos de transmisión-recepción (sistemas de micro-ondas, radiodifusión, Televisión), equipos de fibra óptica, ruteadores, switches, etc.
- Realizar la instalación, mantenimiento preventivo y correctivo; y reparación de los sistemas y equipos de telecomunicaciones e informáticos de la UNL.

6.3.3 Productos y servicios

6.3.3.1 Desarrollo de Software

- Estudio de perfeccionamiento del software que maneja la Universidad en sus diferentes áreas, centros especializados y departamentos.
- Pliegos para la adquisición o contratación de diseños o desarrollos de software especializado, en base a la planificación o proyectos aprobados.
- Planes de diseño, implementación y monitoreo para la optimización de los servicios de gestión académica.
- Planes de perfeccionamiento y control de los diferentes paquetes de software que manejan cada una de las áreas.

- Diseño de software para la automatización y control de los procesos académicos administrativos de la Universidad: Estadísticas, trámites, archivo.
- Informes de soporte técnico y mantenimiento de software otorgado a todos los sistemas que se encuentran en ejecucipon en las áreas, centros especializados y unidades universitarias.
- Fichas técnicas del apoyo en software realizado a la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, para prácticas educativas.
- Planes de adquisición de software e implementación del hardware adquirido como del software desarrollado por la subunidad.
- Informes de aplicación de las políticas de seguridad y respaldo de los sistemas informativos de la institución.

6.3.3.2 Redes y Equipos Informáticos

- Planes de diseño y perfeccionamiento de las redes y equipos informáticos de la Universidad en sus diferentes Áreas, Centros Especializados y Departamentos.
- Informes de mantenimiento del servicio de Internet.
- Planes de implementación de nuevas redes informáticas, según los requerimientos universitarios.
- Planes de distribución adecuada de los diferentes anchos de banda para los servicios de Internet.
- Informes de optimización en la distribución y utilización de redes, subredes y equipos informáticos que presentan servicios de internet.
- Informes de apoyo técnico a la carrera de Ingeniería en Sistemas en la ejecución de prácticas especializadas.
- Planes de cambios o actualizaciones de tecnología en redes computacionales.
- Informes de aplicación de políticas de seguridad para la utilización de la intranet de la universidad.
- Plan de optimización del rendimiento de las redes y equipos informáticos.

6.3.3.3 Electrónica y Telecomunicaciones

- Plan de implementación, mantenimiento y reparación de equipos de telecomunicaciones e información de la Universidad Nacional de Loja.

- Plan de distribución de redes de telecomunicaciones con sus respectivos componentes, memorias técnicas, diseños, detalles constructivos, especificaciones técnicas de cada uno de los proyectos.
- Plan de estudios de perfeccionamiento de las redes que brindan servicios de telecomunicaciones e información a la ciudad universitaria y sus extensiones universitarias, para el ordenamiento e integración, mediante propuesta de conectividades en sus diferentes modalidades.
- Plan de control de las instalaciones y el adecuado funcionamiento de los servicios de Internet.
- Diseño para la optimización de las redes de telecomunicaciones de las diferentes dependencias de la Universidad: TELEMEDICINA, TELEDUCACIÓN, enlaces micro-onda. Fibra óptica y otros.
- Proyectos de expansión de servicios hacia zonas de interés de la Universidad que requieren conectividad: Internet, Telefonía, Telemetría, Videoconferencia y otros.
- Informes de apoyo técnico de las actividades relacionadas a conectividad con los proyectos generados en los Centro de investigación de la Universidad.
- Términos de referencia y pliegos de consultoría para la contratación de estudios de telecomunicaciones y electrónicos.
- Informes de apoyo técnico para la construcción y fiscalización de infraestructura física para informática y telecomunicaciones, principalmente en lo concerniente a casetas, torres, ductos; y, adicionales mecánicos cuando el caso lo requiera.
- Informes de apoyo técnico al Área de Ingeniería Electrónica y Telecomunicaciones, en prácticas pre profesionales **[37]**.

e. Materiales y Métodos

El presente proyecto de tesis fue desarrollado mediante el uso de diferentes recursos materiales, técnicas, métodos científicos de investigación y recolección de información bibliográfica pertinente para su sustentación teórica con el fin del cumplimiento de los objetivos planteados, a continuación se describe:

1. Materiales

El proyecto fue desarrollado utilizando diferentes tipos de recursos materiales, los cuales están descritos a continuación:

1.1 Recusos Humanos:

- Autora del proyecto de tesis (María Gabriela Pardo Cuenca).
- Director de tesis (Ing. Mario Palma)

1.2 Recusos Materiales:

Entre los que tenemos:

1.2.1 Materiales de Oficina:

- Papel para impresión formato A4.
- Suministros para impresión (cartuchos canon 210 y 211).
- Fotocopias de la documentación final.
- Discos compactos.

1.2.2 Servicios Básicos

- Pago de servicio de transporte.
- Pago de servicio de internet y comunicaciones.

1.3 Recursos Técnicos y Tecnológicos

- Computador portátil Toshiba M645-SP4131L
- Memoria Flash de 16GB
- Impresora Canon MP250

1.4 Software

- Licencia para Windows 7 home Premium
- Ganntt Project
- Paquete de software de ofimática (Libre Office)

- Herramienda para análisis de riesgos para metodología MAGERIT v3 (EAR/PILAR 5.4)

2. Método

Método Deductivo: este método permitió la recopilación bibliográfica permitiendo esclarecer conceptos básicos y obtener información que establezca las bases teóricas del proyecto lo mismo que permitió el desarrollo eficaz para la obtención de resultados, permitiendo determinar la solución más adecuada para la adaptación de la norma ISO/IEC 27001 a la Unidad de Telecomunicaciones e Información generando políticas seguridad de la información basadas en su realidad actual en cuanto a riesgos informáticos en sus activos de información.

3. Técnicas

Para la recolección de la información para el desarrollo del proyecto, se ha hecho uso de las siguientes técnicas de investigación:

Entrevista: se utilizó esta técnica en cada fase del proyecto, para con ella obtener información sobre la situación actual de la UTI en cuanto al manejo de seguridad de la información; para determinar la clasificación e inventario de activos de información, determinar su valor en cuanto a su criticidad, las amenazas y vulnerabilidades asociadas a los mismos.

Observación: se hizo uso de esta técnica durante el desarrollo de todo el proyecto, para la obtención de información de importancia, sobre las actividades que se realizan en la UTI, la aplicación de las normativas de seguridad vigentes y el funcionamiento interno de cada sección.

Análisis de Información: esta técnica fue una de las más importantes ya que es la que ha permitió definir en primera instancia las necesidades de seguridad de la información en la UTI, fue clave en la definición de resultados para el análisis de riesgos y definición de los mecanismos de control necesarios en la mitigación de riesgos, y finalmente permitió la creación del *Manual de Políticas de Seguridad de la Información* para la UTI.

Encuesta: se utilizó esta técnica en la fase final del proyecto para la validación de los resultados obtenidos a partir de la socialización del proyecto con el personal técnico de la UTI.

4. Metodología

El proyecto de tesis se lo realizó utilizando los lineamientos definidos en la Norma ISO/IEC27001, tomando como refencia, para el análisis de riesgos, los pasos propuestos en la metodología MAGERIT, partiendo del análisis de la situación actual de la Unidad de Telecomunicaciones e Información en cuanto a seguridad de la información se refiere.

De esta forma se definieron cuatro fases, con tareas a ser cumplidas, descritas a continuación:

Fase Uno: Diagnóstico de la situación actual de la organización:

- Obtener información sobre los controles de seguridad actuales que se manejan en la organización
- Obtener información sobre los activos de información para el estudio
- Obtener información sobre la estructura organizacional interna

Fase Dos: Análisis de Riesgos Informáticos asociados a los activos de información.

- Definir la metodología de análisis de riesgos adaptada a la organización.
- Establecer criterios de aceptación para los riesgos.
- Definir el valor de los activos de información para la organización bajo las dimensiones de criticidad establecidas.
- Identificar las amenazas y vulnerabilidades asociadas a los activos de información.

Fase Tres: Definición de mecanismos de control para el tratamiento de riesgos.

- Evaluar la probabilidad y el impacto de ocurrir un fallo de seguridad.
- Determinar el criterio de aceptación de los riesgos encontrados
- Identificar las opciones de tratamiento de riegos a partir de la selección de mecanismos de control establecidos en el Anexo A de la norma ISO/IEC27001.

Fase Cuatro: Documentación de aplicabilidad para el tratamiento de riegos.

- Definir los motivos de elección y/u omisión de los mecanismos de control.
- Definir la necesidad de continuidad de los controles actuales que se manejan en la organización.

f. Resultados

El trabajo de titulación, estuvo orientado al cumplimiento del objetivo general del mismo, conjuntamente con los objetivos específicos, para lo cual, se consideró dividirlo en cuatro fases con sus respectivas actividades, las cuales se han cumplido de forma ordenada y optima, a continuación se detalla el desarrollo de cada una:

Fase 1: Realizar el diagnostico a la situación actual, en cuanto a seguridad de la información, en función a la estructura organizacional y recursos tecnológicos disponibles en la UTI

1.1 Recolectar información referente a controles de seguridad aplicados actualmente la UTI para la gestión de la información.

Dentro de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja se han definido políticas de seguridad informática acorde a los objetivos, normativas y planes que la Universidad Nacional de Loja tiene respecto a su objetivo institucional, todo esto a partir del periodo 2012.

Los objetivos, planes y políticas, son supervisadas y aprobadas por la Dirección de Telecomunicaciones e Información, considerando la importancia de los servicios que esta ofrece a todas las entidades de la Institución, donde se deben considerar la información que es confiada para su protección, administración, revisión, adaptación, etc., así como también toda acción de incorporación de tecnología y servicios informáticos para la Institución, los mismos que son realizados bajo las normativas establecidas en los procesos de adquisición de equipos y recursos informáticos.

Las políticas institucionales de seguridad informática establecidas en la UTI, están basadas en la "Norma ISO/IEC 17799:2000 la cual es un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", donde esta norma ofrece recomendaciones en la gestión de la seguridad de la información, y define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad **[32].**

Dentro de la UTI, es importante considerar que el manual de políticas general, ha sido creado en base a los requerimientos y necesidades de cada una de las secciones de la Unidad, con el fin de lograr un mejoramiento en cuanto a los equipos informáticos, su distribución y manejo, así como los procesos llevados a cabo dentro de cada sección de la UTI.

Dentro de cada sección se llevan a cabo procesos bajo normas establecidas, donde su aplicación desde la apreciación de los directivos es de un 60% a 70% en forma general, pero al hablar dentro de cada sección la aplicación de las normativas es estricta y fundamentada, en base a las necesidades y actividades realizadas en cada una.

Es importante considerar que la UTI se maneja en base a políticas generales de seguridad informática así como también políticas establecidas en cada sección, como las que se describe a continuación:

POLÍTICAS GENERALES:

Políticas de Definición

- La Unidad de Telecomunicaciones e Información se constituye como Unidad de Servicios Informáticos y Telecomunicaciones para la Universidad Nacional de Loja.
- Los usuarios son responsables exclusivos de los datos que manipulen en los ordenadores proporcionados por la Universidad Nacional de Loja y están normados al uso que la Institución establece **[33]**.

Políticas de prestación de servicios

- Los servicios que la Unidad de Telecomunicaciones e Información en sus diferentes secciones son: Mantenimiento Electrónico, Redes y Equipos Informáticos, Telecomunicaciones y Desarrollo de Software.
- Los servicios prestados deben, para todos los casos, poseer una métrica de calidad, mediante la cual se midan: tiempos de respuesta, calidades de solución, calidades de satisfacción usuaria, entre otras variables.
- La prestación de servicios de las secciones de la Unidad de Telecomunicaciones e Información debe, en todo momento, estar dotado de trazabilidad de

procedimientos. Lo anterior implica procesos formales de solicitud de servicios, acción, respuesta y aceptación **[33]**.

Políticas de administración de recursos

- La administración y explotación de los sistemas de información serán realizadas con personal responsable perteneciente a la Universidad Nacional de Loja. Este personal está conformado por los profesionales que se encargan de la manipulación directa de la información el cual se identificara como Unidad de Telecomunicaciones e Información.
- Será responsabilidad de la UTI la administración de los recursos asociados a los sistemas de información y comunicación de la UNL. La responsabilidad por la administración de estos recursos.
- La UTI es responsable de la calidad (fidelidad, oportunidad, consistencia y redundancia) de la información de la cual es administrador técnico. Además, deberá definir normas de administración y acceso a la información proporcionada por quienes establezcan los procedimientos de control.
- La UTI deberá proveer los mecanismos de protección y control necesarios que aseguren la integridad y privacidad de los datos almacenados en los archivos y bases de datos que tenga en custodia.
- La UTI deberá proveer de los mecanismos de respaldo necesarios que aseguren la continuidad operativa ante siniestros que afecten a los archivos y bases de datos que tenga en custodia **[33].**

Política de coordinación de actividades

- Todo proyecto de modernización o innovación Tecnológicos que se lleve adelante en la Universidad Nacional de Loja que incluya aspectos relacionados con sistemas de información, equipos computacionales, software y transmisión de datos, voz e imágenes, contará con el apoyo logístico y técnico de la UTI **[33].**

Políticas de cobertura de los servicios

- La UTI procurará extender la cobertura de los servicios de tecnología de información a todas las áreas de la Universidad Nacional de Loja en la medida que ello sea posible y sea del interés de nuestra Institución **[33].**

Políticas de Salvaguarda y Confidencialidad

- Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza, que bajo cualquier medio le sea entregada de parte de la Universidad Nacional de Loja, y que forme parte de los datos, información, procedimientos, conocimientos, comportamientos, actividades, desempeños, funcionamientos, metodologías, rutinas, acciones y en general de toda expresión, en el medio que fuere, que pertenezca a la propiedad exclusiva de la Universidad Nacional de Loja.
- Se incluye en este punto, toda información de tipo comercial, financiero, metodológicas, de procesos, de conocimientos propios y adquiridos, experimentales, ya sea su conocimiento de carácter privado o público y que pertenezca a la Universidad Nacional de Loja **[33].**

Políticas de Protección de datos y sistemas

El equipo computacional perteneciente a la Universidad Nacional de Loja estará bajo la exclusiva administración de la UTI y por lo tanto queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:

- Manipulación no autorizada.
- Apertura, reemplazo y/o desconexión de componentes.
- Reasignaciones permanentes o temporales sin autorización.
- Instalación de programas, sistemas, módulos y/o archivos externos.
- Empleo de juegos y/o programas con fines no laborales.
- Modifica la configuración de sistemas, programas o dispositivos.
- Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.
- Conexión a redes eléctricas o de Datos no certificadas y o autorizadas

Respecto de lo definido con el fin de proteger las instalaciones, equipos, datos y sistemas de la acción de virus computacionales, será lo estipulado por la UTI lo que permanezca vigente y con prohibición para los usuarios el modificar y/o transgredir las disposiciones establecidas **[33].**

Políticas de documentación digital o Impresa

- Respecto a la documentación, toda la Unidad de Telecomunicaciones e Información deberá documentar todas sus actividades que realizan en la Institución, en un sistema informático de documentación y el sistema de registro de solicitudes de los usuarios de la institución, con el fin de medir el trabajo realizado y la eficiencia del servicio brindado.

Se debe considerar el uso de normativas exclusivas para cada una de las secciones de la UTI (***ver Anexo 3***) las cuales permiten el desarrollo adecuado de las actividades definiendo los procesos que se deben desarrollar para cada una de ellas.

A continuación se describen las políticas consideradas en cada sección:

Políticas de la Sección de Desarrollo de Software

Dentro de la Sección de Desarrollo de Software, se definen diferentes subsecciones consideras para ejecución de sus funciones, como son:

Desarrollo de nuevos Proyectos de la Universidad relacionados con tecnología de información, los mismos que deben estar incluidos en el Plan de Desarrollo de la UTI y ser autorizados por las autoridades máximas de la Universidad o estructura administrativa competente. Donde existen consideraciones para contrataciones para desarrollo de sistemas con empresas externas.

Metodologías de Desarrollo donde las políticas establecidas pretenden garantizar el desarrollo de sistemas mediante técnicas estructuradas de análisis y diseño de sistemas, así como el almacenamiento de datos del sistema a ser desarrollado en base a las estructuras establecidas en la Institución.

Demandantes, mantenimiento y explotación de Sistemas, al momento del diseño un nuevo sistema que sea requerido por diferentes áreas demandantes, debe existir comprometimiento y colaboración para el desarrollo efectivo del mismo, así como también al momento del mantenimiento de algún sistema, este debe llevarse a cabo

bajo la dirección de la UTI donde se establecerán los recursos, plazos y costos. Una vez finalizado el desarrollo, al momento de la explotación del sistema el personal encargado de la administración de los equipos e información deberá asumir su responsabilidad, así como el personal de la UTI será el encargado de proporcionar o coordinar la capacitación de usuarios para la incorporación, operación y uso de sistemas de información desarrollados.

Cabe considerar que dentro de la sección los controles aplicados, se basan en el manejo de usuarios como es el caso de auditorías de usuarios administrativos (secretarios, secretarios abogados, auxiliares) respecto al SGA, también la creación de usuarios para delegación de funciones, buscado la centralización, para evitar duplicidad, también se considera dentro de los controles importantes el manejo de servidores, buscando la centralización de los mismos en un solo servidor blade, actualmente el 80% de los servicios que ofrece el SGA se encuentra en el servidor, aún falta la migración de algunos de los servicios debido a la complejidad de configuraciones **[33].**

Políticas de la Sección de Mantenimiento Electrónico.

Dentro de la Sección de Mantenimiento Electrónico se definen subsecciones o servicios para la ejecución de sus funciones y tareas, entre estas subsecciones tenemos:

Mantenimiento Preventivo y Correctivo de los Recursos Informáticos, el objetivo de esta es mantener el control de las visitas mediante un cronograma de trabajo y normas orientadas a los usuarios que facilitaran el trabajo de los técnicos del área de mantenimiento.

Servicio de Soporte Técnico este servicio se ofrece a través de reserva de turnos que permite resolver los problemas oportunamente.

Mantenimiento de las configuraciones computacionales que es responsabilidad del personal técnico de la Sección de Mantenimiento Electrónico.

Respaldo de Información, existen normativas que permiten gestionar de forma adecuada los procedimientos para respaldo de información que corresponde a la Sección de Mantenimiento Electrónico, donde se consideran diferentes tipos de respaldo sobre equipos informáticos de la Institución.

Estaciones de Trabajo, dentro de la sección de Mantenimiento Electrónico se mantienen políticas de adquisición, control y mantenimiento de microcomputadores.

Administración de equipamiento la sección de Mantenimiento Electrónico ha establecido políticas para la asignación de equipos a usuarios finales nombrándolos como custodios responsables de los mismos.

Derechos de Autor y Propiedad Intelectual del Software, para esta tarea la sección de Mantenimiento considera dos categorías (shareware, freeware) para la adquisición de nuevo software, donde la licencia que se otorga al software determina las condiciones de uso del mismo **[33].**

Cabe considerar que las políticas son aplicadas al 100%, considerando como la más importante mantener los respaldos de los equipos así como la seguridad de la información respaldada.

Políticas de la Sección Redes y Equipos Informáticos

El objetivo principal de las políticas de esta sección es regular el uso de los servicios de Redes, Correo Electrónico y el acceso a Internet, para lo cual se emiten los siguientes lineamientos para todo el personal que utilice los recursos de Red.

La Sección de Redes y Equipos Informáticos cumple con diferentes tareas las mismas que tienen políticas a ser cumplidas como son:

Redes de Microcomputadores donde bajo la coordinación de la UTI se crean y se supervisan nuevas conexiones para permitir el acceso a diferentes ambientes, independientes de su ubicación.

Estándares Aplicables en la Instalación de redes de datos, al momento de realizar instalación de los diferentes tipos de redes de datos que son requeridos a la UTI se consideras los estándares de cableado estructural como:

- **EIA/TIA 568B** (Estándar de cableado para telecomunicaciones en edificios comerciales.)
- **EIA/TIA 569A** (Estándar de cableado para telecomunicaciones en edificios comerciales rutas y espacios).
- **EIA/TIA 606A** (Estándar de administración para la infraestructura de telecomunicaciones en edificios comerciales).

- **EIA/TIA 607A** (Requerimientos para uniones y puesta a tierra para telecomunicaciones en edificios comerciales) **[34, 35]**

De la misma forma se considera políticas en cuanto a riesgos laborales **OSHA 1800 y 9001** para trabajo del personal, donde dicha norma hace que la organización controle los riesgos laborales derivados de la práctica de su actividad y mejore su ejecución ***[2,5]***.

Uso de la Red, la UTI con su sección de Redes es responsable de ofrecer servicios con fines académicos, donde todo el personal perteneciente a la Institución puede hacer uso de la red siempre y cuando sea un usuario autorizado como son: alumnos activos, profesional, docentes, personal de apoyo, departamentos y direcciones. Los servicios ofrecidos por la UTI son: conectividad a la red local (LAN) con nodos alámbricos e inalámbricos, acceso a Internet, acceso a servicio ofrecidos por la UNL (correo electrónico institucional, bibliotecas virtuales, etc.), cabe considerar que la UTI reserva sus derechos a denegar o restringir servicios de red que pudiesen ocasionar inconvenientes de tráfico, mal manejo de información o que ocasione inconvenientes de seguridad dentro de la red de datos. Es importante considerar las facultades que tiene la UTI en cuanto al manejo de la red como es la reserva del derecho a monitorear las cuentas que presente un comportamiento sospechoso para la seguridad de la UNL y su comunidad, y a partir de esto aplicar las sanciones correspondientes donde por incumplimiento por parte del usuario del buen uso se puede suspender y dar de baja su cuenta **[33].**

Políticas de la Sección de Telecomunicaciones

El objetivo de las normativas establecidas en la Sección de Telecomunicaciones de la UTI es preservar la integridad de los equipos de radiocomunicación y equipos computacionales utilizados en la Institución. Así como también se han establecido las normas de comportamiento que el personal debe acatar al hacer uso de salas de cómputo de la Institución, así como las sanciones pertinentes al infringir alguna de las normativas.

1.2 Recolectar información sobre la administración de los activos tecnológicos existentes en la UTI

Para la recolección de información referente a la administración de los activos de información de la UTI, se lo ha realizado mediante la utilización de registros que

mantienen las diferentes secciones de la UTI, de acuerdo a los equipos que tienen a su cargo.

Los equipos tecnológicos a cargo de la UTI están esquematizados en la topología de red levantada por parte de la sección de Redes y Equipos Informáticos junto con la Sección de Telecomunicaciones ***(ver Anexo 4)***, la Sección de Desarrollo de Software cuenta con un inventario de aplicaciones ***(ver Anexo 5)*** , finalmente la Sección de Mantenimiento Electrónico, se lo ha tomado como un caso especial ya que esta sección está a cargo de todos los equipos informáticos que maneja el personal universitario en diferentes áreas, oficinas, centros de cómputo y bibliotecas, como son equipos de computación de escritorio y portátiles, equipos de impresión y proyectores, para lo cual se los ha agrupado en categorías para generalizar su tratamiento, a continuación se muestran una tabla resumen de acuerdo a cada sección que existe en la UTI ***(ver Tabla III)***.

TABLA III. Inventario de Activos de Información de la UTI

INVENTARIO DE ACTIVOS DE INFORMACIÓN					
CÓDIGO	***TIPO***	***CARACTERISTICA***	***DESCRIPCIÓN***	***RESPONSABLE***	***LOCALIZACIÓN***
TEC001	TECNOLOGIA	CISCO	**INFORMACIÓN CONFIDENCIAL**	SECCIÓN DE REDES Y EQUIPOS INFORMÁTICOS / SECCIÓN DE TELECOMUNICACIONES	EDIFICIO DE ADMINISTRACIÓN CENTRAL - UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN
TEC002	TECNOLOGIA	DISTRIBUCIÓN DE SERVIDORES			
TEC003	TECNOLOGIA	Web-Mail			
TEC004	TECNOLOGIA	WEB			
TEC005	TECNOLOGIA	SGA (Servicios)			
TEC006	TECNOLOGIA	Med Cursos			
TEC007	TECNOLOGIA	AEIRNNR			
TEC008	TECNOLOGIA	MED Virtual			
TEC009	TECNOLOGIA	EVA			
TEC010	TECNOLOGIA	Financiero			
TEC011	TECNOLOGIA	Cursos			
TEC012	TECNOLOGIA	Blade			
TEC013	TECNOLOGIA	SGAGW2			
TEC014	TECNOLOGIA	Proxy Wirelles			
TEC015	TECNOLOGIA	SGAGW			
TEC016	TECNOLOGIA	DNS-DHCP			
TEC017	TECNOLOGIA	NOC			
TEC018	TECNOLOGIA	OS-Ticket			
TEC019	TECNOLOGIA	Nagios			
TEC020	TECNOLOGIA	Nessus			
TEC021	TECNOLOGIA	Radius			
TEC022	TECNOLOGIA	ASA			

TEC023	TECNOLOGIA	CONTROLADORA	INFORMACIÓN CONFIDENCIAL		
TEC024	TECNOLOGIA	CONTROLADORA WLC			
TEC025	TECNOLOGIA	UBIQUITI			
TEC026	TECNOLOGIA	Motorola			
TEC027	TECNOLOGIA	CMM MICRO			
TEC028	TECNOLOGIA	CMM MICRO			Área de la Salud
TEC029	TECNOLOGIA	CMM MICRO			San Cayetano
TEC030	TECNOLOGIA	CMM MICRO			Extensión MOTUPE
TEC031	TECNOLOGIA	SWITCHES (diferentes marcas y características)			Diferentes áreas y departamentos de la Universidad.
TEC032	TECNOLOGIA	ACCESS POINT			Diferentes áreas y departamentos de la Universidad.
TEC033	TECNOLOGIA	ROUTER			Bloque de nivelación y bloque de estadio
TEC034	TECNOLOGIA	RELOJ BIOMÉTRICO			Diferentes áreas y departamentos de la Universidad.
TEC035	TECNOLOGIA	SERVIDOR PROXI			Diferentes áreas y departamentos de la Universidad.
TEC036	TECNOLOGIA	CENTRALILLAS TELEFÓNICAS			Ubicadas en cada una de las Áreas de la Universidad
INT001	INSTALACIONES	CENTRO DE CARGA			Instalaciones de la Unidad de Telecomunicaciones e Información.
INT002	INSTALACIONES	TENDIDO DE LA RED DE DATOS ALÁMBRICA			Diferentes áreas y departamentos de la Universidad.
INT003	INSTALACIONES	RED DE CONEXIÓN INALAMBRICA			Campus Universitario
INT004	INSTALACIONES	ENLACES DE CONEXIÓN			Campus Universitario
APL001	APLICACIONES	Sistema de Gestión Académica		SECCIÓN DE DESARROLLO DE SOFTWARE	Instalaciones de la Unidad de Telecomunicaciones e Información.
APL002	APLICACIONES	Consulta de Estadísticas del SGA			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL003	APLICACIONES	Sistema de Gestión de Aprendizaje Moodle (modalidad presencial y a distancia)			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL004	APLICACIONES	Sistema de Evaluación de Docentes			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL005	APLICACIONES	Sistema de Gestión Documental Quipux			Instalaciones de la Unidad de Telecomunicaciones e Información.

APL006	APLICACIONES	Limesurvey	INFORMACIÓN CONFIDENCIAL		Instalaciones de la Unidad de Telecomunicaciones e Información.
APL007	APLICACIONES	Sistema de Gestión Bibliotecaria			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL008	APLICACIONES	OSTicket			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL009	APLICACIONES	Gestión Académica de Carrera			Algunas carreras
APL010	APLICACIONES	Forestweb			Laboratorio de Análisis de Madera, Carrera de Ingeniería Forestal
APL011	APLICACIONES	Sistema de Seguimiento de Egresados y Graduados			Instalaciones de la Unidad de Telecomunicaciones e Información.
APL012	APLICACIONES	Sistema de emisión y reposición de títulos			Secretaria General de la Universidad
APL013	APLICACIONES	Página web de la Universidad			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT001	DATOS	Sistema de Gestión Académica			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT002	DATOS	Consulta de Estadísticas del SGA			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT003	DATOS	Sistema de Gestión de Aprendizaje Moodle (modalidad presencial y a distancia)			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT004	DATOS	Sistema de Evaluación de Docentes			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT005	DATOS	Sistema de Gestión Documental Quipux			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT006	DATOS	Limesurvey			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT007	DATOS	Sistema de Gestión Bibliotecaria			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT008	DATOS	OSTicket			Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT009	DATOS	Gestión Académica de Carrera			Algunas carreras
DAT010	DATOS	Forestweb			Laboratorio de Análisis de Madera, Carrera de Ingeniería Forestal

DAT011	DATOS	Sistema de Seguimiento de Egresados y Graduados	INFORMACIÓN CONFIDENCIAL		Instalaciones de la Unidad de Telecomunicaciones e Información.
DAT012	DATOS	Sistema de emisión y reposición de títulos			Secretaria General de la Universidad
DAT013	DATOS	Página web de la Universidad			Instalaciones de la Unidad de Telecomunicaciones e Información.
EAX001	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS		SECCIÓN DE MANTENIMIENTO ELECTRÓNICO	Oficinas o departamentos del personal administrativo
EAX002	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS			Oficinas o departamentos del personal docente
EAX003	EQUIPOS AUXILIARES	PROYECCIÓN AUDIO-VISUAL			Oficinas o departamentos del personal docente
EAX004	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO			Oficinas o departamentos del personal administrativo
EAX005	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO			Centros de cómputo o bibliotecas de las diferentes áreas de la Universidad
EAX006	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO			Oficinas o departamentos del personal docente
EAX007	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES			Oficinas o departamentos del personal administrativo
EAX008	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES			Oficinas o departamentos del personal docente
EAX009	EQUIPOS AUXILIARES	EQUIPOS Y/O HERRAMIENTAS PARA MANTENIMIENTO			Sección de mantenimiento de Informático

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

Cabe considerar que existen propuestas para cambios en la distribución de la topología de la red implantada actualmente, donde se propone migrar a partir del diseño topográfico plano a un diseño jerárquico, donde se implementaran nuevos y modernos equipos de gran importancia para el mejoramiento de la seguridad de la información, monitoreo y administración, en la sección de Redes y Equipos Informáticos.

1.3 Recolectar información sobre los roles y actividades que realiza el personal técnico y administrativo de la UTI

Dentro del Estatuto por procesos de la Universidad Nacional de Loja [37], se estipula la organización de la Unidad de Telecomunicaciones e Información, donde consta la distribución de atribuciones y responsabilidades, así como la descripción de los productos y servicios que aquí se ofrecen.

A partir de esto se esquematiza el orgánico estructural vigente en la Unidad al 2014.

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

Figura 7 Orgánico Estructural de la UTI

Se debe considerar que el orgánico estructural ***(ver* Figura 7*)*** esta normalizado con sus secciones y responsables de los mismas pero la delegación de funciones en algunos casos no está inscrita solamente se ha llegado a acuerdos internos con los responsables de la sección, como es el caso de la *Sección de Desarrollo de Software* y la *Sección de Mantenimiento Electrónico* donde los responsables en su rol de trabajo no constan como directivos de la sección.

A partir de la estructura orgánica establecida en la UTI, se encuentran identificadas las ***funciones y responsabilidades*** de cada una de las áreas o secciones, así como la misión y responsabilidades generales de la unidad (ver Sección 4.3 de la Revisión de Literatura).

Es importante considerar que dentro de cada sección no existen normativas dedicadas a resolver inconvenientes y delegación de funciones claras a cada miembro de la unidad donde todos los miembros realizan diferentes actividades, y no existe una correcta distribución de trabajo, donde actualmente se atienden las necesidades a prioridad o conforme se presentan a la Unidad, lo que genera inconvenientes en el control de actividades y en la organización del personal.

Uno de los principales inconvenientes presentes en cada sección es el personal limitado para la ejecución de funciones, donde los directivos de cada sección organizan las actividades, buscando cubrir las necesidades presentes de forma óptima y eficiente con el personal limitado con el que se cuenta.

1.4 Recolectar información sobre los procesos que se llevan a cabo dentro de la UTI, en las diferentes áreas de trabajo.

Dentro de la Unidad de Telecomunicaciones e Información, de acuerdo a cada sección de trabajo se tienen a cargo diferentes actividades las mismas que basadas en las políticas y normas establecidas se llevan a cabo, por parte del personal designado.

De forma general, al hablar de la Unidad de Telecomunicaciones e Información se constituye como Unidad de Servicios Informáticos y Telecomunicaciones para la Universidad Nacional de Loja.

Donde los usuarios son responsables exclusivos de los datos que manipulen en los ordenadores proporcionados por la Universidad Nacional de Loja y están normados al uso que la Institución establece.

Al hablar de los procesos y flujos de trabajo que se realizan en cada sección, estos no se encuentran normalizados, donde los procesos se realizan de forma rudimentaria atendiendo los requerimientos de forma prioritaria y buscando solucionarios de acuerdo a la naturaleza de los mismos, más no utilizando documentos o plantillas estandarizadas que permitan tener un control claro y preciso de las actividades que se realizan en cada sección. Cabe considerar que los directivos de cada sección han organizado las actividades y los procesos de acuerdo a su experiencia procurando cumplir con las funciones encomendadas de manera óptima y con los tiempos establecidos.

1.5 Analizar la información recolectada para la determinación de la situación actual dentro de la UTI que permite determinar el alcance del SGSI

A partir de la información recolectada, comentarios y sugerencias del personal se tiene una visión general de lo concerniente a la seguridad de la información dentro de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, donde se ha considerado diferentes puntos de importancia que permiten definir el alcance del modelo de gestión de seguridad planteado.

1. Considerando los controles de seguridad informática descritos en el manual general que la UTI maneja, se puede decir que este permite a cada sección mantener un control general sobre las actividades que debe realizar, pero no se profundiza en la forma en cómo se realizan los procesos, ni determina la forma en como estos deben realizarse, por lo tanto cada sección realiza sus actividades en base a normativas establecidas por el director de sección de forma extraoficial

y de acuerdo a las necesidades, siendo estas adaptadas a las demandas de los usuarios y no de forma estandarizada, lo que dificulta el control de actividades.

2. En cuanto a los activos tecnológicos o equipos informáticos que maneja la UTI, la sección de *Redes y Equipos Informáticos* y la sección de *Telecomunicaciones* mantienen el registro de las características, posición y configuración de cada uno de ellos así como también se realiza monitoreo frecuente con el fin de evaluar el funcionamiento de estos, reducir brechas de seguridad que puede repercutir en intromisiones externas que alteren el funcionamiento adecuado de la red de datos de la Universidad, así como también controlar el estado funcional de servicio de los equipos para el mantenimiento de hardware y software de los mismos.

   Es importante considerar que se están realizando cambios para el mejoramiento de servicios y seguridad en cuanto a los servidores que maneja la Unidad, con la migración de los mismos a un servidor blade que permite aprovechar el espacio, reducir el consumo de energía y simplificar su monitoreo y control, cabe destacar que actualmente la UTI presentó un proyecto para el mejoramiento de la red de datos de la Universidad, en cuanto al diseño de su topología haciendo que esta cambie del diseño plano a un diseño jerárquico, con nuevos equipos y tecnología, que permitirá mejorar los servicios informáticos ofrecidos por la UTI.

   En cuanto a la sección de Desarrollo de Software, se mantiene el registro de las aplicaciones desarrolladas o instaladas para el funcionamiento adecuado de los sistemas de información que maneja la UTI para la Universidad.

   En la sección de Mantenimiento, debido a que están a cargo del mantenimiento de todos los equipos informáticos de la Universidad, se ha generalizado en tipos de activos con el fin de que el modelo de seguridad pueda abarcar el tratamiento en la seguridad de todos los activos.

3. En cuanto a las actividades y roles que se realizan en cada sección, estos se encuentran estipulados en el estatuto por procesos de la Universidad, donde se describe de forma general las funciones y actividades que se realizan en la unidad, siendo este el orgánico funcional, a partir del cual se describe el orgánico estructural de la UTI, es importante considerar que el personal asignado para el cumplimiento de sus funciones, en algunos casos no está asignado legalmente

a sus funciones, sino que realiza las mismas a partir de las disposiciones del director de la UTI.

Al hablar de las funciones y actividades que se realizan en cada sección, el estatuto dispone de forma general las responsabilidades inherentes al cargo que ocupan, pero estas no son todas, cada director en sus funciones organiza y asigna actividades para ser realizadas en base a las necesidades institucionales presentadas en la UTI, las mismas que son realizadas en base a la prioridad de la misma y de acuerdo al criterio del personal, así mismo los directores de cada sección crean planes para la ejecución de las actividades en base a la naturaleza de las mismas con el fin de poder llevar un control organizado y claro del trabajo de su sección, teniendo en cuenta que estos planes no están normalizados ni estandarizados.

Es importante considerar que en cuanto a la asignación de las actividades al personal estas no se encuentran normalizadas, es decir que las obligaciones y funciones de las secciones no están distribuidas de manera clara al personal donde cada persona realiza diferentes actividades y no solamente las que les corresponde a sus funciones.

4. A partir de lo observado y los comentarios de los directivos de cada sección se puede decir que en cuanto a los procesos para el desarrollo de las actividades estos no están organizados o normalizados, si no que el responsable de la sección asume el desarrollo de los mismos estableciendo el proceso para el desarrollo de actividades y el cumplimiento de funciones generando los resultados esperados para satisfacer las necesidades que los usuarios han presentado a la unidad.

Fase 2: Identificar los riesgos a los que está expuesta la información manejada en la Unidad de Telecomunicaciones e Información.

2.1 Definir la metodología de evaluación de riesgos apropiada para la planificiación del SGSI.

Para la definición de la metodología de evaluación del riesgo, es importante considerar que la norma ISO/IEC 27001 es flexible en cuanto al uso de la metodología, por lo tanto existen numerosas metodologías disponibles para el análisis de riesgos, partiendo de ello se han considerado las más utilizadas, donde se ha analizado dichas metodologías a partir de criterios generales con el fin de elegir aquella que se ajusta a las necesidades y permita obtener información relevante en el análisis de riegos, así como también facilite la aplicación y comprensión de los resultados ya que la seguridad de la información es responsabilidad de todas las personas que son parte directa o indirectamente de la Unidad de Telecomunicaciones e Información **[28,29]**

Partiendo de lo mencionado anteriormente, se ha creado una tabla esquematizada (ver TABLA IV) de las opciones elegidas, así como su tabla (ver TABLA V) comparativa a partir de la cual se ha identificado la opción más adecuada para el desarrollo del trabajo.

TABLA IV. Resumen de características asociadas a metodologías de análisis de riesgos

METODOLOGÍA	DESCRIPCIÓN	CARACTERÍSTICAS					
		Versión e Idioma	***Ventajas***	***Desventajas***	***Faces***	***Documentación***	***Software***
OCTAVE Operationally Critical Threat, Asset and Vulnerability Evaluation	Técnica de planificación y consultoría estratégica en seguridad basada en los riesgos ***[28,29]***.	2001 - 2007 Presenta tres versiones: ***OCTAVE*** (versión original), ***OCTAVE-S*** (Versión para pequeñas empresas), ***OCTAVE-ALLEGRO*** (versión simplificada) ***[[28,29]***	La definición de los riegos y amenazas se basan en los activos definidos como críticos ***[28,29]***	Se especializa en el riesgo de tipo organizacional ***[28]***.	**Fase 1: Visión Organizativa** Activos, Amenazas, Prácticas actuales, Vulnerabilidades organizativas, Requerimientos de seguridad ***[28,29]***	No posee documentación oficial para desarrollo o aplicación del método, pero existe una guía de implementación en tres versiones: *OCTAVE METHOD, OCTAVE-S METHOD, OCTAVE Allegro Method* ***[28,29]***	No posee herramientas informáticas oficiales para su aplicación ***[28,29]***
			Identifica los riesgos de la seguridad que pueden impedir la consecución del objetivo de la organización ***[28,29]***	Para la implementación no posee ayuda técnicas, no tiene una herramienta informática que facilite su aplicación ***[28]***.			
	Conjunto de herramientas, técnicas y métodos para desarrollar análisis de riesgos basado en la gestión y planeación estratégica de la organización ***[28,29]***		Crea una estrategia de protección con el objetivo de reducir los riegos de seguridad de la información prioritaria ***[28,29]***.	No posee documentación específica orientara a guiar paso a paso su aplicación ***[28].***	**Fase 2: Vista Tecnológica** Componentes clave, Vulnerabilidades técnicas ***[28,29]***		
			Identifica las amenazas y vulnerabilidades tanto organizativas como tecnológicas ***[28,29]***		**Fase 3: Estrategia y desarrollo del plan** Riesgos, Estrategia de protección, Planes de mitigación ***[28,29]***		
	Desmitifica la falsa creencia de: "La Seguridad Informática es un asunto meramente técnico ***[28,29]***	**Idioma:** *INGLÉS* ***[1]***	Es compatible con la norma ISO27001 ***[28]***				
EBIOS	Es una herramienta de gestión para los sistemas de seguridad informática, creada por la Dirección Central de Seguridad de los Sistemas de	Iniciada en 1995 Mantenida por DCSSI **Idioma:** *Francés* **[5,30]**	Compatible con normas internacionales como la ISO 13335 (GMITS), ISO 15408 (criterios comunes) y la ISO 17799 ***[5,29]***.	Por su fecha de origen no se acopla adecuadamente a los cambios y mejoras establecidos en la norma ISO/IEC 27001 ***[5,30]***	**1. Estudio del contexto** Durante este proceso se realiza un análisis de los activos de la organización ***[5,31]***	Se mantienen los usuarios activos que contribuyen al desarrollo del método y mantener actualizada la información respecto al método.	El software libre de asistencia para la utilización del método puede obtenerse solicitándolo a la DCSSI ***[5,30,31]***
			Permite ser utilizado para estudiar tanto sistemas		**2. Expresión de las necesidades de seguridad**		

	Información de Francia[7] ***[5,29]***.		por diseñar como sistemas ya existentes ***[5,29]***.			Juego de guías para su aplicación [***31]***	
			Es adaptativo al contexto de cada organización y se ajusta a sus herramientas y costumbres metodológicas ***[5]***.		Estudio de las necesidades de seguridad para los activos determinados ***[5,31]***		
			Presenta y describe los tipos de entidades, métodos de ataque vulnerabilidades, objetivos de seguridad y requerimientos de seguridad ***[5,30]***.		**3. Estudio de amenazas** Estudio de las amenazas y vulnerabilidades a las que está expuesta la organización ***[5,31]***		
					4. Expresión de los objetivos de seguridad Se dedica a disminuir los riesgos ***[5]***		
					5. Determinar los requerimientos de seguridad Determinar las funcionalidades de seguridad esperadas, así como el cumplimiento de los objetivos de seguridad sugeridos ***[5,31]***		
MAGERIT (Metodología de Análisis de Gestión de Riesgos de sistemas de Información)	Desarrollada por el Ministerio de Administraciones Públicas español, esta metodología de análisis de riesgos describe los pasos para realizar un análisis del estado de riegos y para gestionar su mitigación., enfocada a la información mecanizada y a los sistemas	VERSIÓN 1: 1997	Divide los activos de la organización en varios grupos, para identificar mayor cantidad de riegos y amenazas ***[24,27]***.	El software desarrollado específicamente para el método, necesita de licencias de uso de tipo privativo, se debe gestionar una licencia para evaluación ***[24,27]***.	1. Identificación de activos	Libro I Método	Herramienta PILAR *(Herramienta de Análisis y Gestión de Riesgos)* ***[24,27]***
		VERSIÓN 2: 2005			2. Valoración de activos	Libro II Catálogo de Elementos	
		VERSIÓN 3: 2012	Se acopla a los requerimientos de la norma ISO/IEC 27001 ***[24,27]***.		3. Identificación de amenazas.		
		Idioma: *Español* ***[24,27]***	Documentación amplia y asociada a los requerimientos del método ***[24,27***		4. Determinación de Impacto.	Libro III Guía de Técnicas ***[24,27]***	
			Se adapta a cualquier tipo de organización ***[24,27]***		5. Determinación de Riesgo.		
					6. Identificación de Salvaguardias.		
					7. Riesgo Residual ***[24,27]***		

[7] Dirección Central de Seguridad de los Sistemas de Información de Francia (DCSSI)

	informáticos que la tratan ***[24,27]***.		Cuenta con una herramienta informática para su aplicación ***[24,27]***				
CRAMM	Metodología de análisis de riesgos desarrollada por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido ***[20, 24]***.	Fue creada en 1987, actualmente se encuentra en versión 5 **Idioma:** *Inglés [24]*	Dicada al análisis y gestión de riesgos de manera formal, disciplinada y estructurada, que pretende la protección de la confidencialidad, integridad y disponibilidad de un sistema de sus activos ***[20, 24]***. Busca construir los planes de recuperación de desastres y continuidad del negocio ***[20, 24].20, 24]***. Incluye herramientas de evaluación de riesgos que son compatibles con la norma ISO/IEC 27001 ***[20, 24]***. Cuenta con una herramienta informática para su aplicación	No posee documentación específica orientara a guiar paso a paso su aplicación ***[24]***	1. Identificar y Evaluar los bienes 2. Identificar las amenazas y vulnerabilidades calculando sus riesgos. 3. Identificar y priorizar las medidas de defensa o contramedidas ***[20, 24]***.	No posee documentación específica orientara a guiar paso a paso su aplicación ***[24]***	Herramienta CRAMM V (Tiene tres revisiones: CRAMM Expert, CRAMM Express, y BS7799) ***[20, 24]***.

TABLA V. Tabla comparativa de metodologías de análisis de Riesgos

CARACTERISTICA	METODOLOGÍA			
	OCTAVE	EBIOS	MAGERIT	CRAMM
Versión:	2007 en vigencia	Iniciada en 1995	Versión 3: 2012	Versión 5:2011
Idioma:	INGLÉS	FRÁCES	ESPAÑOL	INGLÉS
Normas Internacionales que es compatible	ISO/IEC 27001	ISO 13335 (GMITS), ISO 15408 (criterios comunes) y la ISO 17799.	ISO/IEC 27001	ISO/IEC 27001
Identificación de activos:	Lo realiza de forma general y se enfoca a aspecto organizacionales.	Análisis general de activos tecnológicos	Divide los activos en varios grupos para identificación de mayor cantidad de riesgos	Identificación de activos relevantes de la organización.
Plan de salvaguardias:	Estrategias de protección y planes de mitigación	Se dedica a la disminución de riegos en base al estudio de amenazas y evalúa el cumplimiento	Identifica las salvaguardias en base a la determinación del impacto y su riesgo.	Identifica y prioriza las medidas de defensa o contramedidas.
Documentación asociada	No posee documentación oficial, pero presenta guías de aplicación del método en tres versiones diferentes	Se mantienen usuarios activos que contribuyen al desarrollo del método y dan soporte	Contiene amplia documentación con 3 guías de aplicación: Libro I Método, Libro II Catálogo de Elementos y Libro III Guía de Técnicas	No posee documentación oficial para aplicación.
Herramienta Informática	No posee herramienta informática	EBIOS: licencia libre que debe ser gestionado con la DCSSI	*PILAR 5.4.2* con licencia comercial y/o licencia de evaluación que debe ser gestionada con los desarrolladores	Herramienta CRAMM V (tiene 3 versiones: CRAMM Expert, CRAMM Express y BS7799)

Partiendo del análisis de las características más relevantes de las metodologías y de la documentación considerada se ha determinado que la metodología de análisis más apropiada es la ***MAGERIT*** que actualmente trabaja en la versión 3, debido a su características de orden y cumplimiento en la realización del análisis de riesgos, así como la documentación asociada a la misma que permite realizar un trabajo eficaz, considerando también que por su origen, tanto como la documentación y su herramienta están en idioma español.

Este método nos permite facilitar la implementación y aplicación de esquemas de seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información, partiendo de los criterios de valoración de los activos (disponibilidad, integridad y confidencialidad), donde estos son los pilares del funcionamiento de esta metodología, permitiendo identificar las amenazas a las que está sometido cada activo, así como los riegos a los que dicho activo está asociado en caso de que una amenaza explote una vulnerabilidad, MAGERIT permite determinar el nivel

del riesgo y establecer las medidas de control o salvaguardas que logren la mitigación o reducción de dicho riesgo logrando un nivel de protección adecuado para la organización.

Cabe considerar que la elección de esta metodología viene asociada al uso de la herramienta PILAR en su versión 5.4.2, donde se ha solicitado una licencia de trabajo que permite realizar el análisis de riesgo de forma automatiza y obtenido resultados de alta confiabilidad, cabe considerar que, para fines académicos, se gestionó la licencia de uso, la misma que fue otorgada bajo consideraciones especiales y normas de uso específicas, estableciendo la responsabilidad del uso de la misma ***(ver Figura 8 y Anexo 7)***.

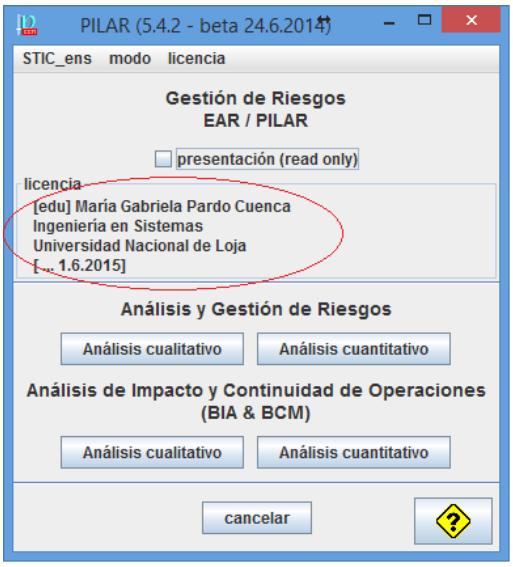


Figura 8: Licencia de uso de la Herramienta Pilar

2.2 Establecer los criterios para la aceptación de riesgos.

Se debe considerar los conceptos básicos sobre lo que se entiende por riesgo, donde se pueda analizarlo desde el punto de vista en que un activo de información se encuentra expuesto a una amenaza que puede causar daños o perjuicios a la organización. Es decir que el riesgo define lo que podría ocurrir con los activos si no son protegidos adecuadamente ***[5,24]***.

Se deben considerar los cuatro tipos o calificaciones de decisiones para el tratamiento de riesgos, determinándose de la siguiente manera:

- **Riesgo Mitigable:** donde el riesgo puede ser reducible con la aplicación de controles de seguridad dedicados, debido a la gravedad del mismo.

- **Riegos Asumible:** donde el riesgo asociado al activo puede ser aceptable por la UTI en el sentido en que no se van a tomar acciones para reducirlo o eliminarlo **[5, 20,38]**.

Partiendo de los tipos de riesgo que se puede obtener al hacer el análisis, se debe considerar lo que nos dice la metodología, donde a partir de los resultados obtenidos en el análisis se debe considerar los niveles hasta donde la UTI puede asumir un riesgo o tratarlo. Para ello es necesario esquematizar como la metodología sugiere que el riesgo sea asumido y en qué nivel lo clasifica.

La metodología permite asignar los niveles o criterios de aceptación del riesgo (ver TABLA VI), fundamentándose en los resultados obtenidos en el análisis en base a las vulnerabilidades y amenazas asociadas a cada activo, y la probabilidad de ocurrencia del fallo al ser explotada una vulnerabilidad a partir de la amenaza, determinando el nivel de impacto o daño que se tendría sobre el activo. Para ello a continuación se presentan las tablas que permitirán determinar el nivel de aceptación del riego en función al impacto y probabilidad de ocurrencia, la misma que será aplicada en la tercera fase del proyecto donde se determinará los riegos a ser tratados o minimizados con la aplicación de los mecanismos de control del Anexo A de la norma ISO/IEC 27001.

Partiendo de lo mencionando, se esquematiza la descripción de la escala del riegos, que servirá como guía para la asignación del nivel del riegos.

TABLA VI. Descripción de Escalas del Riesgo [5,24]

Nivel de Riesgo	Descripción del Riesgo y Acciones Necesarias
DESASTRE - CATÁSTROFE	Se requiere fuertes medidas correctivas, así como planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa del personal responsable de la sección.
MUY CRÍTICO – EXTREMADAMENTE CRÍTICO	Se requiere vigilancia de la alta del responsable de la sección con planes de tratamiento implementados y reportados al director de la UTI
MUY ALTO - CRÍTICO	Se requiere acciones correctivas controladas y coordinadas por el responsable de la sección, se sugeriría planes de tratamiento
MEDIO - ALTO	Es un riego que debe ser administrado bajo procedimientos normales de control.
DESPRESIABLE - BAJO	Es un riegos que no necesariamente debe ser tratado o controlado, en este caso se puede decidir aceptar el riego

Teniendo en cuenta la escala del riesgo se puede establecer qué tipo de tratamiento tendría el riego, el cual se muestra a continuación **(ver Figura 9)**:

NIVEL	CARACTERISTICA	SIGLAS
7.1 - 9	DESASTRE – CATÁSTROFE	D - C
5.1 – 7	MUY CRÍTICO – EXTREMADAMENTE CRÍTICO	MC - EC
3.1 - 5	MUY ALTO - CRÍTICO	MA - C
1.1 – 3	MEDIO - ALTO	M - A
0 – 1	DESPRESIABLE - BAJO	D – B

Figura 9: Criterios de aceptación del Riesgo

Haciendo uso de estos criterios o niveles de riesgo se puede determinar la clasificación que tendrían los riesgos a partir del análisis que se realizará en la fase tres del proyecto, donde de esta forma se le determinará la importancia del activo bajo el riesgo asociado y se establecerán las medias de mitigación o aceptación.

2.3 Identificar las amenazas y vulnerabilidades asociadas a los activos de la UTI.

Las amenazas pueden presentarse en dos diferentes ambientes, que son: ***su origen y la intencionalidad.***

En cuando a su origen pueden existir dos tipos:

- **Externas:** Que son ocasionadas por agentes externos o que no pertenecen a la UTI que pueden ser personas como hackers, personal docente o administrativo, empleados o estudiantes, así como objetos intangibles externos como virus informáticos; pudiendo ser estas deliberadas o accidentales.
- **Internas:** Este tipo de amenazas se originan por personas que pertenecen al personal de la UTI, ya sea personal de planta o personal temporal; pudiendo ser estas deliberadas o accidentales

En cuanto a la intencionalidad pueden ser amenazas de dos tipos:

- **Deliberadas:** que son amenazas donde existe la intención de provocar daño, como: robos, denegación de servicios, ingeniería social, etc.; donde estas pueden ser ocasionadas por agentes interno o externos.

- **Accidentales:** que son amenazas sin intención de provocar daño a la organización, como: desastres naturales, averías de equipos, etc.; donde estas pueden ser ocasionadas por agentes interno o externos.

En cuanto a las vulnerabilidades, es importante tener en cuenta que es toda aquella circunstancia o característica de un activo que puede explotar una amenaza, se debe considerar que una vulnerabilidad por sí sola no puede ocasionar daño, debe existir una amenaza que haga que el daño se produzca **[5,24]**.

A continuación se presenta el análisis de amenazas y vulnerabilidades para los activos de información de la UTI determinados a partir de entrevistas realizadas a los responsables de cada sección de la UTI y en base al análisis de incidentes comunes de seguridad informática, haciendo uso del *Libro 2 de Magerit V3: Catálogo de elementos,* donde se presenta una amplia gama de incidentes comunes de seguridad informática y la forma en que deben ser clasificados, ordenados y descritos (ver TABLAS VII,VIII, VIX, X, XI).

TABLA VII. Especificaciones y codificación de tipos de amenazas, activos de información, criterios de valoración de activos**.**

AMENAZAS		
CÓDIGO	**TIPO**	**DESCRIPCIÓN**
[AAC]	**Amenazas Accidentales**	Sucesos que pueden ocurrir sin intención de ocasionar daño a los activos de información, por agentes internos o externos a la UTI.
[ADL]	**Amenazas Deliberadas**	Sucesos que pueden ocurrir por el mero hecho de causar daño a los activos de información, por agentes internos o externos a la UTI.
ACTIVOS DE INFORMACIÓN		
CÓDIGO	**TIPO**	**DESCRIPCIÓN**
[TEC]	**Tecnología**	Equipos utilizados para gestionar la información y las comunicaciones.
[INT]	**Instalaciones**	Lugares en los que se alojan los sistemas de información
[APL]	**Aplicaciones**	El software que se utiliza para la gestión de la información
[DAT]	**Datos**	Todos aquellos datos que se generan, recogen, gestionan, transmiten y destruyen en la organización
[EAX]	**Equipo Auxiliar**	Todos aquellos activos que dan soporte a los sistemas de información.
CRITERIOS DE VALORACIÓN DE ACTIVOS		
CÓDIGO	**TIPO**	**DESCRIPCIÓN**
[COF]	**Confidencialidad**	Información que debe ser accedida solamente por las personas autorizadas
[INT]	**Integridad**	Información debe estar completa y correcta en todo momento
[DIS]	**Disponibilidad**	La información estará lista para acceder a ella o utilizarse cuando se necesite.

[AAC] AMENAZAS ACCIDENTALES:

TABLA VIII. Amenazas accidentales (Desastres naturales)

[AAC1] DESASTRES NATURALES: Sucesos que pueden ocurrir sin intervención humana		
Amenaza: **- [AAC1.1] Fuego** **- [AAC1.2] Daños por agua** **- [AAC1.3] Desastres naturales**	Tipos de Activos: - [TEC] Tecnología - [INT] Instalaciones - [EAX] Equipos Auxiliares	Criterio de valoración de activo de información que es afectado: - [DIS] Disponibilidad
Descripción: ***Fuego:*** existe la posibilidad de que el fuego acabe con activos de información que son tangibles. ***Daños por agua:*** existe la posibilidad de que el agua acabe con activos de información que son tangibles. ***Desastres Naturales****:* sucesos naturales impredecibles como: tormentas, rayos, terremotos, daños en estructura física de las instalaciones de la universidad por el deterioro, se consideran excluidos de esta clasificación a los sucesos accidentales ocasionados por humanos [10, 11].		

TABLA VIX. Amenazas accidentales (tipo industrial)

[AAC2] ACCIDENTES DE TIPO INDUSTRIAL: Sucesos derivados de la actividad humana que son accidentales		
Amenaza: - [AAC2.1] Fuego - [AAC2.2] Daños por agua - [AAC2.3] Desastres de tipo industrial - [AAC2.4] Contaminación de mecánica. - [AAC2.5] Avería de origen físico o lógico. - [AAC2.6] Condiciones inadecuadas de temperatura o humedad. - [AAC2.7] Interrupción de otros servicios o suministros esenciales.	**Tipos de Activos:** - [TEC] Tecnología - [INT] Instalaciones - [EAX] Equipos Auxiliares - [APL] Aplicaciones	**Criterio de activo de información que es afectado:** - [DIS]Disponibilidad
Descripción: ***Fuego:*** existe la posibilidad de que el fuego acabe con activos de información que son tangibles, donde el origen del mismo no depende de la naturaleza sino del entorno de trabajo. ***Daños por agua:*** existe la posibilidad de que el agua acabe con activos de información que son tangibles, donde el origen del mismo no depende de la naturaleza sino del entorno de trabajo, como fugas de agua de tuberías o descuido del personal con las baterías sanitarias. ***Desastres Industriales:*** Desastres ocasionados por la actividad humana o agentes industriales incontrolables como: explosiones, sobrecarga o fluctuaciones de eléctricas (malas instalaciones eléctricas a nivel de toda la universitaria), corte de suministro eléctrico, interferencias de radio, campos magnéticos, etc.; donde estos desastres repercuten en daños físicos a los activos de información. ***Contaminación Mecánica:*** Sucesos que repercuten en daños físicos a los activos como son: polvo, suciedad, vibraciones, intrusos animales que dañan a los equipos. ***Avería de origen físico o lógico:*** Fallos inherentes de los equipos, por deterioro o falta de mantenimiento, así como fallos en las aplicaciones, por lo tanto ocasionan daños en activos de tipo: *tecnología, aplicaciones, equipos auxiliares.* ***Condiciones inadecuadas de temperatura o humedad:*** deficiencias en la aclimatación del DATA CENTER así como en laboratorios, bibliotecas, oficinas, etc., donde estos exceden los márgenes de trabajo de los equipos que ocasionaría daños físicos. *Interrupción de otros servicios o suministros esenciales:* otros servicios o recursos de los que depende la operación de los equipos como suministros para equipos (suministros de impresoras, lámparas para proyectores, repuestos para diferentes equipos) o herramientas para mantenimiento [10, 11].		

[AAC3] ERRORES Y FALLOS NO INTENCIONADOS

TABLA X. Amenazas accidentales (errores o fallos no intencionados)

[AAC3] ERRORES Y FALLOS NO INTENCIONADOS: Sucesos o fallos ocasionados por personas no intencionados		
Amenaza: - [AAC3.1] Errores de usuario - [AAC3.2] Errores de administrador. - [AAC3.3] Errores de configuración. - [AAC3.4] Difusión de software dañino. - [AAC3.5] Escapes de información. - [AAC3.6] Alteración o destrucción accidental de la información. - [AAC3.7] Errores de mantenimiento o actualización de software. - [AAC3.8] Errores de mantenimiento o actualización de hardware. - [AAC3.9] Caída del sistema por falta de algún recurso. - [AAC3.10] Pérdida o robo de equipos.	**Tipos de Activos:** - [TEC] Tecnología - [INT] Instalaciones - [EAX] Equipos Auxiliares - [DAT] Datos. - [APL] Aplicaciones	**Criterio de valoración de activo de información que es afectado:** - [DIS] Disponibilidad - [INT] Integridad. - [CON] Confidencialidad
Descripción: ***Errores de usuario:*** Sucesos ocasionados por equivocación de los usuarios al ingresar a los servicios, datos, etc., donde el usuario puede modificar su información personal o cambiar sus claves y luego perderla, ingresar a directorios indebidos y ocasionar algún daño, etc. ***Errores de administrador:*** Sucesos ocasionados por equivocaciones del personal de la UTI encargado de instalaciones u operaciones, donde el administrado pudiese dar privilegios a usuarios inadecuados, modificar información de base de datos, cambiar funciones del sistema, etc. ***Errores de configuración:*** Sucesos ocasionados por introducción de datos de configuración errónea, el análisis de esta amenaza es de gran importancia ya que todos los activos dependen de su configuración. ***Difusión de software dañino:*** Sucesos ocasionados por usuarios o administradores de propagación de virus no intencionados. ***Escapes de información:*** Sucesos ocasionados al momento de divulgar información, donde esta llega accidentalmente a otros destinatarios que no deberían tener conocimiento de ella. ***Alteración o destrucción accidental de la información:*** Sucesos ocasionados por los usuarios que por mala gestión ocasionan daño a la información que ellos manejan, por lo general esto se presenta en usuarios finales de los sistemas de información, así como los equipos informáticos que se han incluido en [EAX] equipos auxiliares que son responsabilidad de la sección de Mantenimiento Electrónico. ***Errores de mantenimiento o actualización de software:*** Sucesos que se pueden ocasionar por defectos en los procesos o controles de actualizaciones del código fuente. ***Errores de mantenimiento o actualización de hardware:*** Sucesos que se pueden ocasionar por procedimientos o controles de actualización de los equipos que pueden alterar su funcionamiento del equipo antes de su tiempo normal de uso [10,11].		

[ADL] AMENAZAS DELIBERADAS

TABLA XI. Amenazas deliberadas

[ADL] AMENAZAS DELIBERADAS		
Amenaza: - [ADL1] Manipulación de la configuración - [ADL2] Suplantación de la identidad del usuario. - [ADL3] Abuso de privilegios. - [ADL4] Difusión de software dañino. - [ADL5] Acceso no autorizado. - [ADL6] Interceptación de información. - [ADL7] Modificación o destrucción deliberada de la información.	**Tipos de Activos:** - [TEC] Tecnología - [INT] Instalaciones - [EAX] Equipos Auxiliares - [DAT] Datos - [APL] Aplicaciones	**Criterio de valoración de activo de información que es afectado**: - [DIS] Disponibilidad - [CON] Confidencialidad - [INT] Integridad

- [ADL8] Divulgación de información. - [ADL9] Manipulación de programas. - [ADL10] Manipulación de los equipos. - [ADL11] Ingeniería social		
Descripción: ***Manipulación de la configuración:*** Se debe considerar esta amenaza ya que todos los activos dependen de su configuración para que funcionen adecuadamente, por lo tanto la mala configuración de los mismos puede ser deliberada por parte de los usuarios administradores. ***Suplantación de la identidad del usuario:*** Sucesos que se ocasiona cuando existe alguna intromisión por usuarios externos que utilizan la identidad de usuarios autorizados y pueden ocasionar diferentes problemas en los sistemas de información. ***Abuso de privilegios:*** Se debe considerar que cada usuario disfruta de su nivel de privilegios para un propósito determinado, existen inconvenientes cuando los usuarios abusan sus privilegios lo que acontece a problemas posteriores. ***Difusión de software dañino:*** Se refiere a la difusión intencionada de virus o software malicioso en los equipos en la red de datos administrada por las diferentes secciones de la UTI, así como en los equipos de la universidad asignados al personal. ***Acceso no autorizado:*** Sucesos que se ocasionan por atacantes que logran acceder a los recursos del sistema sin tener autorización para ello. ***Interceptación de información:*** Sucesos que se ocasionan cuando un atacante llega a tener acceso a información que no le corresponde. *Modificación o destrucción deliberada de la información:* Sucesos que se ocasionan por usuarios que alteran o destruyen información que pertenece a la Universidad y que esta almacenada en los equipos bajo responsabilidad del personal de la UTI o por los custodios designados. ***Divulgación de información:*** Sucesos que pueden ser ocasionados por personal de la Universidad al entregar información de forma deliberada con fines ajenos a los intereses de la Universidad. ***Manipulación de programas:*** Alteración intencionada del funcionamiento de las aplicaciones. ***Manipulación de los equipos:*** Alteración intencionada del funcionamiento de los equipos. ***Ingeniería social:*** Abuso de la voluntad de las personas para obtener información, realizando actividades que interesan a terceros [10, 11].		

A continuación se presentan las tablas que se han realizado a partir de la clasificación de las amenazas, de acuerdo a los activos para cada sección de la UTI ***(ver TABLA XII, XIII, XIV y anexo 6)***, poniendo atención a las vulnerabilidades asociadas que estos tendrían a partir de los criterios de valoración establecidos (disponibilidad, integridad y confidencialidad).

TABLA XII: Amenazas y vulnerabilidades asociadas a los activos de la Sección de Redes y Equipos Informáticos – Sección de Telecomunicaciones.

SECCIÓN DE REDES Y EQUIPOS INFORMÁTICOS - SECCIÓN DE TELECOMUNICACIONES

INFORMACIÓN DE ACTIVOS				*AMENAZAS Y VULNERABILIDADES*		*CRITERIO AFECTADO*		
CÓDIGO	***TIPO***	***CARACTERISTICA***	***DESCRIPCIÓN***	***TIPO DE AMENAZA***	***VULNERABILIDAD***	***[CON]***	***[INT]***	***[DIS]***
TEC001	TECNOLOGIA	CISCO	ROUTER	**INFORMACIÓN CONFINDENCIAL**				
TEC002	TECNOLOGIA	DISTRIBUCIÓN DE SERVIDORES	SWITCH	**INFORMACIÓN CONFINDENCIAL**				
TEC003	TECNOLOGIA	Web-Mail	SERVIDOR WEB: servicios UTI	**INFORMACIÓN CONFINDENCIAL**				
TEC004	TECNOLOGIA	WEB						
TEC005	TECNOLOGIA	SGA (Servicios)						
TEC006	TECNOLOGIA	Med Cursos	SERVIDOR: servicio UTI	**INFORMACIÓN CONFINDENCIAL**				
TEC007	TECNOLOGIA	AEIRNNR						
TEC008	TECNOLOGIA	MED Virtual						
TEC009	TECNOLOGIA	EVA						
TEC010	TECNOLOGIA	Financiero						
TEC011	TECNOLOGIA	Cursos						
TEC012	TECNOLOGIA	Blade	FIREWALL					
TEC013	TECNOLOGIA	SGAGW2						
TEC014	TECNOLOGIA	Proxi Wireless						
TEC015	TECNOLOGIA	SGAGW						
TEC016	TECNOLOGIA	DNS-DHCP	SERVIDOR DE ACCESO A LA RED	**INFORMACIÓN CONFINDENCIAL**				
TEC017	TECNOLOGIA	NOC						

TEC018	TECNOLOGIA	OS-Ticket		**INFORMACIÓN CONFINDENCIAL**
TEC019	TECNOLOGIA	Nagios		
TEC020	TECNOLOGIA	Nessus		
TEC021	TECNOLOGIA	Radius		
TEC022	TECNOLOGIA	ASA	FIREWALL: Seguridad	**INFORMACIÓN CONFINDENCIAL**
TEC023	TECNOLOGIA	Blue Coat PacketShaper	Blue Coat PacketShaper	**INFORMACIÓN CONFINDENCIAL**
TEC024	TECNOLOGIA	CONTROLADORA WLC	Controladora de conexión y tráfico de red	**INFORMACIÓN CONFINDENCIAL**
TEC025	TECNOLOGIA	UBIQUITI	RADIOS	**INFORMACIÓN CONFINDENCIAL**
TEC026	TECNOLOGIA	Motorola		
TEC027	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Administración Central	**INFORMACIÓN CONFINDENCIAL**
TEC028	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Área de la Salud	
TEC029	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: San Cayetano	
TEC030	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Motupe	
TEC031	TECNOLOGIA	SWITCHES (diferentes marcas y características)	**INFORMACIÓN CONFINDENCIAL**	**INFORMACIÓN CONFINDENCIAL**

TEC032	TECNOLOGIA	ACCESS POINT	**INFORMACIÓN CONFINDENCIAL**	**INFORMACIÓN CONFINDENCIAL**
TEC033	TECNOLOGIA	ROUTER	ROUTER: Microtick	**INFORMACIÓN CONFINDENCIAL**
TEC034	TECNOLOGIA	RELOJ BIOMÉTRICO	RELOJ BIOMÉTRICO	**INFORMACIÓN CONFINDENCIAL**
TEC035	TECNOLOGIA	SERVIDOR PROXI	SERVIDOR PROXI: Proxy Energía, Proxy MED, Proxy Agropecuaria, Proxy Jurídica, Proxi Educación	**INFORMACIÓN CONFINDENCIAL**
TEC036	TECNOLOGIA	CENTRALILLAS TELEFÓNICAS	Centralillas telefónicas para comunicación entre departamentos	**INFORMACIÓN CONFINDENCIAL**
INT001	INSTALACIONES	DATA CENTER	Centro de Datos donde se encuentran los servidores y equipos de conexión de red para servicios.	**INFORMACIÓN CONFINDENCIAL**
INT002	INSTALACIONES	TENDIDO DE LA RED DE DATOS ALÁMBRICA	Conexiones de la Red de datos por medio de dispositivos físicos	**INFORMACIÓN CONFINDENCIAL**
INT003	INSTALACIONES	RED DE CONEXIÓN INALAMBRICA	Redes de comunicación inalámbrica de la Universidad	**INFORMACIÓN CONFINDENCIAL**
INT004	INSTALACIONES	ENLACES DE CONEXIÓN	Enlaces inalámbricos de conexión	**INFORMACIÓN CONFINDENCIAL**

Nota: La información omitida en las tablas es CONFINDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

TABLA XIII. Amenazas y vulnerabilidades asociadas a los activos de la Sección de Desarrollo de Software.
SECCIÓN DE DESARROLLO DE SOFTWARE

INFORMACIÓN DE ACTIVOS				*AMENAZAS Y VULNERABILIDADES*		*CRITERIO DE VALORACIÓN AFECTADO*		
CÓDIGO	*TIPO*	*CARACTERISTICA*	*DESCRIPCIÓN*	*TIPO DE AMENAZA*	*VULNERABILIDAD*	*[CON]*	*[INT]*	*[DIS]*
APL001	APLICACIÓN	Sistema de Gestión Académica	**INFORMACIÓN CONFINDENCIAL**	**INFORMACIÓN CONFINDENCIAL**				
APL002	APLICACIÓN	Consulta de Estadísticas del SGA	Cliente de Servicios WEB,	**INFORMACIÓN CONFINDENCIAL**				
APL003	APLICACIÓN	Sistema de Gestión de Aprendizaje Moodle (modalidad presencial y a distancia)	Sistema de Información.	**INFORMACIÓN CONFINDENCIAL**				
APL004	APLICACIÓN	Sistema de Evaluación de Docentes	Sistema de Información	**INFORMACIÓN CONFINDENCIAL**				
APL005	APLICACIÓN	Sistema de Gestión Documental Quipux	Sistema de información	**INFORMACIÓN CONFINDENCIAL**				
APL006	APLICACIÓN	Limesurvey	Sistema de información	**INFORMACIÓN CONFINDENCIAL**				
APL007	APLICACIÓN	Sistema de Gestión Bibliotecaria	Sistema de Información	**INFORMACIÓN CONFINDENCIAL**				
APL008	APLICACIÓN	OSTicket	Sistema de Información	**INFORMACIÓN CONFINDENCIAL**				

APL009	APLICACIÓN	Gestión Académica de Carrera	Sistema de Información	**INFORMACIÓN CONFINDENCIAL**
APL010	APLICACIÓN	Forestweb	Sistema de registro y análisis de información referente a la madera	**INFORMACIÓN CONFINDENCIAL**
APL011	APLICACIÓN	Sistema de Seguimiento de Egresados y Graduados	Sistema de Información	**INFORMACIÓN CONFINDENCIAL**
APL012	APLICACIÓN	Sistema de emisión y reposición de títulos	Sistema de Información, plataforma	**INFORMACIÓN CONFINDENCIAL**
APL013	APLICACIÓN	Página web de la Universidad	Portal de información	**INFORMACIÓN CONFINDENCIAL**
DAT001	DATOS	Sistema de Gestión Académica	Utiliza base de datos Postgres	**INFORMACIÓN CONFINDENCIAL**
DAT002	DATOS	Consulta de Estadísticas del SGA		**INFORMACIÓN CONFINDENCIAL**
DAT003	DATOS	Sistema de Gestión de Aprendizaje Moodle (modalidad presencial y a distancia)	Utiliza base de datos MySQL	**INFORMACIÓN CONFINDENCIAL**
DAT004	DATOS	Sistema de Evaluación de Docentes	Utiliza base de datos Postgres	**INFORMACIÓN CONFINDENCIAL**
DAT005	DATOS	Sistema de Gestión Documental Quipux	Utiliza base de datos Postgres	**INFORMACIÓN CONFINDENCIAL**

DAT006	DATOS	Limesurvey	Utiliza base de datos MySQL	**INFORMACIÓN CONFINDENCIAL**
DAT007	DATOS	Sistema de Gestión Bibliotecaria	Utiliza base de datos MySQL	**INFORMACIÓN CONFINDENCIAL**
DAT008	DATOS	OSTicket	Utiliza base de datos MySQL 5.0	**INFORMACIÓN CONFINDENCIAL**
DAT009	DATOS	Gestión Académica de Carrera	Utiliza base de datos ACCESS	**INFORMACIÓN CONFINDENCIAL**
DAT010	DATOS	Forestweb	Utiliza base de datos MongoDB	**INFORMACIÓN CONFINDENCIAL**
DAT011	DATOS	Sistema de Seguimiento de Egresados y Graduados	Utiliza base de datos MySQL	**INFORMACIÓN CONFINDENCIAL**
DAT012	DATOS	Sistema de emisión y reposición de títulos	Utiliza base de datos Visual Fox Pro	**INFORMACIÓN CONFINDENCIAL**
DAT013	DATOS	Página web de la Universidad	Utiliza base de datos MySQL 5.0	**INFORMACIÓN CONFINDENCIAL**

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

TABLA XIV. Amenazas y vulnerabilidades asociadas a los activos de la Sección de Mantenimiento Electrónico

SECCIÓN DE MANTENIMIENTO ELECTRÓNICO

INFORMACIÓN DE ACTIVOS				*AMENAZAS Y VULNERABILIDADES*		*CRITERIO DE VALORACIÓN AFECTADO*		
CÓDIGO	*TIPO*	*CARACTERISTICA*	*DESCRIPCIÓN*	*TIPO DE AMENAZA*	*VULNERABILIDAD*	*[CON]*	*[INT]*	*[DIS]*
EAX001	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS	Equipos de impresión, copiadoras, escáneres, plotters, etc. De uso del personal administrativo	**INFORMACIÓN CONFIDENCIAL**				
EAX002	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS	Equipos de impresión, copiadoras, escáneres, plotters, etc. Del uso del personal docente	**INFORMACIÓN CONFIDENCIAL**				
EAX003	EQUIPOS AUXILIARES	PROYECCIÓN AUDIO-VISUAL	Equipos de proyección, pantallas de proyección, lámparas, etc. Del uso del personal docente	**INFORMACIÓN CONFIDENCIAL**				
EAX004	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de oficinas o departamentos. Del uso del personal administrativo	**INFORMACIÓN CONFIDENCIAL**				

EAX005	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de centros de cómputo o bibliotecas	**INFORMACIÓN CONFIDENCIAL**
EAX006	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de oficinas o departamentos. Del uso del personal docente	**INFORMACIÓN CONFIDENCIAL**
EAX007	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES	Equipos portátiles con responsabilidad del personal administrativo	**INFORMACIÓN CONFIDENCIAL**
EAX008	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES	Equipos portátiles con responsabilidad del personal docente	**INFORMACIÓN CONFIDENCIAL**
EAX009	EQUIPOS AUXILIARES	EQUIPOS Y/O HERRAMIENTAS PARA MANTENIMIENTO	Equipos y/o herramientas para mantenimiento necesarias	**INFORMACIÓN CONFIDENCIAL**

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomuniciones e Información de la Universidad Nacional de Loja

2.4 Identificar la importancia de los activos de información de la UTI, en base a las amenazas y vulnerabilidades.

A partir del análisis de amenazas asociadas a los activos de información que maneja la UTI en cada una de sus secciones, así como el análisis de las vulnerabilidades asociadas a las mismas, y partiendo de los conceptos básicos, se puede decir que para cada activo existen amenazas de todo tipo que pueden ser explotadas por sus vulnerabilidades, por lo tanto existiría un riesgo intrínseco, donde su impacto estaría asociado a la valoración para cada activo ***(ver anexo 6)***, de acuerdo a los criterios de valoración establecidos (confidencialidad, integridad y disponibilidad) ***[5]***.

Para la valoración de los activos bajo estos criterios se ha hecho uso de las siguientes tablas de valoración (ver Tablas XV, XVI y XVII):

DISPONIBILIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Cuál sería la importancia o trastorno que tendría que el activo no estuviera disponible?

TABLA XV. Escala de Valoración para la disponibilidad del activo de información [5,24].

VALOR	CRITERIO
1	No es relevante / importancia de disponibilidad del 0% - 9%
2	Debe estar disponible al menos el 10% - 49% del tiempo
3	Debe estar disponible al menos el 50% - 90% del tiempo
4	Debe estar disponible 90% o más del tiempo.

INTEGRIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Qué importancia tendría que el activo fuera alterado sin autorización ni control?

TABLA XVI. Escala de Valoración para la integridad del activo de información [5,24].

VALOR	CRITERIO
1	No es relevante / importancia de modificación menor al 9%
2	No es relevante los errores que se presenten o la información que falte
3	Tiene que estar correcta y completa al menos en un 50%
4	Tiene que estar correcta y completa al menos en un 95% o más

CONFIDENCIALIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Cuál es la importancia que tendría que el activo se accediera de manera no autorizada?

TABLA XVII. Escala de Valoración para la confidencialidad del activo de información [5,24].

VALOR	CRITERIO
1	No es relevante / importancia de acceso menor al 9%
2	Daños muy bajos, el incidente no trascendería del área afectada
3	Los daños serían relevantes, el incidente implicaría a otras áreas
4	Los daños serían catastróficos, la reputación y la imagen de la UTI se verían comprometidos.

Basándonos en los criterios de valoración con su respectiva escala, con ayuda de las personas encargadas de cada una de las secciones de la UTI, se realizado la valoración de los activos (ver TABLA XVIII y XIX), para determinar el impacto de los riegos asociados en cada uno de los activos, donde el impacto está asociado al valor de los activos, mediante la **sumatoria de la valoración dada a los mismos en sus tres criterios, en un rango de 0 a 12 puntos**, donde se puede ver la importancia de cada activo para la organización, a continuación se presentan las tablas de valoración realizadas.

Tabla XVIII. Valoración de activos de la UTI

INFORMACIÓN DE ACTIVOS					VALORACIÓN DE ACTIVOS				OBSERVACIÓN
CÓDIGO	*TIPO*	*CARACTERISTICA*	*DESCRIPCIÓN*	*LOCALIZACIÓN*	[DIS]	[INT]	[CON]	TOTAL	
TEC001	TECNOLOGIA	CISCO 7460	ROUTER	EDIFICIO DE ADMINISTRACIÓN CENTRAL - UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN	**INFORMACIÓN CONFIDENCIAL**				
TEC002	TECNOLOGIA	DISTRIBUCIÓN DE SERVIDORES	SWITCH						
TEC003	TECNOLOGIA	Web-Mail	SERVIDOR WEB: servicios UTI						NO ESTA ACTIVO
TEC004	TECNOLOGIA	WEB							
TEC005	TECNOLOGIA	SGA (Servicios)							
TEC006	TECNOLOGIA	Med Cursos	SERVIDOR: servicio UTI						
TEC007	TECNOLOGIA	AEIRNNR							
TEC008	TECNOLOGIA	MED Virtual							
TEC009	TECNOLOGIA	EVA							
TEC010	TECNOLOGIA	Financiero							
TEC011	TECNOLOGIA	Cursos							
TEC012	TECNOLOGIA	Blade	FIREWALL: servidores virtualizados, enlace, protección y seguridad						
TEC013	TECNOLOGIA	SGAGW2							
TEC014	TECNOLOGIA	Proxy Wirelles							NO EXISTE
TEC015	TECNOLOGIA	SGAGW							
TEC016	TECNOLOGIA	DNS-DHCP	SERVIDOR DE ACCESO A LA RED						
TEC017	TECNOLOGIA	NOC							Funciona únicamente como servidor
TEC018	TECNOLOGIA	OS-Ticket							Standby
TEC019	TECNOLOGIA	Nagios							
TEC020	TECNOLOGIA	Nessus							Standby
TEC021	TECNOLOGIA	Radius							
TEC022	TECNOLOGIA	ASA	FIREWALL: Seguridad						
TEC023	TECNOLOGIA	Blue Coat PacketShaper	Blue Coat PacketShaper						
TEC024	TECNOLOGIA	CONTROLADORA WLC	Controladora de conexión y tráfico de red						
TEC025	TECNOLOGIA	UBIQUITI	RADIOS						

TEC026	TECNOLOGIA	Motorola			**INFORMACIÓN CONFIDENCIAL**	
TEC027	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Administración Central			Al momento no se encuentra operando
TEC028	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Área de la Salud	Área de la Salud		Al momento no se encuentra operando
TEC029	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: San Cayetano	San Cayetano		Al momento no se encuentra operando
TEC030	TECNOLOGIA	CMM MICRO	TORRES DE COMUNICACIÓN: Motupe	Extensión MOTUPE		Al momento no se encuentra operando
TEC031	TECNOLOGIA	SWITCHES (diferentes marcas y características)	**INFORMACIÓN CONFIDENCIAL**	Diferentes áreas y departamentos de la Universidad.		
TEC032	TECNOLOGIA	ACCESS POINT	**INFORMACIÓN CONFIDENCIAL**	Diferentes áreas y departamentos de la Universidad.		
TEC033	TECNOLOGIA	ROUTER	ROUTER: Microtick	Bloque de nivelación y bloque de estadio		
TEC034	TECNOLOGIA	RELOJ BIOMÉTRICO	RELOJ BIOMÉTRICO	Diferentes áreas y departamentos de la Universidad.		
TEC035	TECNOLOGIA	SERVIDOR PROXI	SERVIDOR PROXI: Proxi Energía, Proxy MED, Proxy Agropecuaria, Proxy Jurídica, Proxi Educación	Diferentes áreas y departamentos de la Universidad.		Utilizado para monitoreo
TEC036	TECNOLOGIA	CENTRALILLAS TELEFÓNICAS	Centralillas telefónicas para comunicación entre departamentos	Ubicadas en cada una de las Áreas de la Universidad		
INT001	INSTALACIONES	CENTRO DE CARGA	Centro de Datos donde se encuentran los servidores y equipos de conexión de red para servicios.	Instalaciones de la Unidad de Telecomunicaciones e Información.		
INT002	INSTALACIONES	TENDIDO DE LA RED DE DATOS ALÁMBRICA	Conexiones de la Red de datos por medio de dispositivos físicos	Diferentes áreas y departamentos de la Universidad.		
INT003	INSTALACIONES	RED DE CONEXIÓN INALAMBRICA	Redes de comunicación inalámbrica de la Universidad	Campus Universitario		

INT004	INSTALACIONES	ENLACES DE CONEXIÓN	Enlaces inalámbricos de conexión	Campus Universitario	**INFORMACIÓN CONFIDENCIAL**	
APL001	APLICACIÓN	Sistema de Gestión Académica	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL002	APLICACIÓN	Consulta de Estadísticas del SGA	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL003	APLICACIÓN	Sistema de Gestión de Aprendizaje Moodle (modalidad presencial y a distancia)	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL004	APLICACIÓN	Sistema de Evaluacion de Docentes	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL005	APLICACIÓN	Sistema de Gestión Documental Quipux	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL006	APLICACIÓN	Limesurvey	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL007	APLICACIÓN	Sistema de Gestión Bibliotecaria	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL008	APLICACIÓN	OSTicket	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL009	APLICACIÓN	Gestión Académica de Carrera	**INFORMACIÓN CONFIDENCIAL**	Algunas carreras		
APL010	APLICACIÓN	Forestweb	**INFORMACIÓN CONFIDENCIAL**	Laboratorio de Análisis de Madera, Carrera de Ingeniería Forestal		Fue un proyecto realizado para la carrera, no se registra información para la UTI
APL011	APLICACIÓN	Sistema de Seguimiento de Egresados y Graduados	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de Telecomunicaciones e Información.		
APL012	APLICACIÓN	Sistema de emisión y reposición de titulos	**INFORMACIÓN CONFIDENCIAL**	Secretaria General de la Universidad		
APL013	APLICACIÓN	Página web de la Universidad	**INFORMACIÓN CONFIDENCIAL**	Instalaciones de la Unidad de		

				Telecomunicaciones e Información.		
DAT001	DATOS	Sistema de Gestión Académica	Utiliza base de datos Postgres	Instalaciones de la UTI.	**INFORMACIÓN CONFIDENCIAL**	
DAT002	DATOS	Consulta de Estadísticas del SGA		Instalaciones de la UTI		Dentro de la aplicación de consulta que funciona con la base de datos del Sistema de Gestión Académica
DAT003	DATOS	Sistema de Gestión de Aprendizaje Moodle	Utiliza base de datos MySQL	Instalaciones de la UTI.		
DAT004	DATOS	Sistema de Evaluacion de Docentes	Utiliza base de datos Postgres	Instalaciones de la UTI.		
DAT005	DATOS	Sistema de Gestión Documental Quipux	Utiliza base de datos Postgres	Instalaciones de la UTI.		
DAT006	DATOS	Limesurvey	Utiliza base de datos MySQL	Instalaciones de la UTI		
DAT007	DATOS	Sistema de Gestión Bibliotecaria	Utiliza base de datos MySQL	Instalaciones de la UTI		
DAT008	DATOS	OSTicket	Utiliza base de datos MySQL	Instalaciones de la UTI.		
DAT009	DATOS	Gestión Académica de Carrera	Utiliza base de datos ACCESS	Algunas carreras		
DAT010	DATOS	Forestweb	Utiliza base de datos MongoDB	Laboratorio de Análisis de Madera, Carrera de Ingeniería Forestal		
DAT011	DATOS	Sistema de Seguimiento de Egresados y Graduados	Utiliza base de datos MySQL	Instalaciones de la Unidad de Telecomunicaciones e Información.		
DAT012	DATOS	Sistema de emisión y reposición de titulos	Utiliza base de datos Visual	Secretaria General de la Universidad		
DAT013	DATOS	Página web de la Universidad	Utiliza base de datos MySQL	Instalaciones de la UTI.		
EAX001	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS	Equipos de impresión, copiadoras, escaners, ploters, etc.	Oficinas o departamentos del personal administrativo		
EAX002	EQUIPOS AUXILIARES	REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS	Equipos de impresión, copiadoras, escaners, ploters, etc.	Oficinas o departamentes del personal docente		

EAX003	EQUIPOS AUXILIARES	PROYECCIÓN AUDIO-VISUAL	Equipos de proyección, pantallas de proyección, lamparas, etc.	Oficinas o departamentos del personal docente	**INFORMACIÓN CONFIDENCIAL**	
EAX004	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de oficinas o departamentos.	Oficinas o departamentos del personal administrativo		
EAX005	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de centros de cómputo o bibliotecas	Centros de cómputo o bibliotecas de las diferentes áreas de la Universidad		
EAX006	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN DE ESCRITORIO	Equipos de escritorio de oficinas o departamentos.	Oficinas o departamentos del personal docente		
EAX007	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES	Equipos portátiles con responsabilidad del personal administrativo	Oficinas o departamentos del personal administrativo		
EAX008	EQUIPOS AUXILIARES	EQUIPOS DE COMPUTACIÓN PORTATILES	Equipos portátiles con responsabilidad del personal docente	Oficinas o departamentos del personal docente		
EAX009	EQUIPOS AUXILIARES	EQUIPOS Y/O HERRAMIENTAS PARA MANTENIMIENTO	Equipos y/o herramientas para mantenimiento necesarias	Sección de mantenimiento de Informático		

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

TABLA XIX. Tabla resumen de la valoración de activos de información.

valor Numérico	Nivel de Importancia	Activos valorados
0	Sin valor apreciable	**INFORMACIÓN CONFIDENCIAL**
3- 4	Nivel Bajo	
5 – 7	Nivel Medio	
8 – 10	Nivel Alto	
11 - 12	Nivel Muy Alto	

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

Con la tabla resumen (ver TABLA XIX) desarrollada en base a los resultados de la valoración de los activos bajo los criterios tomados para el estudio, se permite apreciar el valor de impacto o la importancia que los mismo tienen para la UTI en sus diferentes secciones.

Considerando que gran cantidad de activos están en el nivel más alto de la valoración establecida para el estudio se puede decir, que los daños que estos puedan sufrir ocasionarían grandes pérdidas a la UTI como seria, la paralización de sus actividades, suspensión de servicios para la universidad, pérdidas materiales, etc.

Partiendo de estas consideraciones se da el primer paso para el análisis de riegos, donde el valor de los activos para la organización cumplen uno de los roles más importantes en la estimación de los mecanismos de control para la mitigación de riegos.

Fase 3: Determinar los mecanismos de control necesario para el tratamiento de los riesgos identificados.

3.1 Evaluar el impacto de ocurrir un fallo en la seguridad en relación a las amenazas y vulnerabilidades.

Para la resolución de esta sección, se ha considerado los resultados previos obtenidos como son la valoración de activos bajo las tres dimensiones establecidas (disponibilidad, integridad y confidencialidad), así como la determinación de las amenazas a las que están expuestos o que puede afectar a cada activo en las diferentes dimensiones del mismo; cabe considerar que para la correcta evaluación de la probabilidad de ocurrencia de un fallo y el impacto del mismo sobre el activo se necesitan datos referentes a, en que momento pueda ocurrir un fallo y el daño que demanda la materialización de una amenaza.

Partiendo de lo mencionado el primer paso es la valoración de las amenazas asociadas a los activos, para lo cual se ha considerado en gran medida las entrevistas previas realizadas a los responsables de cada sección de la Unidad de Telecomunicaciones e Información **(ver Anexo 8)**, así como se ha considerado las pautas y la clasificación de amenazas dadas en el Catalogo de Elementos que nos da ***Magerit v3***, donde permite orientar de forma ordenada las diferentes amenazas a las que están sometidos los activos de información de forma global y clara. Para la valoración es importante considerar que cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones necesariamente, ni se degradan en la misma medida, por lo tanto se valora el daño de un activo en base a su degradación (cuán perjudicado resulta el activo) y probabilidad (cuán probable o improbable es que la amenaza se materialice) [**5,24**].

Al realizar el cálculo de estos valores, se debe considerar que la herramienta PILAR v5.4.2 ha sido utilizada para efectos de analices y obtención de resultados más eficientes, permite generar estos valores de forma automática considerando la clasificación del activo y sus características, pero en este caso se ha optado por el análisis de incidentes de seguridad ocurridos en la UTI en las diferentes secciones, donde se debe destacar que debido a la falta de documentos históricos se optó realizarlo mediante entrevista directa a los responsables de las secciones y personas encargadas de los diferentes activos de información que mediante su experiencia y consideraciones técnicas han permitido determinar la probabilidad de materialización de amenazas así

como la degradación que estos activos pudieran sufrir en caso de que sucediera algún tipo de fallo de seguridad.

Para esta valoración se consideraron las siguientes tablas (**ver Tabla XX y Tabla XXI):**

Probabilidad: Donde esta se ha medido para cada amenaza asociada a cada activo y de forma independiente:

TABLA XX. Probabilidad de materialización de una amenaza para un activo de información [5,28,29]

CALIF.	VALOR	SIGNIFICADO	TIEMPO ESTIMADO
5	MR	Muy Raro	Siglos
4	PP	Poco Probable	Cada varios años
3	P	Posible	Una vez al año
2	MP	Muy Posible	Mensualmente
1	S	Casi seguro	A diario

Degradación: Donde esta se ha medido para cada dimensión considerando cada amenaza y activo a la que está asociada, considerando que una amenaza no afecta necesariamente a todas las dimensiones al mismo tiempo.

TABLA XXI. Valores para la degradación de un activo frente a la materialización de una amenaza [5,24,39].

CALIF.	VALOR	SIGNIFICADO	TIEMPO ESTIMADO
5	T	Total	80% - 100%
4	MA	Muy Alta	61% - 80%
3	A	Alta	41% - 60%
2	M	Media	21% - 40%
1	B	Bajo	0% - 20%

Con los datos obtenidos de la valoración de amenazas partiendo de la degradación que los activos sufrirían al ocurrir un fallo de seguridad, así como el valor del activo y las amenazas a las que está sometido se puede determinar el impacto este pude sufrir, es decir la medida del daño sobre el activo derivado de la materialización de una amenaza.

Se considera en primera instancia el Impacto acumulado (ver **Tabla XXII**), el mismo que permite determinar las salvaguardas que se deben considerar para disminuir la degradación de los equipos en caso de materializarse una amenaza, en la siguiente tabla de muestra el impacto acumulado de los activos de información **[5,24].**

Para una mejor comprensión de la tabla se adjunta la tabla de valoración del impacto que utiliza PILAR 5.4.2 **(ver Figura 11):**

Figura11: Leyenda de valoración (Impacto) de la Herramienta PILAR 5.4.2

TABLA XXII. Valoración de Impacto acumulado para cada activo de Información.

Activo	**[D]**	**[I]**	**[C]**
[APL] Aplicaciones	**INFORMACIÓN CONFIDENCIAL**		
[APL.APL001] SISTEMA DE GESTION ACADEMICA			
[APL.APL002] Consulta de Estadísticas del SGA			
[APL.APL003] SISTEMA DE GESTION DE APRENDIZAJE MOODLE			
[APL.APL004] SISTEMA DE EVALUACION DE DOCENTES			
[APL.APL005] SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX			
[APL.APL006] LIMESURVEY			
[APL.APL007] SISTEMA DE GESTION BIBLIOTECARIA			
[APL.APL008] PAGINA WEB DE LA UNIVERSIDAD			
[APL.APL009] SISTEMA DE EMISIÓN Y REPOSICIÓN DE TITULOS			
[APL.APLO10] FORESTWEB			
[APL.APL011] SISTEMA DE SEGUIMIENTO DE EGRESADOS Y GRADUADOS			
[TEC] TECNOLOGIA			
[TEC.TEC001] CISCO			
[TEC.TEC002] Switch Servidores			
[TEC.TEC003] SERVIDOR BLADE			
[TEC.TEC004] SERVIDOR WEB			
[TEC.TEC005] SERVIDOR SGA			
[TEC.TEC006] SERVIDOR MED CURSOS			
[TEC.TEC007] SERVIDOR AEIRNNR			
[TEC.TEC008] SERVIDOR MED VIRTUAL			
[TEC.TEC009] SERVIDOR EVA			

[TEC.TEC010] SERVIDOR FINANCIERO	**INFORMACIÓN CONFIDENCIAL**
[TEC.TEC011] SERVIDOR CURSOS	
[TEC.TEC012] BALANCEADOR DE APLICACIONES	
[TEC.TEC013] FIREWALL SGGW	
[TEC.TEC013] PROXI WIRELESS	
[TEC.TEC014] PROXI WIRELESS	
[TEC.TEC015] SERVIDOR DNS-DHCP	
[TEC.TEC016] SERVIDOR NOC	
[TEC.TEC017] SERVIDOR NAGIOS	
[TEC.TEC018] SERVIDOR NESSUS	
[TEC.TEC019] SERVIDOR RADIUS	
[TEC.TEC020] SERVIDOR ASA	
[TEC.TEC021] Blue Coat PacketShaper	
[TEC.TEC022] WLC	
[TEC.TEC023] RADIOS UBIQUITI	
[TEC.TEC024] RADIOS MOTOROLA	
[TEC.TEC025] CMM MICRO (motupe)	
[TEC.TEC026] CMM MICRO (san cayetano)	
[TEC.TEC027] CMM MICRO(ad. central)	
[TEC.TEC028] CMM MICRO (a. salud)	
[TEC.TEC029] SWITCHES	
[TEC.TEC030] ACCESS POINT	
[TEC.TEC031] RELOJ BIOMETRICO	
[TEC.TEC032] ROUTER:Mikrotik	
[TEC.TEC033] CENTRALILLAS TELEFONICAS	
[INT] INSTALACIONES	
[INT.INT001] DATA CENTER	
[INT.INT002] TENDIDO DE LA RED DE DATOS	
[INT.INT003] RED DE CONEXION INALAMBRICA	
[INT.INT004] ENLACES DE CONEXIÓN	
[EAX] Equipo auxiliares	
[EAX.EAX001] REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS (administrativos)	
[EAX.EAX002] REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS (docentes)	
[EAX.EAX003] PROYECCION AUDIO-VIDEO	
[EAX.EXA004] EQUIPOS DE COMPUTACION DE ESCRITORIO (administrativo)	
[EAX.EXA005] EQUIPOS DE COMPUTACION DE ESCRITORIO (bibliotecas)	
[EAX.EXA006] EQUIPOS DE COMPUTACION DE ESCRITORIO (docente)	
[EAX.EAX007] EQUIPOS DE COMPUACIÓN PORTATIL (administrativo)	
[EAX.EAX008] EQUIPOS DE COMPUACIÓN PORTATIL (docente)	
[EAX.EAX009] HERRAMIENTAS PARA MANTEMIENTO	

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

Análisis de Resultados de Impacto Acumulado.

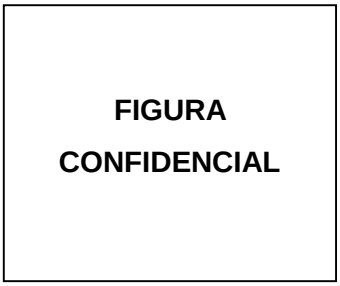


Figura 12: Impacto Acumulado ACTUAL de activos

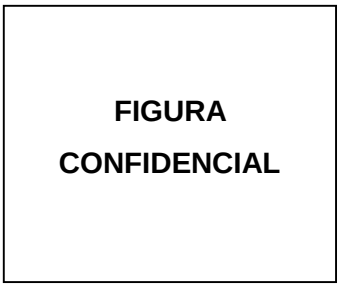


Figura 13: Impacto Acumulado POTENCIAL de activos

Nota: La información del resultado del Impacto Acumulado, resultado del proyecto ha sido omitida por ser información CONFIDENCIAL propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

3.2 Determinar si el riesgo es aceptable o necesita ser tratado a partir de los criterios de aceptación establecidos.

Para el tratamiento de los riesgos es importante considerar que el riesgo crece con el impacto y con la probabilidad de materialización de una amenaza, donde con los resultados se puede clasificar al riesgo para su tratamiento.

Con los datos obtenidos se ha determinado el riesgo acumulado para los activos **(ver TABLA XXIII)**, donde se ha utilizado los datos del impacto acumulado sobre un activo debido a una amenaza y la probabilidad de materialización de la amenaza, considerando que el riesgo acumulado permite determinar las salvaguardas que se propondrían para reducir el daño y la probabilidad de ocurrencia de fallas de seguridad, a continuación se presenta la tabla de valoración del riesgo para cada activo de información en cada una de sus dimensiones y las opciones de tratamiento en base a los criterios de aceptación establecidos en la fase dos del proyecto **(Ver Figura 14).**

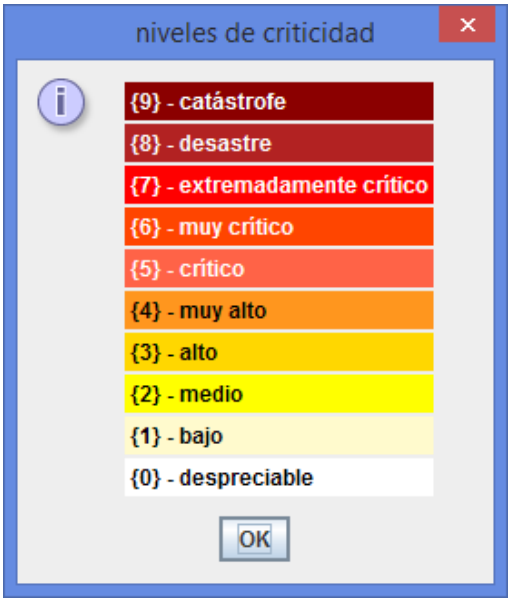


Figura 14: Leyenda de valoración (Niveles de Criticidad) de la Herramienta PILAR 5.4.2

TABLA XXIII. Valoración de Riesgo acumulado para cada activo de Información.

activo	[D]	[I]	[C]	PROMEDIO	CRITERIO	RIESGO
[APL] Aplicaciones						
[APL.APL001] SISTEMA DE GESTION ACADEMICA						
[APL.APL002] Consulta de Estadísticas del SGA						
[APL.APL003] SISTEMA DE GESTION DE APRENDIZAJE MOODLE						
[APL.APL004] SISTEMA DE EVALUACION DE DOCENTES						
[APL.APL005] SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX						
[APL.APL006] LIMESURVEY						
[APL.APL007] SISTEMA DE GESTION BIBLIOTECARIA						
[APL.APL008] PAGINA WEB DE LA UNIVERSIDAD						
[APL.APL009] SISTEMA DE EMISIÓN Y REPOSICIÓN DE TITULOS						
[APL.APLO10] FORESTWEB						
[APL.APL011] SISTEMA DE SEGUIMIENTO DE EGRESADOS Y GRADUADOS						
[TEC] TECNOLOGIA						

INFORMACION CONFIDENCIAL

[TEC.TEC001] CISCO7460						
[TEC.TEC002] Switch Servidores						
[TEC.TEC003] SERVIDOR BLADE						
[TEC.TEC004] SERVIDOR WEB						
[TEC.TEC005] SERVIDOR SGA						
[TEC.TEC006] SERVIDOR MED CURSOS						
[TEC.TEC007] SERVIDOR AEIRNNR						
[TEC.TEC008] SERVIDOR MED VIRTUAL						
[TEC.TEC009] SERVIDOR EVA						
[TEC.TEC010] SERVIDOR FINANCIERO						
[TEC.TEC011] SERVIDOR CURSOS						
[TEC.TEC012] BALANCEADOR DE APLICACIONES						
[TEC.TEC013] FIREWALL SGGW						
[TEC.TEC014] PROXI WIRELESS						
[TEC.TEC015] SERVIDOR DNS-DHCP						
[TEC.TEC016] SERVIDOR NOC						
[TEC.TEC017] SERVIDOR NAGIOS						
[TEC.TEC018] SERVIDOR NESSUS						
[TEC.TEC019] SERVIDOR RADIUS						
[TEC.TEC020] SERVIDOR ASA 5585						
[TEC.TEC021] Blue						
[TEC.TEC022] WLC						
[TEC.TEC023] RADIOS UBIQUITI						
[TEC.TEC024] RADIOS MOTOROLA						
[TEC.TEC025] CMM MICRO (motupe)						
[TEC.TEC026] CMM MICRO (san cayetano)						

INFORMACION CONFIDENCIAL

[TEC.TEC027] CMM MICRO(ad. central)						
[TEC.TEC028] CMM MICRO (a. salud)						
[TEC.TEC029] SWITCHES						
[TEC.TEC030] ACCESS POINT						
[TEC.TEC031] RELOJ BIOMETRICO						
[TEC.TEC032] ROUTER:Mikrotik						
[TEC.TEC033] CENTRALILLAS TELEFONICAS						
[INT] INSTALACIONES						
[INT.INT001] DATA CENTER						
[INT.INT002] TENDIDO DE LA RED DE DATOS						
[INT.INT003] RED DE CONEXION INALAMBRICA						
[INT.INT004] ENLACES DE CONEXIÓN						
[EAX] Equipo auxiliares						
[EAX.EAX001] REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS (administrativos)						
[EAX.EAX002] REPRODUCCIÓN Y ESCANEO DE DOCUMENTOS (docentes)						
[EAX.EAX003] PROYECCION AUDIO-VIDEO						
[EAX.EXA004] EQUIPOS DE COMPUTACION DE ESCRITORIO (administrativo)						
[EAX.EXA005] EQUIPOS DE COMPUTACION DE ESCRITORIO (bibliotecas)						
[EAX.EXA006] EQUIPOS DE COMPUTACION DE ESCRITORIO (docente)						
[EAX.EAX007] EQUIPOS DE COMPUACIÓN PORTATIL (administrativo)						
[EAX.EAX008] EQUIPOS DE COMPUACIÓN PORTATIL (docente)						
[EAX.EAX009] HERRAMIENTAS PARA MANTEMIENTO						

INFORMACION CONFIDENCIAL

Nota: La información omitida en la tabla es CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Partiendo de los resultados obtenidos, se puede observar que dentro de cada sección existen, riesgos que pueden ser considerados como riesgos ACEPTABLES, donde las medidas de mitigación sería consideradas como no prioritarias, es decir que para el

proyecto las enfocaría de forma básica y general, ya que son activos con un impacto y/o probabilidad de ocurrencia que no demanda el uso excesivo de recursos, en el caso de los riesgos que han resultado como TRATABLES, se considerará medidas de mitigación prioritarias, de acuerdo a cada sección, orientadas a reducir el impacto y el riego que estas tienen para la UTI.

Análisis de Resultado de Riesgo Acumulado

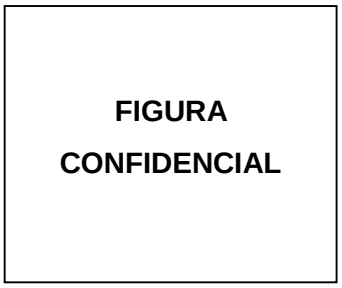


Figura 15 Riesgo Acumulado ACTUAL de activos

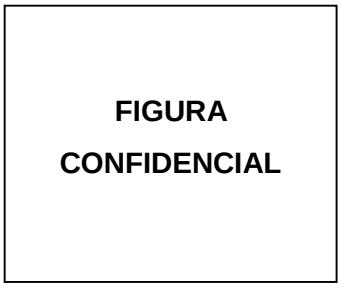


Figura 16: Riesgo Acumulado POTENCIAL de activos

Nota: La información del resultado del Riesgo Acumulado, resultado del proyecto ha sido omitida por ser información CONFIDENCIAL propiedad de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

3.3 Identificar las opciones de tratamiento de los riegos a partir de la selección de los controles adecuados del Anexo A de la norma ISO/EC 27001.

A partir del análisis de la información recolectada (entrevistas, observación y encuestas), los resultados del análisis de riesgos y el análisis de la políticas de seguridad manejadas actualmente en la UTI **(ver Anexo 13)**, se ha podido determinar los mecanismos de control adecuados referenciados en el Anexo A de la norma ISO/IEC 27001 **(ver Anexo 11)**, donde se debe considerar que los **133** mecanismos de control se encuentran distribuidos en **11 secciones** que agrupan mecanismo de protección para áreas en específico, para lo cual se los ha clasificado en base al análisis, haciendo uso de la siguiente tabla de escala **(ver Tabla XXVI):**

TABLA XXV. Tabla de las secciones que maneja el Anexo A de la norma ISO/IEC 27001 [41]

Sección	Dominio – Control	#Ctrls
A5	Política de seguridad de la información	**2**
A6	Organización de la seguridad de la información	**11**
A7	Gestión de activos de información (AI)	**5**
A8	Seguridad de los recursos humanos	**9**
A9	Seguridad física y medioambiental	**13**
A10	Gestión de operaciones y comunicaciones	**32**
A11	Control de acceso (lógico)	**25**
A12	Adquisición, desarrollo y mantenimiento de sistemas de información	**16**
A13	Gestión de incidentes de seguridad de información	**5**
A14	Gestión de continuidad de operaciones	**5**
A15	Cumplimiento regulatorio	**10**

Tabla XXVI. Tabla de Escala para calificación de Mecanismos de Control del Anexo A de la Norma ISO/IEC27001 [41]

Calificación		Descripción
N/A	No Aplica	No aplica.
0	Inexistente	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
20	Inicial	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
40	Repetible	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
60	Definido	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
80	Gestionado	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
100	Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Con los valores asignados de acuerdo al análisis de la información de referencia, se ha determinado el uso de los siguientes mecanismos de control:

Sección A5: Políticas de Seguridad de la Información.

Esta sección hace referencia en dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo a los requisitos institucionales, leyes y reglamentos pertinentes.

Donde se han considerado los dos mecanismos que la componen:

- Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.
- La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.

Sección A6: Organización de la seguridad de la información.

Esta sección hace referencia a la gestión de la organización de la seguridad de la información.

Para lo cual se han considerado los siguientes mecanismos:

- La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.
- Está establecido el proceso de autorización para nuevos activos de información (AI).
- Están definidos acuerdos de confidencialidad y se revisa con regularidad.
- Se mantiene los contactos apropiados con las autoridades pertinentes.
- El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.
- Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.
- Se trata todos los requerimientos de SI antes de dar acceso a los clientes.

Sección A7: Gestión de los Activos de Información.

Esta sección se refiere a la protección adecuada de los activos de información.

En esta sección se han considerado todos los mecanismos que la componen:

- Se mantiene un inventario de Activos de Información[8].

[8] Activos de Información (AI)

- Todo AI tiene asignado un responsable (propietario).
- Se dispone de una normativa de uso de los AI
- La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad
- Se dispone del procedimiento de rotulado y manejo de la información.

Sección A9: Seguridad física y medioambiental

Esta sección hace referencia a la prevención al acceso físico no autorizado, a los daños en las instalaciones y/o activos de información.

Para esta sección se ha hecho referencia a los siguientes mecanismos de control:

- Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.
- Se utiliza mecanismos de control de acceso en entradas críticas.
- Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.
- Se utiliza mecanismos de protección ante amenazas externas y ambientales.
- Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.
- Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).
- Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.
- Los equipos están protegidos frente a fallas de servicios públicos.
- El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.
- Los equipos son mantenidos en forma periódica.
- Se aplica seguridad a los equipos fuera del local
- Todo equipo requiere autorización para ser retirado de la Institución

Sección A10: Gestión de operaciones y comunicaciones:

Esta sección hace referencia al aseguramiento de la operación correcta y segura de los activos de información, considerando para ello los siguientes mecanismos:

- Procedimientos de operación documentados y disponibles a los usuarios.
- Gestión del control de cambios en los recursos de procesamiento de información.
- Separación de los recursos de desarrollo, prueba y producción.

- Procurar que los terceros implementen, operen y mantengan los controles de seguridad.
- Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio así como procesos involucrados y la evaluación de riesgos.
- Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.
- Implementar controles de prevención, detección y recuperación ante software malicioso, así como controles adecuados para la toma de conciencia.
- Se realiza copias de respaldo de información y software, y se prueba regularmente.
- Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.
- Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red están identificados e incluido en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratos.
- Se dispone de procedimientos para el manejo de información de manera confidencial.
- La documentación de los sistemas es protegida del acceso no autorizado.
- Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.
- Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.
- Se protege adecuadamente la información involucrada en los mensajes electrónicos.
- Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.
- Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.
- Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.
- Se registra las actividades del administrador y operador del sistema.
- Se registran las fallas, se analizan y se toma la acción apropiada.

Sección A11: Control de Acceso (Lógico)

Hace referencia al control de a los activos de información de forma lógica, para ello se han considerado los siguientes mecanismos de control:

- Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.
- Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.
- Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.
- Se dispone de procedimiento para la gestión de contraseñas.
- Se audita los derechos de acceso de manera regular.
- Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.
- Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.
- Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.
- Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.
- La identificación del equipo forma parte de la autenticación.
- Se segrega en la red, los usuarios y sistemas de información.
- Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).
- Todo usuario dispone de una cuenta de acceso única.
- El sistema de gestión de claves asegura su calidad.
- Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema **[41]**.

Sección A12: Adquisición, desarrollo y mantenimiento de sistemas de Información

Esta sección hace referencia a establecer la seguridad sea una parte integrar de los sistemas de información, para lo cual se han establecido los siguientes mecanismos de control:

- Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.
- Se validan los datos de entrada a las aplicaciones para asegurar que esta sea correcta y apropiada.
- Se incorpora mecanismos de validación en las aplicaciones para detectar corrupción de la información.
- Se valida la data de salida de las aplicaciones.
- Se controla el acceso al código fuente del sistema.
- Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo, para observar el impacto generado.

Sección A13: Gestión de incidentes de seguridad de información.

Esta sección busca asegurar que los eventos y debilidades de seguridad de información sean comunicados para realizar una acción correctiva oportuna, para cumplir con esto se han establecido los siguientes mecanismos de control:

- Los incidentes de SI se reportan por los canales apropiados tan rápido como sea posible.
- Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.
- Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.
- Se recolecta y mantiene evidencias (para fines de auditoría).

Sección A14: Gestión de continuidad de Operaciones:

Esta sección hace referencia a contrarrestar las interrupciones de las actividades de la organización activando planes de contingencia, para cumplir con ello se han considerado los siguientes mecanismos de control:

- Se dispone de un proceso de gestión de continuidad de operaciones.
- Se realiza gestión de riesgos.
- Se dispone de un Plan de Continuidad de Operaciones (PCO).

Con la elección de los ***74*** mecanismos de control adecuados en las diferentes secciones **(Ver Tabla XXVII),** para el tratamiento de riesgos asociados a los activos de información se puede desarrollar la documentación de aplicabilidad para el tratamiento de los mismos, la cual es una propuesta de solución que pretende, mediante un ***Manual de***

Políticas de Seguridad de la Información, reducir o minimizar la probabilidad y el daño de los Activos de Información al materializarse de amenazas asociadas a los mismos.

TABLA XXVII. Resumen de los mecanismos de control elegidos para el tratamiento de riegos.

Sección	#Ctrls	Detalle
A5. Política de seguridad de la información	2	(2) Política de seguridad de la información
A6. Organización de la seguridad de la información	7	(5) Organización Interna, (2) Entidades externas
A7. Gestión de activos de información (AI)	5	(3) Responsabilidad por los activos, (2) Clasificación de la información
A9. Seguridad física y medioambiental	12	(6) Áreas Seguras, (6) Seguridad del equipo.
A10. Gestión de operaciones y comunicaciones	20	(3) Procedimientos y responsabilidades operacionales, (2) Gestión de la entrega de servicios de terceros, (1) Planeación y aceptación del sistema, (1) Protección contra software malicioso y código móvil, (1) Copias de respaldo (back-up), (2) Gestión de seguridad de redes, (2) Gestión de medios (activos de almacenamiento) (4) Intercambio de información (transferencia) (4) Monitoreo (de actividades no autorizadas)
A11. Control de acceso (lógico)	15	(3) Gestión de acceso de usuarios, (3) Responsabilidades de usuario, (6) Control de acceso a la red, (3) Control de acceso al sistema operativo.
A12. Adquisición, desarrollo y mantenimiento de sistemas de información	6	(1) Requerimientos de seguridad de los sistemas, (3) Procesamiento correcto en las aplicaciones, (1) Seguridad de los archivos del sistema, (1) Seguridad en los procesos de desarrollo y soporte

A13. Gestión de incidentes de seguridad de información	4	(2) Reporte de incidentes y debilidades, (2) Gestión de incidentes y mejoras
A14. Gestión de continuidad de operaciones	3	Gestión de la continuidad operativa
	74	

Fase 4: Desarrollar la documentación de aplicabilidad para el tratamiento de riesgos identificados dentro de la UTI.

Esta última fase se basa en el desarrollo de la propuesta de solución para minimización o mitigación de los diferentes riesgos informáticos asociados a los activos de información gestionados en la Unidad de Telecomunicaciones e Información.

Esta propuesta de solución, se refiere al documento denominado "*Manual de Políticas de Seguridad de la Información"* (**ver Anexo 13**), donde este define el conjunto de Políticas de Seguridad de la Información para la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, las mismas que están encaminadas a contribuir con el cumplimiento del reglamento establecido por la Institución.

El objetivo de la Unidad de Telecomunicaciones e Información es el de gestionar y proteger los activos de información a su cargo, donde se consideran los datos e información institucional, equipos informáticos desinados a cada sección manejada en la UTI, administración de servicios informáticos considerando administración de la red de datos de la institución; creación, puesta en marcha y mantenimiento de los sistemas de información y mantenimiento de equipos informáticos propiedad de la Universidad **[5]**.

Partiendo de este objetivo, se crearon las políticas de seguridad de la información propuestas las mismas que están basadas en los resultados del estudio y análisis de riesgos realizado en el periodo **febrero-octubre de 2014**, cuyo objetivo principal fue el diseño de un modelo de gestión de seguridad de la información para la Universidad Nacional de Loja, gestionado desde la Unidad de Telecomunicaciones e Información. Este modelo de seguridad, se basa en los requerimientos de la ***fase de planificación*** de un Sistema de Gestión de Seguridad de la Información establecido en el Estándar Internacional ISO/IEC 27001 el mismo que está enfocado a: "*Tecnología de la*

Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información[9]*, Requerimientos*"; se debe considerar que este Estándar Internacional ha sido preparado para proporcionar un modelo para **establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI**, haciendo uso del modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA).

Es importante considerar las características o dimensiones de los activos de información dispuestos para el estudio, las mismas que son:

- **Disponibilidad:** La información estará lista para acceder a ella o utilizarse cuando sea necesaria.
- **Integridad:** La información ha de estar completa y correcta en todo momento.
- **Confidencialidad:** A la información solo pueden acceder las personas autorizadas para ello.

Es importante tener en cuenta que lo que busca el modelo de seguridad es cumplir con los requerimientos de la **primera fase de Planificación** de un SGSI, donde basándose en el análisis de riesgos se pretende el resguardo de los activos de información teniendo como referencia las características mencionadas.

Finalmente, para establecer adecuadamente el conjunto de políticas necesarias para la mitigación de los riesgos encontrados y asociados a los activos de información analizados, se ha considerado el ***Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005,*** este contiene 133 mecanismos de control orientados a la seguridad de la información, a partir de los cuales se ha definido el uso de **74** de ellos, con los que permitió la definición de diferentes secciones de políticas encaminadas a brindar una propuesta de solución que cumpla con las características necesarias para la mitigación de riesgos y requerimientos de la Unidad **[5,24,41] (ver Anexo 12 - 15).**

Partiendo de lo mencionando anteriormente, en esta fase se ha cumplido con tareas orientadas a crear la estructura de general del manual, tomando como referencia el "*Modelo de Políticas de Seguridad de la Administración Pública Nacional"* [6], así como también la distribución adecuada de las secciones de políticas de seguridad de la información basadas en los mecanismos de control seleccionados.

[9] Sistema de Gestión de Seguridad de la Información (SGSI)

A continuación se describen las tareas realizadas en esta fase:

4.1 Definir los motivos de elección de los mecanismos de control para el tratamiento de riesgos y la necesidad de continuidad de las políticas que actualmente se manejan en la UTI.

La elección de los **74** mecanismos de control para la creación del manual de políticas de seguridad de la información, se basó en los resultados obtenidos en cada una de las fases del proyecto, haciendo énfasis en el **análisis de las políticas de seguridad informática actuales que se maneja en la UTI y los resultados del análisis de riesgos asociados a los activos de información de las diferentes secciones de la UTI**.

Partiendo de esto se definió la siguiente estructura para las secciones de políticas del manual:

1. **Políticas generales seguridad de la información**

En esta sección se busca considerar los principios de una cultura organizacional sobre Seguridad Informática partiendo de los **9 mecanismos de control** seleccionados de las secciones **A5 y A6** del Anexo A de la Norma ISO/IEC 27001, para la definición de las políticas de esta sección, donde el compromiso del personal de la UTI es indispensable para la difusión, consolidación y cumplimiento de normativas básicas que se proponen, considerando el objetivos de la misma que es el de "*Asegurar y mantener una cultura de seguridad de la información, para la protección de los activos de información de la Universidad Nacional de Loja gestionados por la UTI, frente a las diferentes amenazas, internas o externas, deliberadas o accidentales*".

La estructura de esta sección es la siguiente:

- *Políticas de Definición*
- *Políticas de prestación de servicios*
- *Políticas de administración de recursos*
- *Política de coordinación de actividades*
- *Políticas de cobertura de los servicios*
- *Políticas de Salvaguarda y Confidencialidad*
- *Políticas de Protección de datos y sistemas*

- *Políticas de documentación digital o Impresa*
- *Políticas de incidentes de Seguridad de la Información*

Cada una de estas subsecciones está encaminada al cumplimiento del objetivo general de la sección, considerando que esta se enfocó en la continuidad de las políticas actuales manejadas en la UTI, ya que estas cubren los requisitos de los mecanismos de control definidos (**Ver Sección de Políticas generales seguridad de la información del Anexo 3 y Anexo 13**).

2. Políticas de gestión de activos de información

Esta sección va enfocada a cubrir los **5** mecanismos de control seleccionados propuestos por la sección **A7** del Anexo A de la Norma ISO/IEC 27001, estos mecanismos permiten definir la gestión de activos de información en cada una de las secciones de la UTI por parte de los responsables o custodios asignados a los mismos, donde se debe tener conocimiento de las características de estos para ser clasificados de acuerdo a la sensibilidad y criticidad de la información que manejan, así como también en base a su funcionalidad, permitiendo una rotulación eficaz para el tratamiento y protección de dichos activos **[5,24,41]**.

Cumpliendo con ello con el objetivo general de la sección que es: "*Controlar y mantener la protección adecuada de los activos de información manejada desde la Unidad de Telecomunicaciones e Información, mediante la adecuada organización y clasificación de los mismos, garantizando que los activos de información reciban un apropiado nivel de protección*".

La estructura de la sección es la siguiente:

- *Inventario de Activos.*
- *Consideraciones para clasificación de información.*

Cada una de estas subsecciones se enfoca a cubrir los mecanismos de control seleccionados, es importante considerar que se desarrolló plantillas para inventarios de activos que permiten una mejor gestión y organización de los mismos, dichas plantillas se las realizó en base a los tipos de activos, características y funcionalidades (ver **Sección de Políticas de gestión de activos de información del Anexo 13**).

3. Políticas de Seguridad física y medioambiental

El desarrollo de esta sección de políticas se basó en los **12** mecanismos de control seleccionados de la sección **A9** del Anexo A de la Norma ISO/IEC 27001, donde se pretende con estos minimizar los riesgos de daños físicos por falta de mantenimiento o perdidas de activos originados por accesos físicos no autorizados, daños por errores del personal o daños ocasionados por factores medio ambientales, que pueden interferir en el desarrollo normal de las actividades de la UTI **[24, 41]**, partiendo de esto se busca cumplir con el objetivo de esta sección que es: "*Mantener y controlar la integridad de los activos de información mediante políticas adecuadas de protección*".

La estructura de la sección es la siguiente:

- *Perímetro de Seguridad Física*
- *Control de Acceso Físico al Centro de Datos*
- *Protección de Oficinas, Centros de Cómputo, Bibliotecas e Instalaciones*
- *Desarrollo de Tareas en Áreas Protegidas*
- *Mantenimiento de Equipos (consideraciones generales)*
- *Mantenimiento Preventivo y Correctivo de Activos de Información para la sección de Mantenimiento Electrónico*
- *Políticas de control contra Software Malicioso*
- *Política de desarrollo informático*
- *Seguridad fuera de las Áreas Protegidas y Retiro de Equipos*
- *Políticas de Escritorios y Pantallas Limpias*

Las subsecciones están orientadas a satisfacer los objetivos de los mecanismos de control seleccionados para la creación de esta sección, considerando también que las subsecciones:

- *Mantenimiento Preventivo y Correctivo de Activos de Información para la sección de Mantenimiento Electrónico*
- *Políticas de control contra Software Malicioso*
- *Política de desarrollo informático*

Están enfocadas en las políticas actuales que se manejan en UTI, ya que en base a sus características se vio la necesidad de su continuidad **(ver Anexo 3).**

En esta subsección se creó una plantilla para la gestión de los procedimientos de mantenimiento preventivo, permitiendo con ello un control más adecuado al momento

de realizar este tipo de tareas (ver **Políticas de Seguridad física y Medioambiental del Anexo 13**).

4. Políticas de Gestión de Operaciones y Comunicaciones

Para la definición de esta sección se consideraron los **21** mecanismos de control seleccionados definidos en la sección **A10** del Anexo A de la Norma ISO/IEC 27001, donde se busca la minimización de riesgos de intromisión de software malicioso a los activos de información, ingresos no autorizados a la red de datos de institución, errores o problemas en la transmisión de información que puedan repercutir en la calidad de la misma.

Partiendo de lo mencionado, se busca cumplir con el objetivo de la sección que es: "*Garantizar la confidencialidad, integridad y disponibilidad de la información manejada a través de sistemas de información, asegurando el correcto funcionamiento de las redes de datos de la Institución*".

La estructura de la sección es la siguiente:

- Procedimientos y Responsabilidades Operativas
- Control de cambio en las Operaciones
- Separación entre instalaciones de Desarrollo e instalaciones Operativas.
- Planificación y Aprobación de Sistemas
- Políticas para administración y controles de equipos e infraestructura de Red.
    - ✓ Administración de Servidores
    - ✓ Políticas de uso de la Red
    - ✓ Administración de la Red Interna
    - ✓ Políticas para Acceso Remoto
    - ✓ Políticas para Administración y uso de la Red Inalámbrica
    - ✓ Políticas para Monitoreo de la Red
- Políticas de Uso del Correo Electrónico Institucional
    - ✓ Políticas de uso de las cuentas de correo electrónico institucional (@unl.edu.ec)
    - ✓ Datos técnicos y responsables
    - ✓ Facultades de la UTI
    - ✓ Sanciones.
    - ✓ Políticas Contraseñas

- Políticas de las informaciones contenidas en la Red de Internet
- Políticas de Uso de Página WEB

Con esta estructura se buscó incluir políticas que cubren los requerimientos de los mecanismos de control seleccionados **(ver sección Políticas de Gestión de Operaciones y Comunicaciones en el 13)**, considerando que las subsecciones:

- Políticas de Uso del Correo Electrónico Institucional
- Políticas de las informaciones contenidas en la Red de Internet
- Políticas de Uso de Página WEB

Están enfocadas en las políticas que maneja actualmente la UTI, ya que son servicios que se manejan de forma estandarizada a nivel institucional y son procesos definidos que no ameritan modificación y su aplicación es de importancia, por lo tanto la continuidad de estas es imprescindible **(ver Anexo 3)**.

5. Políticas de Control de Acceso Lógico

El desarrollo de esta sección está basado en los **15** mecanismos de control seleccionados de la sección **A11** del Anexo A de la Norma ISO/IEC 27001, que esta orientados a la seguridad del ingreso a los sistemas de información, bases de datos y servicios de información, contemplando en las políticas el ciclo de vida de acceso a los usuarios, desde su registro inicial hasta dar de baja cuentas que no requieren acceso.

A partir de esta perspectiva se busca cumplir con el objetivo de la sección que es: "*Asegurar la confiabilidad e integridad de la información, mediante la protección de la misma a través de contraseñas, permisos y perfiles de usuario"*

La estructura de la sección es la siguiente:

- Consideraciones Generales
- Registro de Usuario
- Gestión de Contraseñas de Usuario
- Uso de Contraseñas

Cada una de las subsecciones establecidas, buscan cubrir con los aspectos de importancia de los mecanismos de control seleccionados, donde se prioriza establecer consideraciones básicas para la creación de roles y perfiles de usuario para ingreso a

los sistemas de información, con un registro adecuado de los mismos y normativas para la gestión y uso de contraseñas por parte de los usuarios finales evitando con ello accesos no autorizados a los sistemas de información causados por suplantación de identidad de los usuarios (**ver sección Políticas de Control de Acceso Lógico en el Anexo 13)**.

6. **Políticas de Adquisición, desarrollo y mantenimiento de sistemas de información**

El desarrollo de esta sección está basado en el cumplimiento de los **6** mecanismos de control seleccionados de la sección **A12** del Anexo A de la Norma ISO/IEC 27001, donde se debe considerar que estos mecanismos se seleccionaron en base a las actividades que se realiza en la Sección de Desarrollo de Software, con el fin de mantener el control de seguridad en el desarrollo de sistemas de información, en cada una de las fases de su ciclo de vida, para con ello cumplir con el objetivo de esta sección que es: *"Definir normas y procedimientos que serán aplicados durante el ciclo de vida de los sistemas de información para garantizar la integridad, confiabilidad y disponibilidad de la información manejada por dichos sistemas".*

Partiendo de eso la estructura de la sección se definió de la siguiente forma:

- Políticas de proyectos
- Políticas de metodologías de desarrollo
- Políticas de demandantes de sistemas
- Políticas de mantención de sistemas
- Políticas de explotación de sistemas
- Políticas de desarrollo de sistemas y aplicaciones en computadores
- Políticas, normas y procedimientos para la elaboración de sistemas
    - ✓ Políticas para la elaboración de sistemas.
    - ✓ Normas para la elaboración de sistemas
    - ✓ Normas para el análisis de sistemas
    - ✓ Normas para el diseño de sistemas
    - ✓ Normas para la programación y documentación de sistemas
    - ✓ Normas para la implantación de sistemas y capacitación
- Normas para el mantenimiento de sistemas.

Es importante considerar que esta sección está enfocada en las políticas de seguridad manejadas actualmente en la UTI, ya que los procesos de desarrollo de

sistemas de información se encuentran definidos de forma general, y cubren los mecanismos de control seleccionados, por lo tanto es necesaria su continuidad y deben ser incluidos en manual propuesto (ver sección **Políticas de Adquisición, desarrollo y mantenimiento de sistemas de información en el Anexo 13 y ver Anexo 3).**

7. Políticas de Incidentes de Seguridad de la Información y Continuidad de Operaciones

El desarrollo de esta sección es de gran importancia, ya que actualmente en la UTI no existen normativos para el control de incidentes de seguridad o planes de contingencia que permitan la continuidad de operaciones en el caso de materializarse los riegos a los que están sometidos los activos de información de las diferentes secciones de la UTI, es por esto que se consideraron **7** mecanismos de control de las secciones **A13** y **A14** del Anexo A de la Norma ISO/ICE 27001, los mismos que están enfocados tanto a asegurar que los eventos y debilidades de seguridad de información sean comunicados de forma oportuna para ejecutar medidas correctivas de forma oportuna, así como también crear medidas que contrarresten las interrupciones de las actividades de la UTI, asegurando su reanudación oportuna.

La estructura de esta sección se ha definido de la siguiente forma:

- Normativas para incidentes de Seguridad de la Información
- Normativas para Continuidad de Negocio.

Estas subsecciones permiten la aplicación de los mecanismos de control seleccionados y presentan una alternativa para contrarrestar efectos en cuanto a la materialización de riesgos asociados a los activos **(ver Sección Políticas de Incidentes de Seguridad de la Información y Continuidad de Operaciones en el Anexo 13)**

4.2 Definir los motivos de omisión de los objetivos de control del Anexo A de la ISO 27001 excluidos

Partiendo de la información recolectada y los resultados obtenidos del análisis de riesgos, se han definido los mecanismos de control necesarios para el tratamiento de riegos, y de la misma forma se identificaron mecanismos que nos son aplicables al ambiente de la UTI, a continuación se describe la omisión de objetivos de control omitidos.

Sección A6 - Organización de la seguridad de la información: en esta sección se han omitido un total de **4** mecanismos de control, debido a que hacen referencia a la definición de roles y funciones de usuarios de sistemas de información cuya definición no es competencia de la UTI, ya que esto depende tanto del departamento de Recursos Humanos de la Institución así como de la dirección de cada una de las áreas a las que el usuario pertenece, este caso el personal de la UTI en base a las directrices designadas para el usuario crea un perfil de privilegios de ingreso para el manejo de los sistemas de información.

Sección A8 - Seguridad de los recursos humanos: en este caso se ha hecho la omisión de los **9** mecanismos de control que forman dicha sección, debido a que la administración de recursos humanos no son manejados dentro de la UTI, la contratación la realiza el departamento de Recursos Humanos de la Universidad considerando los requerimientos y el perfil del personal necesario sugerido por la Dirección de la UTI.

Sección A10 - Gestión de operaciones y comunicaciones: dentro de esta sección se han omitido **11** mecanismos de control, debido a que estos hacen referencia en primera instancia al tratamiento de equipos móviles, donde son equipos que no se maneja en UTI, también hace referencia a intercambio de información entidades externas a la Universidad, lo cual no es competencia de la UTI y finalmente existen mecanismos que no son aplicables en la Universidad como es la gestión de procesos de comercio electrónico, que este caso no son aplicados para institución de educación superior de carácter publica que no realiza actividades comerciales remuneradas en línea.

Sección A11 - Control de acceso (lógico): en este caso se han omitido **10** mecanismos de control que hacen referencia a temas de auditoria en cuanto al control de acceso a los sistemas, lo cual no se lo ha considerado por el hecho que se está trabajando en modelo para creación de cultura de seguridad de la información en la UTI y en este caso no se puede hacer auditorías a procesos o actividades que aún están en proceso de desarrollo, este tipo de mecanismos serán útiles en otra fase de un Sistema de Gestión de Seguridad de la Información.

Sección A12 - Adquisición, desarrollo y mantenimiento de sistemas de información: Esta sección se la ha tratado de forma especial, ya que para el desarrollo del manual se retomaron las políticas que se manejan actualmente en la Sección de Desarrollo de Software, debido a que no se ha profundizado en las actividades que se

realizan en cada una de las secciones debido a la naturaleza del proyecto, el mismo que busca dar una solución alternativa creando cultura de seguridad de la información en todas las secciones de la UTI y personal universitario cuya actividad o desempeño que depende de los equipos que gestiona la UTI.

Sección A13 - Gestión de incidentes de seguridad de información: en este caso se ha omitido **1** mecanismo de control, ya que este hace referencia a actividades de gestión de riesgos, donde el proyecto desarrollado está enfocado a dar un primer paso en el manejo de seguridad de la Información y este tipo de mecanismos vendrían a incorporarse en otra etapa de un Sistema de Gestión de Seguridad de la Información.

Sección A14 – Gestión de continuidad de Operaciones: en esta sección se han omitido **2** mecanismos de control, ya que estos hacen referencia a retroalimentación de planes de contingencia, los cuales no pueden ser aplicados ya que el manejo de la Seguridad de la Información dentro de la UTI, con el desarrollo del proyecto está en una fase inicial.

Sección A15 – Cumplimiento Regulatorio: esta sección con sus **10** mecanismos de control ha sido omitido debido a que la UTI no tiene competencia en la aplicación de reglamentos o estatutos que puedan obligan al personal al cumplimiento de actividades, esto lo maneja otra entidad dentro de la Universidad, por lo tanto no se puede emitir reglamentos de cumplimiento sobrepasando los límites de la responsabilidad de la UTI.

g. Discusión

El presente proyecto de tesis, presenta a la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, un estudio de riegos encaminados a determinar mecanismos de control adecuados para dotar un nivel apropiado de seguridad a los activos de información pertenecientes a la institución, pretendiendo con ello crear cultura de seguridad de la información a nivel institucional, dando los primeros pasos para la gestión de la información bajo estándares internacionales con la Norma ISO/IEC 27001.

1. Desarrollo de la Propuesta Alternativa

Objetivo 1: Realizar el diagnóstico de la situación actual en cuanto a seguridad de la información en función a la estructura organizacional y recursos tecnológicos disponibles en la UTI.

Para el cumplimiento adecuado de este objetivo, se realizó una entrevista de viabilidad del proyecto con el personal técnico de la UTI, determinando la necesidad de seguridad de la información institucional (Ver anexo 12), partiendo de ello se realizó el análisis de las políticas actuales implementadas en la UTI y destinadas a cada sección con la finalidad de determinar la gestión actual de la información (ver Sección 1.1 de la Fase 1 y el Anexo 3), continuando con la determinación de los activos de información escogidos para el estudio utilizando información de referencia de cada una de las secciones (ver Sección 1.2 de la Fase 1 y Anexos 4 y 5), a partir de la información recolectada se pudo establecer el entorno actual del manejo y gestión de seguridad de la información dentro de la UTI estableciendo con ello los puntos importantes a ser tratados en el desarrollo del proyecto de tesis.

Objetivo 2: Identificar los riesgos a los que está expuesta la información manejada en la UTI.

Para el cumplimiento de este objetivo se llevaron a cabo diferentes actividades siendo una de las más importantes la determinación de una adecuada metodología para análisis de riesgos como lo fue la metodología española MAGERIT v3 conjuntamente con su aplicación informática (PILAR) para la automatización de resultados (ver Sección 2.1 de la Fase 2 y Anexo 7) partiendo de ellos se cumplió con los requerimientos de la Metodología como es el caso de la valoración de los activos de información bajo las tres

dimensiones propuestas para el estudio: *Disponibilidad, Confidencialidad e Integridad (ver Anexo 6),* a partir de esta valoración y mediante entrevistas al personal técnico de cada una de las secciones de la UTI se determinó las amenazas y vulnerabilidades asociadas a los activos de información (ver sección 2.2 y 2.3 de la Fase 2), donde partiendo de ello se estableció la criticidad de los activos de información determinando su importancia para la institución (ver sección 2.4). Los resultados obtenidos fueron el primer paso para el análisis de riegos.

Objetivo 3: Determinar los mecanismos de control necesarios para el tratamiento de los riesgos identificados.

El cumplimiento de este objetivo se basó en la determinación de los riesgos asociados a los activos de información, partiendo de la probabilidad de ocurrencia de incidentes de seguridad, donde esto se obtuvo a partir de entrevistas realizadas a cada uno de los responsables de cada sección de la UTI, donde se consideró su percepción, experiencia y sugerencias técnicas para la recolección de la información (ver sección 3.1 de la Fase 3 y Anexo 8), a partir de estos resultados se determinó el impacto y riesgo actual para los activos de información con la finalidad de establecer los criterios de aceptación de riesgos (ver sección 3.2 de la Fase 3 y Anexos 9 y 10), una vez definidos los riesgos a ser tratados, se identificó los 74 mecanismos de control necesarios para la mitigación de riesgos (ver sección 3.3 de la Fase 3 y Anexo 11).

Con la determinación de los mecanismos de control necesarios a partir del Anexo A de la Norma ISO/IEC 27001, se pudo establecer la estructura de contenidos para el Manual de Políticas de Seguridad de la Información para la UTI.

Objetivo 4: Desarrollar la documentación de la aplicabilidad para el tratamiento de riesgos identificados dentro de la UTI.

Con los resultados obtenidos en las fases 1,2 y 3 del proyecto y la estructura de contenidos del Manual de Políticas de Seguridad de la Información, se determinó la importancia de continuidad de los controles actuales así como también del porque se omitió algunos de los mecanismos dispuestos por la norma (ver Sección 4.1 y 4.2), al finalizar el desarrollo de la propuesta del Manual de Políticas de Seguridad de la Información para la UTI (ver Anexo 13), se socializaron los resultados con el personal técnico de la UTI, dando por validados dichos resultados (ver Anexos 14 y 15), y de esta forma se ha brindado una solución para la mitigación de los riesgos asociados a los

activos de información, permitiendo con ello elevar el nivel de seguridad para la gestión de la información institucional.

2. Valoración Técnica Económica Ambiental.

El desarrollo del presente proyecto de tesis se llevó a cabo mediante el establecimiento de un presupuesto inicial, definiendo diferentes valores en cuento a *talento humano, recursos de hardware y software, técnicos y de comunicaciones*; que fueron primordiales para llegar al cumplimiento de los objetivos propuestos. Cabe considerar que hubo un desbalance en cuanto al propuesto original ya que debido a diferentes inconvenientes en la recolección de la información para las fases finales del proyecto, hubo la necesidad de solicitar un periodo de prórroga y por ende un incremento en los recursos utilizados.

A continuación se describe el presupuesto utilizado para el desarrollo y culminación del proyecto (ver TABLA XXVIII):

TABLA XXVIII. PRESUPUESTO

RECURSOS HUMANOS				
Descripción	Cantidad	Núm. de Horas	Valor Unitario	Valor Total
Gabriela Pardo	1	1200	5	6000,00
Director de Tesis	1	100	0	0,00
			SUBTOTAL	6000,00
RECURSOS MATERIALES				
MATERIALES DE OFICINA				
Papel (Resma)	3	—	3,50	10,50
Cartuchos	4	—	5,00	20,00
Fotocopias	700	—	0,02	14,00
Anillados	3	—	2,00	6,00
CD’s	3	—	1,00	3,00
			SUBTOTAL	53,50
SERVICIOS BÁSICOS				
Transporte	----	—	0,25	100,00
Internet	----	700	0.10	70,00
			SUBTOTAL	170,00
RECURSOS TÉCNICOS TECNOLÓGICOS				

HARDWARE				
Portatil Toshiba M645-SP4131L	1	1000	1000,00	1000,00
Flash Memory	1	—	10,00	10,00
Impresora canon MP250	1	—	60,00	60,00
			SUBTOTAL:	1070,00
SOFTWARE				
Windows 7 home premium	1	1000	150,00	150,00
Ganntt Project	1	---	0,00	0,00
Libre Office	1	---	0,00	0,00
EAR/PILAR 5.4	1	500	0,00	0,00
			SUBTOTAL	150,00
			TOTAL	**7.443,50**

El desarrollo del proyecto de tesis se lo desarrollo utilizando herramientas informáticas necesarias para obtener resultados de forma eficaz y eficiente, se debe considerar que la licencia para el uso de la herramienta de gestión de riesgos EAR/PILAR fue gestionada con los dueños de la aplicación para hacer uso de la misma bajo una licencia de tipo estudiantil o para investigación, la misma que es vendida al público a un valor estimado de 3000 euros.

Todos los gastos incurridos en el desarrollo del proyecto han sido asumidos en su totalidad por la autora del mismo.

h. Conclusiones

- Actualmente en la Unidad de Telecomunicaciones e Información, se maneja un manual de políticas de seguridad de la información que no es *estandarizado,* lo cual no garantiza la correcta protección de los activos de información que se gestionan en ella.
- La falta de registros históricos de los incidentes de seguridad informática ocurridos en la institución y resueltos por la Unidad de Telecomunicaciones e Información es un limitante al momento de realizar un análisis eficaz de riesgos, lo que ha llevado a tomar medidas alternativas para la recolección de información.
- La aplicación de la Norma ISO/IEC 27001, permite cubrir las necesidades más importantes en la gestión de la información a nivel organizacional, ya que esta engloba las mejores prácticas propuestas en sus normas antecesoras (BS77993, ISO/IEC 22301, ISO/IEC20000, UNE 71502:2004), así como normas que vienen a integrarse a ella (TIA, COBIT, ITIL).
- El uso de la metodología MAGERIT v3, en conjunto con la herramienta EAR/PILAR, para el análisis de riesgos de los activos de información, permitió medir las vulnerabilidades y amenazas asociadas a los mismos, con el fin medir su criticidad e impacto para la institución, alertando la necesidad de medidas de corrección que se debe tomar en la Unidad de Telecomunicaciones e Información.
- Los 74 mecanismo de control elegidos a partir del Anexo A de la norma ISO/IEC27001:2005, han sido adaptados para cubrir las necesidades de seguridad de la información identificadas en cada una de las Secciones de la UTI, lo que permitiría una gestión de activos de información adecuada para la mitigación de riesgos informáticos asociados a los mismos.
- La esquematización del Manual de Políticas de Seguridad de la Información propuesto en el proyecto, permitiría a la Unidad de Telecomunicaciones e Información dar los primeros pasos en la creación de cultura de seguridad de la información a nivel institucional.

i. Recomendaciones

- Es importante para la Unidad de Telecomunicaciones e Información, mantener un registro histórico de los incidentes de seguridad de la información para evaluar técnicas de mitigación, así como también crear guías eficaces para la resolución de incidentes.
- El personal técnico de la Unidad de Telecomunicaciones debe realizar análisis de riesgos y evaluación de las salvaguardas aplicadas, periódicamente con la finalidad de realizar retroalimentación en las medidas de protección, para reducir brechas de seguridad, garantizando un nivel de seguridad apropiado para la gestión de la información institucional.
- Se debe considerar realizar un análisis de riegos a profundidad en cada una de las secciones de la UTI con el fin de determinar mecanismos de control especializados en el tratamiento de riesgos asociados a las funciones y actividades específicas de cada sección, considerando que el presente proyecto se ha enfocado a un análisis global de riesgos en la UTI.
- La Unidad de Telecomunicaciones e Información debe considerar el estudio para el manejo de información en base a los procesos o procedimientos que se realizan en ella con el fin de generar un modelo para la gestión de procesos, el mismo que potenciaría la aplicación del modelo de gestión de seguridad propuesto en el proyecto.
- La Unidad de Telecomunicaciones e Información debe considerar una retroalimentación en la aplicación del modelo de gestión de seguridad de la información propuesto, una vez finalizados los cambios de entorno que actualmente se están llevando a cabo, en especial en las secciones de Redes y Telecomunicaciones.
- Para la Unidad de Telecomunicaciones e información es importante considerar la asignación de personal destinado específicamente a la gestión, manejo y aplicación de seguridad de la información a nivel institucional.

j. Bibliografía

[1] MEYER C. "*¿Seguridad informática vs. Seguridad de la Información?"*, [En línea: http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf], [Accedido el: 01-02-2015]

[2] BERTOLIN J., *SEGURIDAD DE LA INFORMACIÓN: REDES, INFORMÁTICA Y SISTEMAS DE INFORMACIÓN*, [En línea: http://books.google.com.ec/books?id=_z2GcBD3deYC&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false], [Accedido: 01.02.2015].

[3] CHAMORRO V., *PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ESTANDAR ISO 13335 APLICADO A UN CASO DE ESTUDIO,* [En línea: http://bibdigital.epn.edu.ec/bitstream/15000/5617/1/CD-4645.pdf], [Accedido el: 01.02.2015].

[4] AGUILERA P., *SEGURIDAD INFORMÁTICA*, [En línea: http://books.google.com.ec/books?id=Mgvm3AYIT64C&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false], [Accedido el: 01.02.2015].

[5] INTECO-CERT, "*CURSO DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGUÓN LA NORMA UNE-ISO/IEC 27000*", [En línea: https://www.dropbox.com/sh/kkb1bud7tba18l4/AAB8pvYU_YB_iipD8xAXRO9la?dl=0] [Accedido el: 03.02.2015].

[6] Portal de ISO 27000 en español, *SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN,* [En línea: http://www.iso27000.es/sgsi.html], [Accedido el: 03.02.2015].

[7] HERNÁNDEZ M., *DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMAICÓN EN UNA EMPRESA DEL SECTOR COMERCIAL,* [En línea: http://www.dspace.espol.edu.ec/handle/123456789/10730], [Accedido el: 03.02.2015].

[8] ISO/IEC27001:2005, *"Norma ISO/IEC 27001:2005",* [En línea: https://www.dropbox.com/s/hjpkml6t1v0t4r6/iso-27001-2005-espanol.pdf?dl=0], [Accedido el: 04.02.2015]

[9] Portal de ISO 27001 en español, *OTROS ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN",* [En línea: http://www.iso27000.es/otros.html], [Accedido el: 05.02.2015]

[10] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, "*NORMA BS7799-3"*, [En línea: https://www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3] , [Accedido el: 05.02.2015]

[11] AMERICAN SOCIETY OF HEATING, REFRIGERATION AND AIR-CONDITIONING ENGINEERS, *"NORMA BICS002",* [En línea: https://www.ashrae.org/], [Accedido el: 05.02.2015]

[12] ADVANCING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY COMMUNITY, *"NORMA ASHRAE"* [En línea: https://www.bicsi.org/book_details.aspx?Book=BICSI-002-CM-14-v5&d=0], [Accedido el: 05.02.2015]

[13] TELECOMMUNICATIONS INDUSTRY ASSOCIATION, *"NORMA TIA 942",* [En línea: http://www.tiaonline.org/], [Accedido el: 06.02.2015]

[14] KIOSKEA, *"COBIT- OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGIAS",* [En línea: https://www.dropbox.com/s/x2i0je33ai0zbjd/cobit.pdf?dl=0], [Accedido el: 06.02.2015].

[15] BITCompany, "*CobiT: UN MARCO DE REFERENCIA PARA LA INFORMACIPON Y LA TECNOLOGÍA",* [En línea: http://www.bitcompany.biz/que-es-cobit/#.VOas0EeG-So] , [Accedido el: 06.02.2015].

[16] Committee of Sponsoring Organizations of Treadway Commission, "*GUIDANCE ON GOVERNANCE AND OPERATIONAL PERFORMANCE", [En línea: http://www.coso.org/governance.htm],* [Accedido el: 07.02.2015]

[17] ECONOCOM OSIATIS, *"FUNDAMENTOS DE LA GESTION TI- ¿QUE ES ITIL?,* [En línea: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php], [Accedido el: 07.02.2015].

[18] ESTÁNDAR INTERNACIONAL ISO/IEC 27001, *TECNOLOGÍA DE LA INFORMACIÓN-TECNICAS DE SEGURIDAD-SISTEMAS DE GETIÓN DE SEGURIDAD DE LA INFORMACIÓN-REQUERIMIENTOS",* [En línea: https://drive.google.com/a/unl.edu.ec/?tab=wo#folders/0B677pBR06RvgQ041c2JPdmhXc0k], [Accedido el: 08.02.2015].

[19] BUENAÑO J., GRANDA M., *PLANEACIÓN Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 – 27002.",* [En línea: http://dspace.ups.edu.ec/bitstream/123456789/3178/1/UPS-GT000102.pdf], [Accedido el: 08.02.2015.

[20] LEON M., MOTA E., NAVARRETE J., *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN USANDO LA NORMA ISO 27000 SOBRE UN SITIO DE COMERCIO ELECTRÓNICO PARA UNA NUEVA INSTITUCIÓN BANCARIA APLICANDO LOS DOMINIOS DE CONTROL ISO 27002:2005 Y UTILIZACIÓN DE LA METODOLOGÍA MEGERIT",* [En línea: https://www.dropbox.com/s/3brtwlydjk1k5jw/Implementaci%C3%B3n%20de%20un%20SGSI.pdf], [Accedido el: 08.02.2015].

[21] ARANDA J., *IMPLEMENTACIÓN DEL PRIMER SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, EN EL ECUADOR, CERTIFICADO BAJO LA NORMA ISO 27001:2005,* [En línea: http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-39433.pdf] , [Accedido el: 03.02.2015].

[22] BUENAÑO J., GRANDA M., *PLANEACIÓN Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 – 27002.,* [En línea: http://dspace.ups.edu.ec/bitstream/123456789/3178/1/UPS-GT000102.pdf], [Accedido el: 03.02.2015].

[23] DIAZ A., *SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNE-ISO/IEC 27001,* [En línea: https://www.dropbox.com/s/lg70ev5j4iuha5k/Sistema%20de%20Gesti%C3%B3n%20de%20la%20Informaci%C3%B3n.pdf] , [Accedido el: 08.02.2015].

[24] GOBIERNO DE ESPAÑA-MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, "*MAGERIT-VERSIÓN 3.0 METODOLOGÍA DE ANALISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN, LIBRO I-MÉTODO*", [En línea: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html],[Accedido el : 26.04.2014]

[25] AGUILERA P., "*SEGURIDAD INFORMÁTICA"*, [En línea: http://books.google.com.ec/books?id=Mgvm3AYIT64C&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false], [Accedido el: 09.02.2015]

[26] DUQUE B. "*METODOLOGÍAS DE GESTIÓN DE RIESGOS",* [En línea: http://goo.gl/syjLxu], [Accedido: 09.02.2015].

[27] DIAZ M. "*ANÁLISIS DE RIESGOS: ISO27005 VS MAGERIT Y OTRAS METODOLOGÍAS*", [En línea: http://goo.gl/TDAKqf], [Accedido el: 09.02.2015].

[28] EAR/PILAR, *"HERRAMIENTA DE ANALISIS DE RIESGOS PILAR",* [En línea: http://www.pilar-tools.com/es/index.html?tools/pilar/index.html], [Accedido: 09.02.2015]

[28] ENRÍQUEZ E., "*OCTAVE, METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS DE TI*", [En línea: http://www.uv.mx/universo/535/infgral/infgral_08.html], [Accedido el: 09.02.2015]

[29] DUQUE B. "*METODOLOGÍAS DE GESTIÓN DE RIESGOS*", [En línea: http://goo.gl/syjLxu], [Accedido el: 09.02.2015.

[30] GÓMEZ R. "*METODOLOGÍA Y GOBIERNO DE LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN*", [En línea: http://www.scielo.org.co/scielo.php?pid=S0121-49932010000100012&script=sci_arttext], [Accedido el:09.02.2015].

[31] EUROPEAN UNION AGENCI FOR NETWORK AND INFORMATION SECURITY, "*IT-GRUNDSHUTZ*", [En línea: http://rm-inv.enisa.europa.eu/methods/m_it_grundschutz.html] , [Accedido el:09.02.2015].

[32] VOUTSSAS J., "PRESERVACIÓN DOCUMENTAL DIGITAL Y SEGURIDAD INFORMÁTICA", [En línea: http://www.scielo.org.mx/pdf/ib/v24n50/v24n50a8.pdf], [Accedido el: 30.01.2014]

[33] UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN, "POLÍTICAS UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN", [En línea: https://www.dropbox.com/s/ui1ki5ktufh5voj/Politicas%20de%20la%20Unidad%20de%20telecomunicaciones.docx?dl=0,], [Accedido: 04.02.2014].

[34] OCHOA M., "Desarrollo de una guía para el diseño de un proyecto de cableado estructurado acorde a las normas aplicables ANSI, EIA/TIA, J-STD, ISO/IEC", [En línea:

http://ftp.puce.edu.ec/bitstream/22000/3373/1/T-PUCE-3408.pdf], [Accedido el: 04.02.2014]

[35] JOSKOWICS J., “Cableado Estructurado”, [En línea; http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf], [Accedido el: 04.02.2014].

[36] CONFEDERACIÓN GRANADINA DE EMPRESARIOS, “Manual de Auditoría de Prevención de Riesgos Laborales”, [En línea: http://www.cge.es/PortalCGE/novedades/2011/PRLCGE/pdfs/promodi2008.pdf], [Accedido el: 04.02.2014]

[37] UNIVERSIDAD NACIONAL DE LOJA, “Estatuto por procesos de la Universidad Nacional de Loja”, [En línea: https://www.dropbox.com/s/k2p1r799lbued96/ESTATUTO%20POR%20PROCESOS%20UNL.pdf.crdownload?dl=0], [Accedido el 04.02.2014].

[38] ALVAREZ F., GARCIA P.,"*IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD*" [En línea: http://goo.gl/UANIDZ], [Accedido el: 27.04.2014]

[39] GOBIERNO DE ESPAÑA-MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, "*MAGERIT-VERSIÓN 3.0 METODOLOGÍA DE ANALISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN, LIBRO II-CATÁLOGO DE ELEMENTOS*", [En línea: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html], [Accedido el: 01.05.2014]

[40] GOBIERNO DE ESPAÑA-MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, "*MAGERIT-VERSIÓN 3.0 METODOLOGÍA DE ANALISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN, LIBRO III-GUIA DE TÉCNICAS*", [En línea: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html], [Accedido el: 01.05.2014].

[41] Anexo A de la Norma ISO/IEC 27001, “Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001”, [En línea: http://www.iso27002.es/], [Accedido el: 01.08.2014

k. Anexos

ANEXO 1: Normas de referencia y su estado de aprobación de Ediciones

Imagen 17: Normas de Referencia y su estado de aprobación de Ediciones

ANEXO 2: Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005.

Imagen 18: Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005

ANEXO 3: Políticas actuales manejadas en la UTI.

UNIVERSIDAD NACIONAL DE LOJA

POLÍTICAS UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

INTRODUCCIÓN

El presente documento define el conjunto de Políticas de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, que regirán durante el periodo 2012.

Las políticas presentadas en este documento se enmarcan dentro del reglamentación establecido por la Institución, que respecto de estas áreas considera:

La definición de los objetivos, políticas y planes informáticos, deben estar siempre acorde a los objetivos, políticas y planes que la Universidad tenga respecto de su acción como entidad educacional.

Los objetivos, planes y políticas, deberán estar supervisadas y aprobadas por la Dirección de Telecomunicaciones e Información. Todo cambio o alteración debe ser informado y respaldado por las mismas autoridades.

La Unidad de Telecomunicaciones e Información se define como el área de servicios que tiene como clientes todas las áreas de nuestra Universidad Nacional de Loja e incluyendo la MED.

La Unidad de Telecomunicaciones e Información deberá cautelar los bienes muebles e inmuebles de la Universidad que le sean de su competencia, dentro de los cuales se consideran los datos e información que le sean confiados para su protección, administración, operación, revisión, adaptación y en general, toda acción relacionada con las funciones que al departamento le son propias.

Toda acción de incorporación de tecnología y servicios informáticos para la Universidad Nacional de Loja, se debe realizar bajo las normativas establecidas en los procesos de adquisición de equipos y recursos informáticos.

Establecer, de acuerdo a los marcos legales existentes los contratos para cada servicio que lo requiera (Internet.....); los que deberán tener una duración tal que asegure la continuidad y calidad del servicio.

Las políticas institucionales de seguridad informática de la CCSS están basadas en lo establecido en la "Norma ISO/IEC 17799:2000 la cual es un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", dicha norma ofrece recomendaciones en la gestión de la seguridad de la información, y define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad. A continuación se definen dichos conceptos:

1. Confidencialidad: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
2. Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
3. Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Este documento contiene una serie de políticas que deberán ser acatadas por los funcionarios, docentes y estudiantes de la Universidad Nacional de Loja.

La Universidad Nacional de Loja tendrá profesionales capacitados y calificados en la Unidad de Telecomunicaciones e Información, en concordancia con la labor y cargo que cada uno desempeñe.

Alcances

La aplicabilidad de estas políticas rige para la Universidad Nacional de Loja en su totalidad y conjunto. Los sistemas, equipos, software, líneas telefónicas y enlaces de comunicación adquiridos o contratados con cualquier finalidad por las diferentes áreas y departamentos, con anterioridad a la fecha de emisión de estas políticas, quedarán igualmente sujetos a ellas y a las auditorías que pudieran realizarse bajo su amparo.

POLITICAS GENERALES

Políticas de Definición

La Unidad de Telecomunicaciones e Información se constituye como Unidad de Servicios Informáticos y Telecomunicaciones para la Universidad Nacional de Loja.

Los usuarios son responsables exclusivos de los datos que manipulen en los ordenadores proporcionados por la Universidad Nacional de Loja y están normados al uso que la Institución establece.

Políticas de prestación de servicios

Los servicios que la Unidad de Telecomunicaciones e Información en sus diferentes secciones son: Mantenimiento Electrónico, Redes y Equipos Informáticos, Telecomunicaciones y Desarrollo de Software.

Los servicios prestados deben, para todos los casos, poseer una métrica de calidad, mediante la cual se midan: tiempos de respuesta, calidades de solución, calidades de satisfacción usuaria, entre otras variables.

La prestación de servicios de las secciones de la Unidad de Telecomunicaciones e Información debe, en todo momento, estar dotado de trazabilidad de procedimientos. Lo anterior implica procesos formales de solicitud de servicios, acción, respuesta y aceptación.

Políticas de administración de recursos

La administración y explotación de los sistemas de información serán realizadas con personal responsable perteneciente a la Universidad Nacional de Loja. Este personal esta conformado por los profesionales que se encargan de la manipulación directa de la información el cual se identificara como Unidad de Telecomunicaciones e Información.

Será responsabilidad de la UTI la administración de los recursos asociados a los sistemas de información y comunicación de la UNL. La responsabilidad por la administración de estos recursos.

La UTI es responsable de la calidad (fidelidad, oportunidad, consistencia y redundancia) de la información de la cual es administrador técnico. Además, deberá definir normas de administración y acceso a la información proporcionada por quienes establezcan los procedimientos de control.

La UTI deberá proveer los mecanismos de protección y control necesarios que aseguren la integridad y privacidad de los datos almacenados en los archivos y bases de datos que tenga en custodia.

La UTI deberá proveer de los mecanismos de respaldo necesarios que aseguren la continuidad operativa ante siniestros que afecten a los archivos y bases de datos que tenga en custodia.

Política de coordinación de actividades

Todo proyecto de modernización o innovación Tecnológicos que se lleve adelante en la Universidad Nacional de Loja que incluya aspectos relacionados con sistemas de información, equipos computacionales, software y transmisión de datos, voz e imágenes, contará con el apoyo logístico y técnico de la UTI.

Políticas de cobertura de los servicios

La UTI procurará extender la cobertura de los servicios de tecnología de información a todas las áreas de la Universidad Nacional de Loja en la medida que ello sea posible y sea del interés de nuestra Institución.

Políticas de Salvaguarda y Confidencialidad

Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza, que bajo cualquier medio le sea entregada de parte de la Universidad Nacional de Loja, y que forme parte de los datos, información, procedimientos, conocimientos, comportamientos, actividades, desempeños, funcionamientos, metodologías, rutinas, acciones y en general de toda expresión, en el medio que fuere, que pertenezca a la propiedad exclusiva de la Universidad Nacional de Loja.

Se incluye en este punto, toda información de tipo comercial, financiero, metodológicas, de procesos, de conocimientos propios y adquiridos, experimentales, ya sea su conocimiento de carácter privado o público y que pertenezca a la Universidad Nacional de Loja.

Políticas de Protección de datos y sistemas

El equipo computacional perteneciente a la Universidad Nacional de Loja estará bajo la exclusiva administración de la UTI y por lo tanto queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:

- Manipulación no autorizada.
- Apertura, reemplazo y/o desconexión de componentes.
- Reasignaciones permanentes o temporales sin autorización.
- Instalación de programas, sistemas, módulos y/o archivos externos.
- Empleo de juegos y/o programas con fines no laborales.
- Modifica la configuración de sistemas, programas o dispositivos.
- Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.
- Conexión a redes eléctricas o de Datos no certificadas y o autorizadas

Respecto de lo definido con el fin de proteger las instalaciones, equipos, datos y sistemas de la acción de virus computacionales, será lo estipulado por la UTI lo que permanezca vigente y con prohibición para los usuarios el modificar y/o transgredir las disposiciones establecidas.

Políticas de documentación digital o Impresa

Respecto a la documentación, toda la Unidad de Telecomunicaciones e Información deberá documentar todas sus actividades que realizan en la Institución, en un sistema informático de documentación y el sistema de registro de solicitudes de los usuarios de la institución, con el fin de medir el trabajo realizado y la eficiencia del servicio brindado.

POLÍTICAS ESPECÍFICAS A LAS SECCIONES DE LA UTI.

POLITICAS DE LA SECCIÓN DE DESARROLLO DE SOSFTWARE

Políticas de proyectos

Los proyectos que la Universidad Nacional de Loja aborde, y que se relacionen con la tecnología de información, deberán estar contemplados en el Plan de Desarrollo la UTI.

El Plan de Desarrollo de la UTI de la Universidad Nacional de Loja, y por lo tanto el plan de desarrollo de sistemas incluido en él, deberán estar autorizados por las autoridades máximas de la Universidad o por la estructura administrativa que sea establecida para tales efectos.

El Plan de Desarrollo deberá ser revisado con una periodicidad mínima de una semana en cuanto a cumplimiento y orientación.

El Plan de Desarrollo de la UTI deberá contemplar, al menos, los siguientes puntos:

- Plan de Sistemas
- Plan de Hardware
- Plan de Software
- Plan de Telecomunicaciones

En los contratos de desarrollo de sistemas, que se convengan con empresas consultoras externas, se incluirá una garantía de cumplimiento de lo convenido contractualmente, por un período de a lo menos un (1) año a contar de su implantación.

Políticas de metodologías de desarrollo

El desarrollo de sistemas se llevará a cabo mediante el uso de técnicas estructuradas de análisis y diseño de sistemas.

Se deberá elaborar, mantener y administrar los datos de la Universidad Nacional de Loja mediante una Base de Datos Institucional.

Las estructuras de almacenamiento de datos de todo sistema de información que se requiera desarrollar, deberán ser diseñadas considerando compatibilidad con la estructura de almacenamiento de la base de datos de la institución.

El diseño de los sistemas de información se orientará a un ambiente cliente-servidor.

La Universidad Nacional de Loja debe poseer un conjunto estructurado de normas y reglas que definan la interfaz que los sistemas presenten al usuario.

Estas reglas deben establecer mecanismos únicos y universales que, establecidos como estándares, se constituyan en el medio de interacción con los datos. Las cuales serán entregadas y aprobadas por el área de desarrollo.

Políticas de demandantes de sistemas

A las diferentes áreas demandantes de sistemas les corresponderá una activa participación en el proceso de desarrollo de sus sistemas, comprometiendo tiempo efectivo de apoyo a las actividades de análisis, modelamiento de datos, diseño administrativo, y puesta en marcha de los sistemas.

Los actuales sistemas en explotación, desarrollados con lenguajes de última generación en un ambiente de Base de Datos Relacional, conforme al modelamiento general de la Universidad Nacional de Loja, se deben certificar por el área de desarrollo.

Políticas de mantención de sistemas

Toda mantención de sistemas, deberá ser dirigida por la UTI de la Universidad Nacional de Loja. Los recursos, plazos y costos que originen las mantenciones de sistemas se regirán por la normativa y procedimientos vigentes al momento de realizarla.

Políticas de explotación de sistemas

La explotación de los sistemas de información residentes en los computadores de la UTI, será de exclusiva responsabilidad de los administradores de los mismos.

La UTI será el organismo encargado de proporcionar o coordinar la capacitación de los usuarios para la incorporación, operación y uso de sistemas de información.

Los funcionarios que tengan equipos, serán responsables de la conservación y buen uso de dicho equipamiento.

Políticas de desarrollo de sistemas y aplicaciones en computadores

Las funciones, procesos, sistemas y aplicaciones que se realicen con los productos de computación, deberán constituirse en parte integral de los sistemas de la Universidad Nacional de Loja, como complemento a los sistemas y/o funciones de ésta y no transformarse en sustitutos de ellos.

La protección, custodia y respaldo de los datos pertenecientes a los sistemas y aplicaciones basados en computadores y que no se tengan en el servidor de la red, serán de responsabilidad exclusiva de sus administradores o usuarios.

La UTI será el organismo encargado de proporcionar apoyo y asesoría técnica a los usuarios para la incorporación y uso de productos estándares de computación que requieran.

POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA ELABORACIÓN DE SISTEMAS

1. Objetivo

Establecer las políticas, normas y procedimientos que permitan homogeneizar el desarrollo de sistemas de información dentro de la Universidad Nacional de Loja.

2. Introducción

El software es el objeto de análisis y estudio de una de las ramas más jóvenes de ingeniería. De hecho, podemos decir que la concepción misma del software, es decir, su naturaleza de construcción y desarrollo es lo que lo hace particularmente distinto. Entre las características fundamentales del software podemos mencionar que su naturaleza es abstracta debido a que su herramienta principal es el manejo de la información. Además el software se desarrolla, no se fabrica como cualquier producto en un sentido clásico; se crea mediante la transformación del poder intelectual y cerebral de los especialistas en el conocimiento.

Consecuentemente, siendo la información uno de los recursos más valiosos de cualquier institución u organización, es de gran importancia contar con sistemas que permitan su uso eficiente, en armonía con todas las áreas. Para garantizar que esto ocurra dentro de la Universidad Nacional de Loja es indispensable contar con políticas, normas y procedimientos que permitan homogeneizar la elaboración de sistemas de información.

3. Políticas para la elaboración de sistemas

La política de calidad se define como las directrices u objetivos generales que tiene la Universidad Nacional de Loja concernientes a la calidad, las cuales son emitidas por la Unidad de Telecomunicaciones e Información.

Objetivo

Establecer un marco de referencia general para garantizar que los sistemas de información que apoyan las tareas sustantivas de una institución o empresa, sean concebidos y desarrollados de una manera tal, que permitan su articulación para una adecuada interacción entre las áreas.

Políticas

- Toda elaboración de sistemas deberá estar orientada a satisfacer las necesidades de manejo de información para las funciones sustantivas de la Universidad Nacional de Loja; es importante concebir el diseño de dichos sistemas de manera que permitan su integración y consolidación en una base de datos.
- Toda elaboración de sistemas, tanto interna como externa, debe cumplir con las normas establecida por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, El cumplimiento de las normas es un requisito indispensable para considerar un sistema apto para su liberación definitiva.
- Toda elaboración de sistemas, tanto interna como externa de carácter institucional, deberá estar avalada por un informe técnico de la unidad de Telecomunicaciones e Información, este debe normar el uso y aprovechamiento de los recursos informáticos de acuerdo al reglamento interno de la Institución.
- La elaboración de sistemas institucionales debe apegarse a los estándares en cuanto al uso de software. Cuando esto no sea posible, el área usuaria deberá solicitar un dictamen técnico a la dirección de informática de la institución o empresa, justificando plenamente el uso de las herramientas propuestas para el desarrollo.
- Todos los sistemas y sus componentes desarrollados por el personal de la institución son propiedad de la Institución, por lo que la Universidad tendrá los derechos de autor para la utilización de dichos desarrollos en las diferentes áreas que así lo requieran.
- Durante el análisis, desarrollo e implantación de cualquier sistema, el área solicitante deberá participar con la Unidad de Telecomunicaciones e Información.
- Es responsabilidad de la Unidad de Telecomunicaciones e Información, el proporcionar la capacitación y asistencia técnica al personal operativo sobre el correcto uso del Sistema.
- La Unidad de Telecomunicaciones e Información establecerá de manera formal su política de calidad en cuanto a las normas y procedimientos por utilizar, con objeto de que funcione eficazmente el sistema informático de la Institución.
- En la elaboración y diseño de sistemas informáticos internos la Unidad de Telecomunicaciones e Información será la encargada de establecer y mantener un sistema de calidad documentado para asegurar productos conforme a los requerimientos especificados por ella misma, además de alcanzar consistentemente los objetivos de calidad de la institución o empresa. Entre los documentos que se generarán por los desarrolladores, están los manuales de procedimientos, técnicos, de instalación, operativos y de usuario.
- la Unidad de Telecomunicaciones e Información será el encargado de establecer políticas de administración, calidad y control de calidad; así como, la justificación y consistencia de éstas. Periódicamente tiene la obligación de revisar las políticas establecidas y evaluar los resultados logrados.

Normas para la elaboración de sistemas

Objetivo

Definir la metodología a la que debe someterse todo el personal involucrado en la elaboración de sistemas, con objeto de obtener productos de alta calidad que resulten de fácil mantenimiento para cualquier miembro del equipo de trabajo.

Normas generales

1. Los desarrollos de sistemas, tanto internos como externos, deberán respetar los lineamientos y estándares definidos por la Unidad de Telecomunicaciones e Información para el Desarrollo de Sistemas.
2. La Unidad de Telecomunicaciones e Información y su sección de Desarrollo de Software deberán registrar, ordenar y inventariar: los programas fuentes y ejecutables, documentación técnica, manual de instalación y manual del usuario.
3. Para los desarrollos internos y externos, cualquier área de la institución deberá entregar a la dirección de Telecomunicaciones e Información el original del sistema con su respectiva

documentación y todos aquellos elementos que hagan posible su incorporación al Repositorio de Sistemas de la Unidad, conservando una copia.

4. Todos las fases del desarrollo de sistemas deberán estar documentadas.
5. Para aquellos sistemas que se desarrollen con un software no estándar para la institución, será requisito indispensable que cuenten con un módulo de intercambio de información (importación/exportación) a través de múltiples protocolos o servicios (Webservice, LDAP). Por ninguna causa se deberá comenzar la etapa de programación del sistema en general, sin antes tener concluidas las etapas de análisis y diseño. Para el caso en que el sistema por su magnitud se haya dividido en módulos, será válido el comenzar la programación de cada uno de ellos si se cuenta con sus etapas de análisis y diseño concluidas, además de un análisis y diseño preliminar de carácter general del sistema.

Normas para el análisis de sistemas

1. Los desarrollos de sistemas deberán contar con un estudio de factibilidad tecnológica y económica que permita identificar y describir las necesidades del usuario con objeto de justificar la elaboración del sistema.
2. Se deberán establecer los grupos de trabajo encargados para las actividades de diseño de encuestas, entrevistas, recopilación de datos, etc.
3. La fase de análisis de sistemas deberá apegarse a las metodologías de análisis orientados a objetos.

Normas para el diseño de sistemas

1. De existir manuales de procedimientos vigentes en la institución o empresa, todos los grupos de trabajo involucrados en el diseño de sistemas deberán tener conocimiento del contenido de ellos, a fin de reflejarlos en el sistema cuando éstos lo afecten.
2. La fase de diseño de sistemas deberá apegarse a las metodologías de análisis y diseño orientado a objetos.
3. Para los casos en los cuales se efectúe un cambio en el diseño de un sistema, dicho cambio deberá ser documentado previa revisión y justificación, así como aprobación de los responsables para posterior control de la documentación, con el fin de que todas las áreas se enteren del cambio efectuado.

Normas para la programación y documentación de sistemas

1. Todos los programas que integren cualquier sistema deberán estar documentados conforme al Manual de Procedimientos para el Desarrollo de Sistemas.
2. El área usuaria deberá aprobar el manual del usuario previo a la liberación de un sistema. La Unidad de Telecomunicaciones e Información deberá revisar que el manual técnico se apegue a las especificaciones.
3. La Unidad de Telecomunicaciones mantendrá un control de la documentación de los sistemas.
4. La Unidad de Telecomunicaciones tendrá un estricto control de documentación, actualizando los contenidos según el mejoramiento continuo de los sistemas.
5. Todos aquellos códigos que sean objeto de programación, ya sean módulos, programas, pantallas, etc., deberán contener información de quién efectuó la programación y en qué fecha; de ser posible en el mismo software, mediante comentarios y adicionalmente en la documentación por escrito.
6. Después de concluida la programación de una parte del sistema, se deberá registrar en un documento que dicha parte del sistema ha sido concluida, especificar el o los nombre(s) del o los programador(es), así como el tiempo de programación en horas; esto con el fin de establecer un control de calidad del trabajo de los programadores.

Normas para la implantación de sistemas y capacitación

1. Antes de liberar un nuevo sistema, éste deberá ser sometido a pruebas de aceptación definidas por el área solicitante, utilizando para ello datos reales. En el caso de nuevas versiones, será necesario realizar corridas en paralelo para verificar su correcto funcionamiento con respecto a la versión anterior.

2. La capacitación al personal técnico-operativo formará parte fundamental de la liberación de un sistema. Dicha capacitación deberá cubrir todas las necesidades y requerimientos que el área usuaria especifique de común acuerdo con la Unidad de Telecomunicaciones e Información.
3. El proceso de capacitación deberá ser posterior a la aprobación de los manuales: a) técnico, b) de instalación, c) de operación y d) del usuario, que constituirán la guía con la que se lleve a cabo dicho proceso.
4. Los manuales de operación deberán especificar los métodos de manejo que permitan cuidar la integridad, tanto física como lógica de los elementos que conforman el sistema, ya sean datos, información, software, hardware y documentación.
5. Las pruebas de aceptación deberán ser clasificadas en: preliminares, para los casos en que se pruebe el módulo o el programa de manera individual, y totales, cuando se encuentren ensamblados todos los componentes del sistema. Para cada una de estas pruebas, se llevará un control de los resultados obtenidos.
6. Las corridas de prueba que se realicen con el fin de acreditar un sistema como aceptado, deberán efectuarse con una cantidad de datos superior al 50% de la cantidad de datos que el sistema correrá de manera cotidiana, y con el equipo de cómputo en el que se pretende operar sistemáticamente. Para el caso de sistemas que operen en red, también se deberán efectuar pruebas con usuarios concurrentes.
7. Los tipos de datos con los cuales se efectúen las pruebas deberán estar apegados a la realidad, a fin de tomar en cuenta el rango de valores que soportará el sistema y posteriormente realizar una gráfica de rendimiento de cantidad de datos contra el tiempo de procesamiento. En el caso de sistemas para trabajo en red, deberán establecerse elementos que permitan observar objetivamente el desempeño del sistema. Si los resultados de rendimiento del sistema no son aceptables para fines prácticos, se consignará el módulo para su re-trabajo en programación.

Normas para el mantenimiento de sistemas

Los usuarios deberán informar, solicitar cambios en el sistema a unidad de Telecomunicaciones e Información, siempre y cuando se identifiquen y justifiquen plenamente los ajustes y cambios basados en el reglamento y que son necesarios que permitan mejorar el desempeño y cobertura del sistema en cuestión.

Aquellos códigos del sistema que no trabajen de manera óptima con respecto a las necesidades o rendimiento que se pretenda satisfacer, serán dispuestos a un proceso de re-trabajo; en primera instancia a quien realizó la programación, y en último caso a un nuevo equipo de trabajo para programación, esto considerando un estilo de programación diferente que sea más adecuado a la necesidad a satisfacer. La situación anteriormente descrita debe registrarse en la documentación correspondiente.

Manual de procedimientos para el desarrollo de sistemas (MPDS)

Introducción

El presente Manual de Procedimientos para el Desarrollo de Sistemas (MPDS) está dirigido a las personas directamente relacionadas con el desarrollo de sistemas; como tal, representa una guía para orientar y normar los trabajos y actividades involucradas en el análisis, diseño y desarrollo de los sistemas.

Existen varias metodologías y tecnologías que apoyan el desarrollo de sistemas, la mayoría de éstas identificadas con los métodos de análisis y diseño orientado a Objetos. Este manual de procedimientos está organizado siguiendo los lineamientos de dichos métodos; establece una metodología constituida por una serie de actividades orientadas a regular las acciones de los analistas.

Los procedimientos para el desarrollo de sistemas que se presentan en este manual se encuentran apoyados en las políticas y normas anteriormente descritas.

Objetivo del MPDS

Describir los procedimientos para cada una de las etapas que comprenden el desarrollo de sistemas.

Etapas para el desarrollo de sistemas

Con el fin de contar con un marco conceptual uniforme, se considera el "ciclo de vida de un sistema" constituido por cinco etapas:

1. Análisis
2. Diseño
3. Programación y documentación
4. Implementación (pruebas) y capacitación
5. Mantenimiento

En las siguientes secciones se define el objetivo de cada etapa, se describe en qué consiste y se listan las principales actividades involucradas.

Por último, en la tabla de formas o formatos para la documentación de sistemas se resumen los productos que deben obtenerse en cada una de las etapas de desarrollo, se identifican los responsables de cada una de ellas: área usuaria (U), área de informática (I) y, en caso de existir, empresa responsable del desarrollo (E). Es de gran importancia integrar estos productos en un expediente que permita conocer todas las etapas del ciclo de vida de un sistema, asegurando así su continuidad a través de la independencia del grupo de trabajo que lo desarrolló.

El desarrollo de sistemas se hará según la metodología de desarrollo ágil de sistemas que será aceptado mediante la discusión del grupo de desarrollo para construir un software de calidad, este resultado será descrito en una acta que servirá para todo el desarrollo de software de la Institución.

Para la etapa de programación será seleccionado el lenguaje de programación considerando que sean de Software Libre, el mismo que después de un consenso, de estabilidad, escalabilidad y tenga su plataforma una vigencia de mínimo 10 años.

El Mantenimiento de sistemas permite garantizar la permanencia en operación de un sistema, mejorándolo, adaptándolo a nuevos requerimientos o corrigiendo problemas que sean detectados durante su operación. Este proceso involucra todas las etapas de su desarrollo. Cuando el objetivo es mejorarlo o adaptarlo, el mantenimiento reinicia los trabajos del desarrollo en la etapa de análisis. Cuando se trata de corregir un problema puede reiniciarse en el análisis, el diseño o la programación, por lo que esta parte del ciclo de vida de un sistema queda sustentada en las secciones anteriores de este manual.

Antes de modificar un sistema debe analizarse cuidadosamente si dicha modificación está justificada; de ser así debe procederse con la misma metodología utilizada durante el desarrollo, para llevar a cabo nuevamente las fases que sean necesarias del análisis, diseño, programación e implantación, poniendo especial atención en dejar una documentación completa y clara de los cambios efectuados, ya que de no hacerlo puede resolverse temporalmente un problema, pero también se contribuye a la rápida degradación del sistema.

POLÍTICAS DE LA SECCIÓN DE MANTENIMIENTO ELECTRÓNICO

Políticas de Mantenimiento Preventivo y Correctivo de los Recursos Informáticos

La Unidad de Telecomunicaciones comunicará el programa de mantenimiento preventivo a las diferentes dependencias de la Universidad Nacional de Loja; informando a los usuarios la fecha de visita de mantenimiento del equipo, con al menos dos días de anticipación.

Antes de llevarse a cabo la actividad de mantenimiento, los usuarios deberán respaldar la información almacenada en la computadora.

Las oficinas deberán programar sus actividades de tal manera que el equipo esté disponible en la fecha programada para el mantenimiento.

El Mantenimiento (mejora ó modificación) de los sistemas de información en operación (En plataforma Base de datos, Web e Intranet), deben estar acorde al Plan estratégico y Plan de Desarrollo Institucional.

Políticas de Servicio de Soporte Técnico

Todas las solicitudes de soporte técnico deberán plantearse a la Unidad de Telecomunicaciones e Información a través del sistema e-tickets quién las recibirá y resolverá oportunamente.

Sólo se atenderán solicitudes que se refieran al software y hardware propiedad de la Universidad Nacional de Loja, es decir que cuenten con el código de bodega correspondiente.

A través de las solicitudes de servicio se cuantificará el servicio prestado y permitirá establecer programas de capacitación y/o adiestramiento enfocados a áreas o temas deficitarios, sustitución de equipo, etc.

Política de mantención de las configuraciones computacionales

Los servicios de mantención técnica de los equipos y de actualización del software básico y programas producto, serán proporcionados por la sección de mantenimiento.

Políticas de respaldos de información

La responsabilidad de la realización de los procedimientos de respaldos corresponde a la sección de Mantenimiento.

Se deberán realizar los siguientes tipos de respaldos sobre equipos informáticos de la Institución:

- Respaldos de disco total.
- Respaldos imagen de disco.
- Respaldos de bases de datos.
- Respaldos Diarios
- Respaldos Semanales.
- Respaldos Mensuales
- Respaldos Semestrales
- Respaldos Anuales

Políticas de estaciones de trabajo

Políticas de adquisición, control y mantención de microcomputadores

Los requerimientos de computadores, ya sea para apoyo de procesos administrativos serán atendidos por la UTI en la siguiente modalidad:

Estación de trabajo: Las estaciones de trabajo serán adquiridas y deberán ser renovados según el período establecido por la Dirección de Recursos Humanos y Servicios Administrativos de la Universidad Nacional de Loja. De este modo se asegurara un nivel tecnológico mínimo, con respecto a lo sugerido por UTI.

Servidores: La UTI cuenta con equipos servidores para procesamiento de datos, que son equipos con tecnología de vanguardia y los cuales anualmente serán chequeados y evaluados para su potenciamiento.

Políticas de administración de equipamiento

Cada equipo con su software será asignado a un usuario (funcionario perteneciente a la Universidad Nacional de Loja), quién será el responsable, para todos los efectos, del uso de dichos recursos.

Por razones de seguridad, se privilegiará la mantención interna de los equipos de computación.

Con relación a los nuevos requerimientos de equipos de computación, éstos serán Adquiridos y/o arrendados a la Empresa que ofrezca la mejor alternativa costo/beneficio y deberán previamente ser autorizados por la Dirección Financiera previo informe técnico de la Unidad de Telecomunicaciones e Información.

Políticas de derechos de autor y propiedad intelectual del software

Se considerarán dos categorías de software que se obtenga por este medio:

1. ***Shareware:*** Es aquel que una persona o entidad física que lo desarrolló ha puesto a disposición del público para un período de prueba, al término del cual el usuario se compromete a pagar un cierto monto si desea seguir utilizándolo; caso contrario deberá eliminarlo de su equipo.
2. ***Freeware:*** Es aquel que la persona o entidad que lo desarrolló ha puesto a disposición del público de manera gratuita, solicitando en ocasiones un donativo para seguir con los trabajos, que el usuario no esta obligado a pagar.

Las licencias que se otorgan con este software determinan las condiciones para su uso, debiendo quedar claro para el usuario a que categoría corresponde el programa obtenido, para proceder conforme al marco que se estipule.

El usuario deberá notificar a la Unidad de Telecomunicaciones información, la existencia de este software, en caso que decida utilizarlo por un período prolongado, incluyendo el nombre, características y funciones del programa, además del motivo para su utilización.

La falta de conocimiento de la existencia de dicho software por parte de la Unidad de Telecomunicaciones e Información será responsabilidad del usuario en caso de la realización de una auditoría informática.

Prohíbase la reproducción o copia no autorizada de los programas computacionales que posee la Universidad Nacional de Loja, así como el uso de programas que no hayan sido adquiridos o autorizados por ésta.

Será responsabilidad de los funcionarios que tengan acceso al uso de equipos, evitar e impedir la reproducción o copia ilegal de programas computacionales, manteniendo un control de los programas en uso.

Los equipos y software de computación estarán destinados exclusivamente a ser utilizados como apoyo a las funciones propias de la Universidad Nacional de Loja y sus unidades.

Política de desarrollo informático

Objetivo:

Esta política tiene como objetivo el disponer de lineamientos que contribuyan a realizar inversiones exitosas en beneficio del desarrollo tecnológico informático institucional.

Los equipos y dispositivos que se adquieran deberán contar con la garantía de línea del fabricante, con el software y documentación técnica correspondiente.

Todos aquellos equipos que son necesarios para el funcionamiento de algún sistema de misión critica deberán contar con un contrato de servicio de soporte, una vez vencida la garantía.

Para la adquisición de computadoras, impresores y servidores se deberá observar que los mismos cubran como mínimo las especificaciones estándar.

Solamente se deben adquirir equipos integrados de fábrica (la totalidad de sus componentes) y cuyas marcas cuente con presencia y permanencia demostradas en el mercado nacional e internacional, y que cuenten con soporte local.

Los dispositivos de almacenamiento así como las interfaces de entrada/salida, deberán estar acordes con el estándar establecido.

Toda mejora de la red informática, sea expansión ó modificación debe estar acorde a las necesidades de la Institución y estándares establecidos.

Para la adquisición de software como: Sistemas Operativos, Bases de Datos, Lenguajes de Programación, Programas Integrados, Antivirus, Correo Electrónico, Control de Proyectos, Diseño Gráfico y Multimedia se deberá observar que los mismos cubran las especificaciones estándares establecidas.

Deberán adquirirse las últimas versiones liberadas de los software seleccionados, y solo en determinados casos bajo situaciones especificas, la Unidad de Telecomunicaciones e Información, podrá recomendar su adquisición en forma distinta.

Todo Software utilizado en la institución debe ser adquirido de forma legal, respetando la ley de Derechos de Autor y Propiedad Intelectual correspondientes.

Los proyectos de desarrollo y/o mantenimiento de sistemas de información de acuerdo a las necesidades de la institución pueden ejecutarse internamente ó a través de la contratación de servicios.

Los sistemas de información desarrollados interna ó externamente deben estar acorde a los estándares establecidos.

Los proyectos de desarrollo informático nacerán como respuesta a la necesidad de cumplimiento de determinados objetivos de la Institución y estarán enmarcados dentro del Plan Estratégico y Plan de Desarrollo Institucional. Por tanto, los proyectos tendrán siempre objetivos y finalidades específicas y hay que considerarlos como las herramientas para el logro de los objetivos institucionales.

Todo Proyecto de desarrollo informático debe iniciar con la etapa de planificación, que nos determina el alcance, etapas, tiempo y recursos necesarios para su ejecución.

El personal informático debe tener una capacitación continua y permanente, para el uso eficiente de los recursos informáticos e implantación de nuevas tecnologías acorde a la necesidades de la Institución.

El personal no informático debe tener una capacitación constante sobre las tecnologías implantadas, para el buen uso y desarrollo de la Institución.

POLÍTICAS DE LA SECCIÓN REDES Y EQUIPOS INFORMÁTICOS

Objetivo.- Regular el uso de los servicios de Redes, Correo Electrónico y el acceso a Internet, para lo cual se emiten los siguientes lineamientos para todo el personal que utilice los recursos de la Red.

Políticas de redes de microcomputadores

La Universidad Nacional de Loja, a través de su Unidad de Telecomunicaciones e Información, orientará la incorporación de redes locales de computadores de plataformas abiertas, en función de satisfacer las necesidades propias de cada unidad y de interconexión con la red Institucional.

La conexión entre redes locales de las diferentes áreas, para permitir el acceso e integración de la información en diferentes ambientes, independiente de su ubicación geográfica, será responsabilidad única y exclusiva de la UTI.

La UTI con su sección de redes Y equipos informáticos supervisará el funcionamiento, uso y mantención de las redes de computadores existentes en la Universidad Nacional de Loja.

Las redes de comunicaciones deberán estar acorde a las normas y estándares aceptados en materias de comunicaciones.

Políticas de enlaces para la transmisión de datos

La UTI será el responsable de estudiar, evaluar y proponer la contratación de enlaces para la transmisión de datos.

Políticas de Estándares Aplicables en la Instalación de Redes de Datos.

Se deberá etiquetar el cableado, las extensiones y los tableros de distribución eléctrica.

Se deberá evitar los cableados sueltos o dispersos, éstos deberán entubarse en el caso de los tendidos horizontales no vistos, en el caso de los tendidos horizontales o verticales vistos deben colocarse canaletas adecuadas.

Para equipos informáticos es recomendable disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

Previo a la instalación de equipos informáticos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

Políticas de uso de la red

La UTI a través de su sección de Redes es el responsable de ofrecer este servicio. Este servicio sólo deberá utilizarse con fines académicos.

Generales :
El servicio de red será proporcionado a todo usuario autorizado que cuenta con una computadora y hace uso de la red. Los usuarios autorizados son:

a. Alumnos activos, profesional, maestría
b. Profesores de cátedra o de planta activos
c. Personal de apoyo activo
d. Departamentos y direcciones.

La UTI a través de su sección de Redes ofrece los siguientes servicios de red:

a. Conectividad a la red local (LAN) con nodos alámbricos e inalámbricos
b. Acceso a Internet
c. Acceso a Servicio ofrecidos por la UNL , siendo estos: Correo electrónico, Bibliotecas Virtuales,
d. Otros

La UTI a través de su sección de Redes se reserva el derecho de bloquear sitios de Internet (si previo aviso) que no cumplan con fines académicos o de investigación.

La UTI a través de su sección de Redes se reserva el derecho de restringir y negar servicio de red (sin previo aviso) en equipos que se detecte algún abuso en el servicio o provocar interrupciones en el servicio por virus y/o gusanos.

La UTI a través de su sección de Redes se reserva el derecho de restringir y negar servicio de red (sin previo aviso) en equipos que se detecte utilizando programas de P2P (Kaza, btorren, imesh, ares y otros) que genere tráfico.

La UTI a través de su sección de Redes restringirá el servicio de red aquellos usuarios que intentan violar la seguridad de cualquier equipo computacional o de red.

No está permitido el uso de la red para juegos recreativos.

No está permitido instalar equipo de red que no sea autorizado por La UTI a través de su sección de Redes

Está prohibido levantar servicios como pueden ser servidores web, ftp, dhcp, dns, irc, de correo o instalar una dirección fija en una máquina.

El usuario que se detecte usando software que invada la privacidad de alumnos, profesores, personal o equipo computacional se le restringirá el servicio de red.

Es responsable el usuario por los sitios que visite en Internet.

El usuario es responsable de la información (audio, video, documentos, etc.) que baje de Internet o Intranet y deberá respetar los derechos de autor. En caso de no hacerlo responderá por el uso la información de la cual no cuente con la licencia o autorización respectiva antes las autoridades que lo requieran

Cada Alumno, profesor o personal de campus universitario, tiene derecho a usar una tarjeta de red alámbrica e inalámbrica siempre y cuando se utilice en el mismo equipo pero no al mismo tiempo por lo que el uso de esta es responsabilidad del usuario.

Los usuarios tiene derecho a utilizar la red siempre y cuando respeten los puntos antes mencionados.

Los usuarios gozan de privacidad de su información, con la excepción de aquellos en los que se detecten acciones que pongan en riesgo la seguridad de la red del campus universitario..

Es responsabilidad del usuario realizar las actualizaciones necesarias a sus sistemas operativos así como las instalaciones críticas de su equipo computacional.

Es responsabilidad del usuario conocer las políticas de uso de la red.

El no tener conocimiento de estas políticas no es justificante para evitar respetarlas.

El usuario que no respete cualquiera de los puntos antes mencionados se le restringirá el servicio de red en el campus de manera temporal hasta que se presente a la UTI para ser revisado su equipo computacional.

Cualquier punto no estipulado en estas políticas queda a juicio de la UTI, al igual que las sanciones correspondientes.

Cualquier punto no contemplado en estas políticas será estudiado y resuelto por la UTI.

Políticas de uso del correo electrónico

Disposiciones Generales

Estas políticas son de carácter general y de cumplimiento obligatorio para todos los alumnos, docentes y empleados que tienen asignada una cuenta de correo en el dominio @unl.edu.ec

La cuenta de correo identifica de manera única a cada usuario y es a través de ella que puede enviar y recibir mensajes de otros alumnos, profesores y empleados de la Universidad Nacional de Loja.

La cuenta se dará de baja en el momento que el alumno, profesor o empleado deje de pertenecer a la Universidad Nacional de Loja.

Si un alumno, profesor o empleado tiene un problema relacionado con su cuenta de correo, deberá tratarlo personalmente, acudiendo a la Unidad de Telecomunicaciones e información de la Universidad Nacional de Loja.

La cuenta de correo electrónico (nombre de usuario y contraseña) se entrega únicamente al titular de la misma, no se puede entregar a través de otra dirección de correo o por teléfono, por motivos de seguridad.

Se asignaran las cuentas por departamento. Las cuentas para Simposios o Grupos Estudiantiles se darán con el visto bueno de la Dirección de la Unidad de Telecomunicaciones e Información.

Obligaciones del Usuario

La cuenta de correo electrónico es personal e intransferible, por lo que queda estrictamente prohibido dar a otros la posibilidad de uso.

El alumno, docente o empleado es completamente responsable de todas las actividades realizadas con su cuenta de correo proporcionada por la UTI.

Una vez que el alumno, docente o empleado haya recibido su cuenta de correo electrónico (nombre de usuario y contraseña), deberá cambiar su contraseña por motivos de seguridad.

El alumno, docente o empleado es responsable de respetar la ley de derechos de autor, no distribuyendo de forma ilegal software licenciado o reproduciendo información sin conocimiento del autor.

El buen uso de su cuenta se entiende por:

- Usar su cuenta con fines académicos y/o investigación.
- Respetar las cuentas de otros usuarios.
- Usar un lenguaje apropiado en sus mensajes.
- No mandar ni contestar cadenas de correo.
- No usar su cuenta para fines comerciales.

- No enviar material obsceno o con intención de intimidar, insultar o acosar.

Es responsabilidad del alumno, docente o empleado depurar continuamente su cuenta para mantener el espacio libre suficiente que garantice la recepción de mensajes.

Es responsabilidad del alumno, docente o empleado respaldar sus archivos de correo. Los mensajes que considere importantes deberá mantenerlos en su equipo personal o en su defecto, en carpetas dentro de su cuenta, cuidando no exceder la cuota permitida.

Está completamente prohibido realizar cualquier abuso de los tipos definidos en el Abuso de Correo Electrónico.

Los alumnos están obligados a reportar cualquier abuso de los tipos definidos en el Abuso de Correo Electrónico a la UTI, para evitar que esto vuelva a suceder al mismo o a otros.

Políticas de uso del servicio de correo electrónico institucional (@unl.edu.ec)

1. Descripción del Servicio

El servicio de correo electrónico institucional con el dominio @unl.edu.ec se lo proporciona a la comunidad universitaria con el objetivo de apoyar las comunicación digital a nivel directivo, departamental, académico, administrativo y estudiantil en la Universidad Nacional de Loja.

El acceso al servicio de correo electrónico de la institución está sujeto a la aceptación de la Política de Uso.

El correo electrónico institucional se encuentra bajo la plataforma educativa de Google Apps for Education, la que proporciona servicios integrados como: Gmail, Google Talk, Google Calendar, Google Drive, Google Sites, Google Groups, Lucidchart, entre otros servicios educativos.

El acceso al correo electrónico se lo realiza por medio del Portal Web Educativo: http://unl.edu.ec, en el banner Correo Electrónico o por medio del enlace directo a la página de ingreso al correo: http://webmail.unl.edu.ec, el servicio se encuentra administrado en la sección de Redes y Equipos Informáticos de la Unidad de Telecomunicaciones e Información.

2. Políticas de uso de las cuentas de correo electrónico institucional (@unl.edu.ec)

Se definen las políticas que cada uno de los miembros de la comunidad universitaria deben de respetar y aceptar:

- Todo docente, personal administrativo, direcciones departamentales y académicas, autoridades, estudiantes, contarán con una cuenta de correo electrónico, la cual deberá ser utilizada y revisada continuamente con fines institucionales.
- Todo oficio, invitación o trámite que no requiera de una firma o sello institucional se lo replicará por medio del correo electrónico.
- Los usuarios son completamente responsables de todas las actividades realizadas con su cuenta de correo electrónico de la institución.
- Como falta grave es facilitar y ofrecer su cuenta de correo electrónico a personas no autorizadas, las cuentas de carácter personal son intransferibles y las cuentas de dependencias son transferibles.
- El servicio de correo electrónico es una herramienta para el intercambio digital de información entre miembros de la comunidad universitaria no es una herramienta de difusión de publicidad, cadenas, entre otros fines.
- No está permitido enviar correos a personas que no desean recibirlo. Si la institución recibe quejas, denuncias o reclamos por estas prácticas se procederá con las sanciones correspondientes de acuerdo al caso.
- Están completamente prohibidas las siguientes actividades:

- Utilizar el correo electrónico para propósitos comerciales, fines de lucro y actividades ajenas a la comunidad universitaria.
- Distribuir de manera masiva grandes cantidades de mensajes con contenidos inapropiados para la comunidad universitaria.

- Ya que el servicio es proporcionado por una solución computacional en la nube que lo brinda Google Apps for Education, el usuario podría almacenar los correos en sus ordenadores institucionales o personales por medio de un cliente de correo y así tener acceso a los mismos en cualquier instante.
- Toda información o contenido que sea transmitido por las cuentas de correo de la institución son responsabilidad únicamente del dueño de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.

3. Datos técnicos y responsables

- La dirección de correo electrónico se compondrá de: nombre.primerapellido@unl.edu.ec, para el sector docente y administrativo; dependencia@unl.edu.ec, para las direcciones departamentales y académicas, [inicialesdenombres][primerapellido][inicialsegundoapellido]@unl.edu.ec, para el sector estudiantil.
- La contraseña que se asigna al crear la cuenta es el número de cédula, le pedirá de manera automático el cambio de misma.
- Las cuentas de correo electrónico son administradas por la Unidad de Telecomunicaciones e Información, en la sección de Redes y Equipos Informáticos.
- Se puede enviar archivos adjuntos por medio de la cuenta de correo electrónico cuyo tamaño total no exceda los 25 Mb.
- Cada cuenta de correo electrónico tienen una capacidad de almacenamiento de 25Gb.
- El uso de API y la compatabilidad facilita la integración de Google Apps con otros sistemas.
- Se cuenta con un certificado de Seguridad ISAE 3402 tipo II lo que permite que los datos privados y seguros de cada una de las cuentas de correo electrónico.
- Cualquier duda o soporte con el correo electrónico se lo puede hacer con envío de un mensaje a la siguiente cuenta institucional: soporte@unl.edu.ec o visitar el sistema de ayuda de escritorio http://soporte.unl.edu.ec para reportar la incidencia.

Facultades de la UTI

La UTI se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la UNL y de su comunidad.

La vigencia de las cuentas será definida por la UTI.

Sanciones.

El incumplimiento por parte del alumno, profesor o empleado del buen uso de su cuenta puede ocasionar la suspensión y posterior baja de su cuenta.

Cualquier situación no contemplada dentro de los puntos anteriores será evaluada por la UTI.

Políticas Contraseñas.

La contraseña deberá cambiarse periódicamente (se recomienda cada semestre).

La contraseña no debe ser la misma que el nombre de usuario; se deberán evitar fechas, nombres de familiares o cualquier dato que pueda ser deducido por alguien.

La contraseña debe estar formada por al menos 8 caracteres. Se recomienda que al menos tenga alguno de estos caracteres: una letra mayúscula, dos números y por lo menos un carácter especial (!$%&*()_-+=[]|?/<>).

Políticas de las informaciones contenidas en la Red de Internet:

La Universidad Nacional de Loja no controla, ni es responsable del contenido y veracidad de las informaciones obtenidas o recibidas a través de la red de Internet. La UTI no se hace responsable por la exactitud o calidad de la información obtenida por este medio.

Los usuarios de Internet de la UNL son responsables de reportar inmediatamente a la Unidad de Informática (vía electrónica, telefónica o por escrito) cualquier situación en la red que pueda comprometer la estabilidad o seguridad del servicio de cualquier forma, así como cualquier violación a esta política.

Políticas de Uso de Página WEB

Los usuarios que tienen los derechos para la actualización de la página web, deben realizar los procedimiento conforme el manual de usuario de la página web.

Es responsabilidad del usuario autorizado informar a la Unidad de Informática a la mayor brevedad, algún daño ocasionado a la página web por mala manipulación de la aplicación de administración de la pagina web.

En todo momento, el usuario es el responsable único y final de mantener en secreto las Claves ó Passwords asignadas, con los cuáles tenga acceso a la aplicación de administración de la pagina web.

El responsable del contenido, calidad y actualidad de los datos publicados en la página web es la persona encargada del área, así dicha información sea obtenida e incorporada por sus colaboradores.

La Unidad de Protocolo y Comunicación es el ente encargado y responsable de revisar la redacción de la información que se publica en la página web.

POLÍTICAS DE LA SECCIÓN DE TELECOMUNICACIONES

Políticas de uso de sistemas de comunicaciones

Las unidades que, para el mejor desempeño de sus actividades, necesiten utilizar sistemas de radiocomunicaciones podrán hacerlo, ateniéndose a las normativas legales vigentes emanadas de la subsecretaría de Telecomunicaciones y autorizadas por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

POLÍTICAS PARA EL USO DEL EQUIPO COMPUTACIONAL

El Objetivo de las siguientes políticas es presentar las principales normas para el acceso de los alumnos, docentes y empleados de la UTI, además del comportamiento que han de observar en beneficio de la comunidad universitaria.

Definiciones:

Equipo Computacional. Se considera como equipo computacional a todo aquel equipo de cómputo, audiovisual, accesorio, periférico de telecomunicaciones y relacionado con cualquiera de éstos, que esté instalado en la sala de computadoras, laboratorios de cómputo, aulas tecnológicas, oficinas, administrados por la Unidad de Telecomunicaciones e Información.

Usuarios. Se consideran usuarios de los servicios de cómputo a los alumnos y profesores y empleados activos del campus universitario.

Políticas de uso del equipo computacional.

El equipo computacional deberá utilizarse como herramienta de apoyo para labores académicas y administrativas. Su uso es exclusivo para los alumnos, profesores y empleados activos inscritos en el período académico.

Normas de Comportamiento

El comportamiento de todos los usuarios debe ir a favor de la moral y de las buenas costumbres.

El uso adecuado del equipo computacional será responsabilidad del usuario, por lo que cualquier daño que se haga al equipo o a las instalaciones, será evaluado por la UTI, y si fuere necesario, el usuario se hará acreedor a una sanción y multa que cubra el monto del daño.

El personal de Seguridad y el personal de la UTI está autorizado a pedir al usuario que se retire de la Sala, Laboratorio de Computo especializado, aula teórica u oficina, por jugar, por tener una conducta inapropiada y/o cometer alguna falta expresada en este reglamento, el usuario deberá mostrar respeto y obedecer las indicaciones.

Prohibiciones dentro de la Sala, Laboratorio de Computo especializado, aula u oficina

- Introducir alimentos, bebidas o fumar.
- Desconectar, mover y/o extraer equipo computacional o sus partes.
- Alterar o dañar las etiquetas de identificación del equipo computacional.
- Utilizar grabadoras, radios o equipos de sonido sin audífonos.
- Utilizar los equipos computacionales como máquinas de juegos; esto incluye utilizar software de juegos o el acceso a servicios que impliquen el uso de juegos.
- Utilizar el equipo computacional para desarrollar programas o proyectos ajenos al interés académico de la Universidad.
- Copiar y/o alterar software.
- Utilizar los equipos computacionales para acceder a servicios locales o remotos a los que el usuario no tenga autorización explícita, o en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional.
- Utilizar claves de acceso de otros usuarios, o permitir que otros usuarios utilicen la propia.
- Enviar mensajes a otros usuarios de manera anónima.
- Utilizar una identidad diferente a la propia, ya sea de otro usuario o ficticia, para enviar mensajes vía electrónica.
- Utilizar los equipos como medio de comunicación interactiva.
- Llevar a cabo acciones que puedan interferir con la operación normal de los equipos computacionales.

Sanciones
Las sanciones por infracción a cualquier punto del reglamento son:

Por la primera vez se notificará a su superior y se le suspenderá por un día el acceso a los equipos.
En la segunda ocasión se suspenderá por una semana su cuenta de acceso a equipos y se dará aviso a su superior.

En la tercera ocasión se suspenderá su cuenta de acceso a equipos definitivamente y por igual se dará aviso a su superior.

Bloqueo de equipo.

Políticas de Seguridad Computacional

Políticas de Uso Aceptable

La UTI no es responsable por el contenido de datos ni por el tráfico que en su red circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.

No se permite el uso de los servicios de la red cuando provoquen una carga excesiva sobre recursos escasos.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la UNL y se usarán exclusivamente para actividades académicas relacionadas con la institución.

Todas las cuentas de acceso a los sistemas y recursos de cómputo son personales e intransferibles, se permite su uso única y exclusivamente a los propietarios de las mismas.

Cuando se detecta un uso no aceptable de la red, se cancela la cuenta o se desconecta temporal o permanentemente al usuario involucrado. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

ANEXO 4: Topología de Red al 2013 levantada por el personal técnico de la UTI

Figura 19: Topología de Red de la Universidad Nacional de Loja al 2013

ANEXO 5: Inventario de aplicaciones que maneja la UTI

Tabla XXIX. Inventario de Aplicaciones de la Sección de Desarrollo de Software

Departamento	Nombre	Categoría (Tipo	Plataforma (SO)	# Licencias	Fecha Inicio de	Uso que se le da	Forma de operación	Estado
Sección de Desarrollo de	Sistema de Gestión	Sistema de	GNU/Linux, Python		Octubre de 2008	Gestión de la información	Gestionado de forma	En producción
Sección de Desarrollo de	Consulta de	Cliente de Servicios	GNU/Linux, PHP			Consultar datos estadísticos de la	Gestionado de forma	
Sección de Desarrollo de	Sistema de Gestión de	Sistema de	GNU/Linux, PHP	GPL	Octubre 2011	Gestionar Trabajos Autónomos de	Gestionado de forma	En producción
Sección de Desarrollo de	Sistema de Evaluación	Sistema de	GNU/Linux, Python		Julio 2012	Generación de Encuestas	Gestionado de forma	En producción
Sección de Desarrollo de	Sistema de Gestión	Sistema de	GNU/Linux, PHP	GPL	Octubre 2010	Crear, enviar, recibir, almacenar,	Gestionado de forma	Pendiente fase de
Sección de Desarrollo de	Limesurvey	Sistema de	GNU/Linux, PHP	GPL		Repositorio de encuestas físicas de	Gestionado de forma	En producción
Sección de Desarrollo de	Sistema de Gestión	Sistema de	GNU/Linux, Java		Octubre 2012	Gestión de todos los recursos		En producción
Unidad de	OSTicket	Sistema de	GNU/Linux, PHP	GPL	Enero 2012	Sistema de gestión y reportes de	Gestionado de forma	En producción
Algunas carreras	Gestión Académica de	Sistema de	Visual Basic			Administración de información		En producción
Laboratorio de Análisis de	Forestweb	Sistema de registro	Python		Enero 2012	Registro y edición de maderas,	Se opera como una	En producción
Unidad de	Sistema de	Sistema de	GNU/Linux, PHP		Aun no tiene inicio	Administración de información		
Secretaría General de la	Sistema de emisión y	Sistema de	Visual Fox Pro		desde el 2008	Registro , emisión y rectificaciones	Instalado sobre un	En producción
Unidad de	Página web de la	Portal de	GNU/Linux, PHP		No hay expediente	Publicación y divulgación de toda la	Gestionado de forma	En producción

ANEXO 6: Entrevista para valoración de activos en cada sección.

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Sistemas

María Gabriela Pardo Cuenca, egresada de la carrera de Ingeniería en Sistemas, solicito a usted se digne responder la presente encuesta, que permitirá recolectar información referente a la valoración de los activos de información que maneja la Unidad de Telecomunicaciones e Información (UTI) de la Universidad Nacional de Loja, los mismos que han sido clasificados de acuerdo a cada sección que maneja la UTI, a continuación se describe los aspectos para la valoración de los activos, definidos en los criterios de evaluación en los que se basa la norma ISO/IEC 27001, esta información es de gran importancia para sustentar la *fase dos* de mi proyecto de tesis denominado: "*MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001*".

DESCRIPCIÓN:

La valoración de los activos es de gran importancia para analizar las amenazas y vulnerabilidades a las que puedan estar sometidos los mismos, es por ello que es importante conocer el valor que estos tienen para la organización y su importancia. Para esto se debe calcular cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

Esta valoración se hará de acuerdo con una escala cualitativa con un rango numérico de 1 -4 bajo los criterios de **DISPONIBILIDAD, INTEGRIDAD y CONFIDENCIALIDAD**, de acuerdo a lo que se mostrara en las siguientes tablas:

DISPONIBILIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Cuál sería la importancia o trastorno que tendría que el activo no estuviera disponible?

TABLA XXX. Valoración de Disponibilidad

VALOR	CRITERIO
1	No es relevante / importancia de disponibilidad del 0% - 9%
2	Debe estar disponible al menos el 10% - 49% del tiempo
3	Debe estar disponible al menos el 50% - 90% del tiempo
4	Debe estar disponible 90% o más del tiempo.

INTEGRIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Qué importancia tendría que el activo fuera alterado sin autorización ni control?

TABLA XXXI. Valoración de Integridad

VALOR	CRITERIO
1	No es relevante / importancia de modificación menor al 9%
2	No es relevante los errores que se presenten o la información que falte
3	Tiene que estar correcta y completa al menos en un 50%
4	Tiene que estar correcta y completa al menos en un 95% o más

CONFIDENCIALIDAD: Para la valoración de este criterio debe responderse la siguiente pregunta:

¿Cuál es la importancia que tendría que el activo se accediera de manera no autorizada?

TABLA XXXII. Valoración de Confidencialidad

VALOR	CRITERIO
1	No es relevante / importancia de acceso menor al 9%
2	Daños muy bajos, el incidente no trascendería del área afectada
3	Los daños serían relevantes, el incidente implicaría a otras áreas
4	Los daños serían catastróficos, la reputación y la imagen de la UTI se verían comprometidos.

TABLA XXXIII. Valoración de Activos Sección de Redes y Equipos Informáticos – Sección de Telecomunicaciones*.

TABLA XXXIV. Valoración de Activos de la Sección de Desarrollo de Software*

TABLA XXXV. Valoración de Activos Sección de Mantenimiento Electrónico*.

***Nota: La información, resultado de la entrevisa, fue omitida por ser CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Univerdad Nacional de Loja.**

ANEXO 7: Licencia de uso para la Herramienta Pilar

gabi pardo cuenca <mgpardoc@unl.edu.ec>

SOLICITUD DE LICIENCIA PARA ESTUDIO

gabi pardo cuenca <mgpardoc@unl.edu.ec> 12 de junio de 2014, 13:47
Para: ccn@cni.es

Saludos,
Yo, Maria Gabriela Pardo Cuenca, de nacionalidad Ecuatoriana, me encuentro realizando mi proyecto de tesis para la carrera Ingenieria en Sistemas de la Universidad Nacional de Loja (www.unl.edu.ec), el mismo que se titula: "Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la Norma ISO/IEC 27001", donde para la fase de análisis de Riegos del proyecto he elegido la metodologia Magerit, donde la herramienta que PILAR seria de gran ayuda para la aplicación de dicha metodologia, por lo tanto, solicito a quien corresponda se me permita obtener una licencia EDUCATIVA dirigida exclusivamente para el desarrollo de mi proyecto que es dedicado para la Universidad y con intereses netamente educativos.

Esperando su respuesta, expreso mi agradecimiento.

Atentamente,

Maria Gabriela Pardo Cuenca
Estudiante de la Carrera de Ingenieria en Sistemas de la Universidad Nacional de Loja
LOJA - ECUADOR

Figura 20: Solicitud de Licencia de Herramienta PILAR

gabi pardo cuenca <mgpardoc@unl.edu.ec>

pilar /licencia /edu

jose a. manas <jmanas@pilar-tools.com> 13 de junio de 2014, 11:14
Para: gabi pardo cuenca <mgpardoc@unl.edu.ec>

LA INFORMACIÓN ANEXA LE CAPACITA PARA EL USO DEL PROGRAMA

EAR / PILAR
EAR / Pilar Basic
EAR / microPILAR

DE ANÁLISIS DE RIESGOS Y GESTIÓN DE CONTINUIDAD.
EL USO ES CONCEDIDO POR A.L.H. J. MAÑAS BAJO LOS TÉRMINOS
DESCRITOS EN LA LICENCIA INCLUIDA CON EL PAQUETE
PARA SU USO EN:

- actividades educativas
- actividades de investigación

QUEDANDO EXPLÍCITAMENTE EXCLUIDO CUALQUIER USO LUCRATIVO.

El profesor solicitante asume la responsabilidad de que la
licencia recibida se emplee exclusivamente en el ámbito de
la actividad formativa para la que se ha concedido,
así como el compromiso de reportar los incidentes que
pudieran producirse al respecto.

Los incidentes se reportarán a la dirección

info@pilar-tools.com

Se adjunta la licencia de uso (fichero .lic).
Por favor, conserve a mano una copia de esta licencia
para futuras referencias.

El paquete se descarga desde la web

http://www.pilar-tools.com

Utilice la licencia para activar la copia descargada,
siguiendo las instrucciones

http://www.pilar-tools.com/es/index.html?tools/pilar/first_time/

La documentación puede descargarla o consultarla en línea en la misma sede web.

También puede interesarle la formación en línea

http://www.pilar-tools.com/es/training/audea.html

Dirección de soporte técnico:

support@pilar-tools.com

La licencia incluye el uso de la siguiente versión

http://www.pilar-tools.com/download/pilar_beta.htm


http://www.pilar-tools.com/download/pilar_basic_beta.htm
http://www.pilar-tools.com/download/pilar_micro_beta.htm

Por favor, note que se encuentra en estado beta,
por lo que su utilización es bajo su exclusiva responsabilidad.

Atentamente,
José A. Mañas <jmanas@pilar-tools.com>

C36218.lic
1K

Figura 21: Licencia para el Uso de Herramienta PILAR

ANEXO 8: Entrevista de Probabilidad

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Sistemas

María Gabriela Pardo Cuenca, egresada de la carrera de Ingeniería en Sistemas, solicito a usted se digne responder la presente encuesta, que permitirá recolectar información referente a la valoración de amenazas que pueden afectar a los activos de información que son responsabilidad de la Unidad de Telecomunicaciones e Información (UTI) de la Universidad Nacional de Loja, los mismos que han sido clasificados de acuerdo a cada sección que maneja la UTI, a continuación se describe los aspectos para la valoración de amenazas asociadas a cada activo, los criterios de evaluación se basan en los propuestos en la norma ISO/IEC 27001, esta información es de gran importancia para sustentar la fase tres de mi proyecto de fin de carrera denominado: "MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001".

1. Datos del proyecto

PFC	Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001
Departamento	Unidad de Telecomunicaciones e Información
Autora	María Gabriela Pardo Cuenca
date	Enero - Noviembre de 2014

Descripción

Para la identificación de amenazas a las que están sometidos cada uno de los activos, se ha considerado la información recolectada a partir de entrevistas realizados a las personas responsables de cada una de las secciones de la UTI, así como también analizando datos referentes a investigaciones similares a nivel nacional, y considerando el "catálogo de elementos" que proporciona la metodología Magerit v3 de análisis de riesgos, la misma que ha sido elegida para el desarrollo del proyecto.

La clasificación que se ha considerado para las amenazas es la siguiente:

De origen natural: accidentes naturales (terremotos, inundaciones, etc.) que pueden suceder y causar daños a los activos.

Del entorno (de origen industrial): accidentes o desastres industriales (contaminación, fallos eléctricos, etc.) ante los cuales los sistemas de información son víctimas pasivas.

Causada por las personas de forma accidental: Las personas con acceso a los sistemas de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada: Las personas con acceso a los sistemas de información pueden causar daño o problemas intencionados, donde dichos ataques pueden ser con ánimo de beneficiarse indebidamente, o con ánimo de causar daño y perjuicios a los legítimos propietarios.

Se debe considerar que no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía, para lo cual se debe evaluar la amenaza en base a la influencia en el activo, en dos dimensiones:

Degradación: cuán perjudicado resultaría el valor del activo, donde la degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

Probabilidad: cuán probable o improbable es que se materialice la amenaza.

Para medir estos valores, se considera la experiencia del personal a cargo de cada sección así como sucesos históricos ocurridos en la UTI, considerando que en algún momento pueden llegar a ocurrir, para ello se consideran las siguientes escalas de medición:

PROBABILIDAD: La probabilidad se mide para cada amenaza asociada a cada activo y de forma independiente.

CALIF.	VALOR	SIGNIFICADO	TIEMPO ESTIMADO
5	MR	Muy Raro	Siglos
4	PP	Poco Probable	Cada varios años
3	P	Posible	Una vez al año
2	MP	Muy Posible	Mensualmente
1	S	Casi Seguro	A diario

DEGRADACIÓN: La degradación se mide en las tres dimensiones de valorización del activo disponibilidad, integridad y confidencialidad, considerando que debe ser para cada amenaza asociada para cada activo.

CALIF.	VALOR	SIGNIFICADO	PORCENTAJE ESTIMADO
5	T	Total	81% - 100%
4	MA	Muy alta	61% - 80%
3	A	Alta	41 – 60%
2	M	Media	21 – 40%
1	B	Bajo	0 – 20%

2. Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
-

3. Dominios de seguridad

- [base] Unidad de Telecomunicaciones e Información
  Director de la Unidad Ing. Milton Palacios

4. Valoración amenazas / activo

***Nota: La información, resultado de la entrevisa, fue omitida por ser CONFIDENCIAL y propiedad de la Unidad de Telecomunicaciones e Información de la Univerdad Nacional de Loja.**

ANEXO 9: Gráficas de impacto acumulado actual y potencial

IMPACTO ACUMULADO ACTUAL

FIGURA CONFINDENCIAL

Figura 22: Impacto actual Sección de Desarrollo de Software

FIGURA CONFINDENCIAL

Figura 23: Impacto actual Sección de Desarrollo de Mantenimiento Electrónico

FIGURA CONFINDENCIAL

Figura 24: Impacto actual Sección de Redes y Equipos Informáticos- Sección de Telecomunicaciones

FIGURA CONFINDENCIAL

Figura 25: Impacto potencial Sección de Desarrollo de Software

Figura 26: Impacto potencial Sección de Desarrollo de Mantenimiento Electrónico

Figura 27: Impacto potencial Sección de Redes y Equipos Informáticos- Sección de Telecomunicaciones

Nota: Las gráficas, resultado del análisis del impacto, fueron omitida por ser CONFIDENCIALES y propiedad de la Unidad de Telecomunicaciones e Información de la Univerdad Nacional de Loja.

ANEXO 10: Gráficas de riesgo acumulado actual y potencial

Figura 28: Riesgo actual Sección de Desarrollo de Software

Figura 29: Riesgo actual Sección de Desarrollo de Mantenimiento Electrónico

Figura 30: Riesgo actual Sección de Redes y Equipos Informáticos- Sección de Telecomunicaciones

Figura 31: Riesgo potencial Sección de Desarrollo de Mantenimiento Electrónico

FIGURA CONFINDENCIAL

Figura 32: Riesgo potencial Sección de Redes y Equipos Informáticos- Sección de Telecomunicaciones

Nota: Las gráficas, resultado del análisis de riesgo, fueron omitida por ser CONFIDENCIALES y propiedad de la Unidad de Telecomunicaciones e Información de la Univerdad Nacional de Loja.

ANEXO 11: Tabla de valoración de Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001.

TABLA XXXVIII. Valoración de Mecanismos de control del Anexo A de la Norma ISO/IEC 27001:2005

N°		Dominio - Control	#Ctrls
A5	**Política de seguridad de la información**		**2**
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.		
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.	
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.	
A6	**Organización de la seguridad de la información**		**11**
	Gestionar la organización de la seguridad de información.		
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.	
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.	1
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.	1
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).	
A.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.	
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.	
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.	1
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.	
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.	
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.	
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad , que abarcan los requerimientos de SI relevantes.	1

A7	**Gestión de activos de información (AI)**		**5**
	Lograr y mantener la protección apropiada de los activos de información		
A.7.1.1	Responsabilidad por los activos	Se mantiene un inventario de AI.	
A.7.1.2		Todo AI tiene asignado un responsable (propietario).	
A.7.1.3		Se dispone de una normativa de uso de los AI	
A.7.2.1	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad	
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.	
A8	**Seguridad de los recursos humanos**		**9**
	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y asi reducir el riesgo de robo, fraude o mal uso de los activos de información.		
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidadesde de SI, de todo el personal.	1
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.	1
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.	1
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.	1
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.	1
A.8.2.3		Se tiene establecido un procesos disciplinario ante el incumplimiento de SI.	1
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.	1
A.8.3.2		Se procura la entrega de activos al témino de contrato.	1
A.8.3.3		Se retira los derechos de acceso al término del contrato.	1
A9	**Seguridad física y medioambiental**		**13**
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.		
A.9.1.1	Áreas seguras	Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.	
A.9.1.2		Se utiliza mecanismos de control de acceso en entradas críticas.	
A.9.1.3		Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.	
A.9.1.4		Se utiliza mecanismos de protección ante amenzas externas y ambientales.	
A.9.1.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.	
A.9.1.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).	
A.9.2.1	Seguridad del equipo	Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.	
A.9.2.2		Los equipos están protegidos frente a fallas de servicios públicos.	
A.9.2.3		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.	
A.9.2.4		Los equipos son mantenidos en forma periódica.	
A.9.2.5		Se aplica seguridad a los equipos fuera del local	
A.9.2.6		Antes de dar de baja un equipo se elimina la información	
A.9.2.7		Todo equipo requiere autorización para ser retirado de la Institución	

A10	Gestión de operaciones y comunicaciones		32
	Asegurar la operación correcta y segura de los activos de información.		
A.10.1.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados y disponible a los usuarios.	
A.10.1.2		Gestión del control de cambios en los recursos de procesamiento de información.	
A.10.1.3		Segregación de responsabilidades para reducir el mal uso de los activos.	1
A.10.1.4		Separaración de los recursos de desarrollo, prueba y producción.	
A.10.2.1	Gestión de la entrega de servicios de terceros	Procurar que los terceros implementen, operen y mantengan los controles de seguridad.	
A.10.2.2		Monitoreo y auditoría regular de los servicios e informes de terceros.	
A.10.2.3		Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio asi como procesos involucrados y la evaluacion de riesgos.	
A.10.3.1	Planeación y aceptación del sistema	Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.	
A.10.3.2		Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.	1
A.10.4.1	Protección contra software malicioso y código móvil	Implementar controles de prevención, detección y recuperación ante software malicioso, asi como controles adecuados para la toma de conciencia.	
A.10.4.2		Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.	1
A.10.5.1	Copias de respaldo (back-up)	Se realiza copias de respaldo de información y software, y se prueba regularmente.	
A.10.6.1	Gestión de seguridad de redes	Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.	
A.10.6.2		Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red estan identificados e incluido en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratos.	
A.10.7.1	Gestión de medios (activos de almacenamiento)	Se dispone de procedimientos para la gestión de medios removibles.	1
A.10.7.2		Se dispone de procedimientos formales para la eliminación de medios.	1
A.10.7.3		Se dispone de procedimientos para el manejo de información de manera confidencial.	
A.10.7.4		La documentación de los sistemas es protegida del acceso no autorizado.	
A.10.8.1	Intercambio de información (transferencia)	Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.	
A.10.8.2		Se firma acuerdos para el intercambio de información y software con entidades externas	1
A.10.8.3		Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.	
A.10.8.4		Se protege adecuadamente la información involucrada en los mensajes electrónicos.	
A.10.8.5		Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.	

A.10.9.1	Servicios de comercio electrónico	Se protege la información de comercio electrónico que se trasmite en redes públicas, contra actividades fraudulentas, litigios contractuales y divulgación o modificación.	1
A.10.9.2		Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad.	1
A.10.9.3		Se protege la integridad de la información disponible públicamente.	1
A.10.10.1	Monitoreo (de actividades no autorizadas)	Se registra pistas de auditoria, excepciones y eventos de seguridad.	1
A.10.10.2		Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.	
A.10.10.3		Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.	
A.10.10.4		Se registra las actividades del administrador y operador del sistema.	
A.10.10.5		Se registran las fallas, se analizan y se toma la acción apropiada.	
A.10.10.6		Los relojes de los sistemas de procesamiento de información se mantienen sincronizados.	1
A11	**Control de acceso (lógico)**		**25**
	Controlar el acceso lógico a los activos de información		
A.11.1.1	Requerimientos	Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.	1
A.11.2.1	Gestión de acceso de usuarios	Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.	
A.11.2.2		Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.	
A.11.2.3		Se dispone de procedimiento para la gestión de contraseñas.	
A.11.2.4		Se audita los derechos de acceso de manera regular.	1
A.11.3.1	Responsabilidades de usuarios	Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.	
A.11.3.2		Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.	
A.11.3.3		Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.	

A.11.4.1	Control de acceso a la red	Los usuarios solo tienen acceso a los servicios que están autorizados.	
A.11.4.2		Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.	
A.11.4.3		La identificación del equipo forma parte de la autenticación.	
A.11.4.4		Se controla el acceso para el diagnóstico y configuración de puertos.	1
A.11.4.5		Se segrega en la red, los usuarios y sistemas de información.	
A.11.4.6		Se restringe la capacidad de conexión de usuarios a redes compartidas.	
A.11.4.7		La red se configura de modo que no se infrinja los controles de acceso.	
A.11.5.1	Control de acceso al sistema operativo	Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).	
A.11.5.2		Todo usuario dispone de una cuenta de acceso única.	
A.11.5.3		El sistema de gestión de claves asegura su calidad.	1
A.11.5.4		Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema.	
A.11.5.5		Las sesiones inactivas se cierran luego de un tiempo de inactividad.	1
A.11.5.6		Se restringe el horario de acceso a las aplicaciones de alto riesgo.	1
A.11.6.1	Control de acceso a las aplicaciones e información	Se restringe el acceso a los usuarios y al personal de TI.	1
A.11.6.2		Los sistemas sensibles están en un ambiente aislado.	1
A.11.7.1	Computación móvil y teletrabajo	Se dispone de política de protección de equipos móviles.	1
A.11.7.2		Se dispone de política y procedimiento para teletrabajo.	1
A12	**Adquisición, desarrollo y mantenimiento de sistemas de información**		**16**
	Procurar que la seguridad sea una parte integral de los sitemas de información.		
A.12.1.1	Requerimientos de seguridad de los sistemas	**Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.**	
A.12.2.1	Procesamiento correcto en las aplicaciones	**Se validan los datos de entrada a las aplicaciones para asegurar que esta sea correcta y apropiada.**	
A.12.2.2		**Se incorpora mecanismos de validación en las aplicaciones para detectar corrupción de la información.**	
A.12.2.3		Se identifican los requisitos para asegurar la autenticidad e integridad de los mensajes en las aplicaciones.	1
A.12.2.4		**Se valida la data de salida de las aplicaciones.**	

A.12.3.1	Controles criptografícos	Se dispone de una política de uso de controles criptografícos para proteger la información.	1
A.12.3.2		Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas.	1
A.12.4.1	Seguridad de los archivos del sistema	Se dispone de procedimientos para la instalación del software de los sistemas.	1
A.12.4.2		Se selecciona, protege y controla los datos de prueba del sistema.	1
A.12.4.3		**Se controla el acceso al código fuente del sistema.**	
A.12.5.1	Seguridad en los procesos de desarrollo y soporte	Los cambios se controlan mediante el uso de procedimientos de control de cambios.	1
A.12.5.2		**Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo, para observar el impacto generado.**	
A.12.5.3		Se limita a los cambios necesarios (no se fomenta las modificaciones a los paquetes).	1
A.12.5.4		Se procura evitar las fugas o filtraciones de información.	1
A.12.5.5		Se supervisa y monitorea el desarrollo tercerizado de software.	1
A.12.6.1	Gestión de vulnerabilidades técnicas	Se procura minimizar la explotación de vulnerabilidades de los sistemas.	1
A13	**Gestión de incidentes de seguridad de información**		**5**
	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva oportuna.		
A.13.1.1	Reporte de incidentes y debilidades	Los incidentes de SI se reportan por los canales apropiados tan rápido como sea posible.	
A.13.1.2		Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.	
A.13.2.1	Gestión de incidentes y mejoras	Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.	
A.13.2.2		Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de SI.	1
A.13.2.3		Se recolecta y mantiene evidencias (para fines de auditoría).	
A14	**Gestión de continuidad de operaciones**		**5**
	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativas o desastres, y asegurar su reanudación oportuna.		
A.14.1.1	Gestión de la continuidad operativa	Se dispone de un proceso de gestión de continuidad de operaciones.	
A.14.1.2		Se realiza gestión de riesgos.	
A.14.1.3		Se dispone de un Plan de Continuidad de Operaciones (PCO).	
A.14.1.4		Se maneja un único marco referencial de PCO.	1
A.14.1.5		El PCO se prueba y actualiza en forma regular.	1

A15	**Cumplimiento regulatorio**		**10**
	Evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamentao o contractuales, y de cualquier requisito de seguridad.		
A.15.1.1	Con los requerimientos legales	Se ha definido, documentado y mantiene actualizado todos los requisitos legales, reglamentarios, contractuales pertinentes.	1
A.15.1.2		Se dispone de procedimientos para respetar la propiedad intelectual.	1
A.15.1.3		Se protege los registros importantes de la organización.	1
A.15.1.4		Se protege la privacidad de la información personal, según la regulaciones.	1
A.15.1.5		Se sensibiliza al personal para evitar usos no autorizados.	1
A.15.1.6		Se hace uso de cifrado, según las regulaciones.	1
A.15.2.1	Con las políticas y estándares de S.I.	Se procura el cumplimiento de los procedimientos de SI.	1
A.15.2.2		Se procura el cumplimiento de la normativa de SI en los sistemas de información.	1
A.15.3.1	Auditoría de los sistemas de información	Se planifica las auditorías internas de sistemas de información.	1
A.15.3.2		Se protege el acceso a las herramientas de auditoría de sistemas de información.	1
			133

ANEXO 12: Certificación para el desarrollo del proyecto.

Loja, 09 de diciembre de 2013

Conscientes de la necesidad de la implementación de un **Sistema de Gestión de Seguridad de la Información** en la Unidad de Telecomunicaciones e Información, certificamos que el proyecto ***"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001"*** planteado por la aspirante **Pardo Cuenca María Gabriela** con cédula de identidad 1104616576 , egresada de la carrera de Ingeniería en Sistemas, es parte constitutiva y fundamental para solventar dicha necesidad.

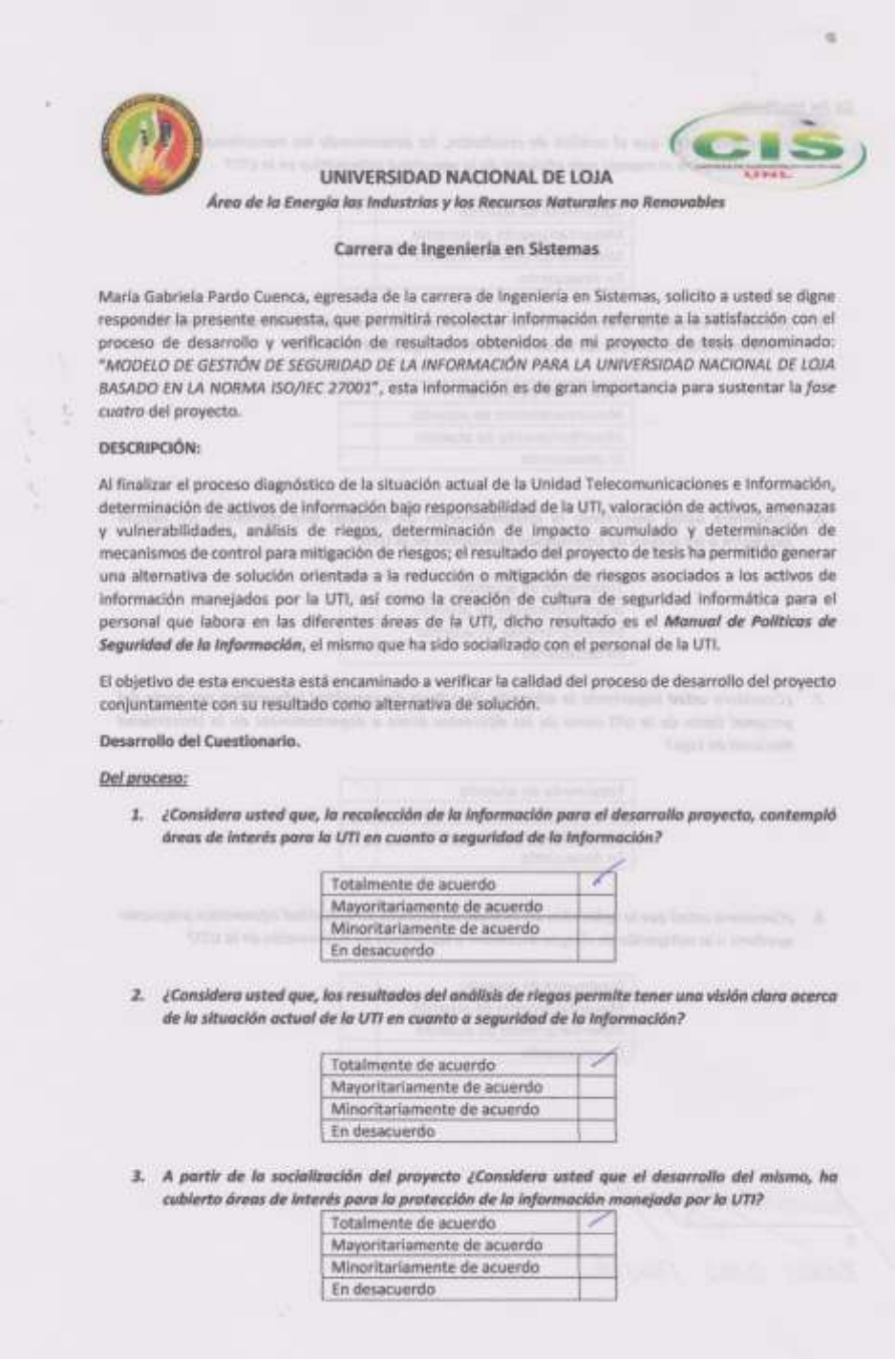
Para constancia de lo mismo adjunto firmo:

Ing. Milton Labanda
Técnico de la UTI

Figura 33: Certificación para desarrollo del Proyecto de Tesis

ANEXO 13: Manual de Políticas de Seguridad de la Información para la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

ANEXO 14: Encuesta de resultados del proyecto de tesis al personal de la UTI.



UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Sistemas

María Gabriela Pardo Cuenca, egresada de la carrera de Ingeniería en Sistemas, solicito a usted se digne responder la presente encuesta, que permitirá recolectar información referente a la satisfacción con el proceso de desarrollo y verificación de resultados obtenidos de mi proyecto de tesis denominado: *"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001"*, esta información es de gran importancia para sustentar la *fase cuatro* del proyecto.

DESCRIPCIÓN:

Al finalizar el proceso diagnóstico de la situación actual de la Unidad Telecomunicaciones e Información, determinación de activos de información bajo responsabilidad de la UTI, valoración de activos, amenazas y vulnerabilidades, análisis de riegos, determinación de impacto acumulado y determinación de mecanismos de control para mitigación de riesgos; el resultado del proyecto de tesis ha permitido generar una alternativa de solución orientada a la reducción o mitigación de riesgos asociados a los activos de información manejados por la UTI, así como la creación de cultura de seguridad informática para el personal que labora en las diferentes áreas de la UTI, dicho resultado es el ***Manual de Políticas de Seguridad de la Información***, el mismo que ha sido socializado con el personal de la UTI.

El objetivo de esta encuesta está encaminado a verificar la calidad del proceso de desarrollo del proyecto conjuntamente con su resultado como alternativa de solución.

Desarrollo del Cuestionario.

Del proceso:

1. ***¿Considera usted que, la recolección de la información para el desarrollo proyecto, contempló áreas de interés para la UTI en cuanto a seguridad de la información?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

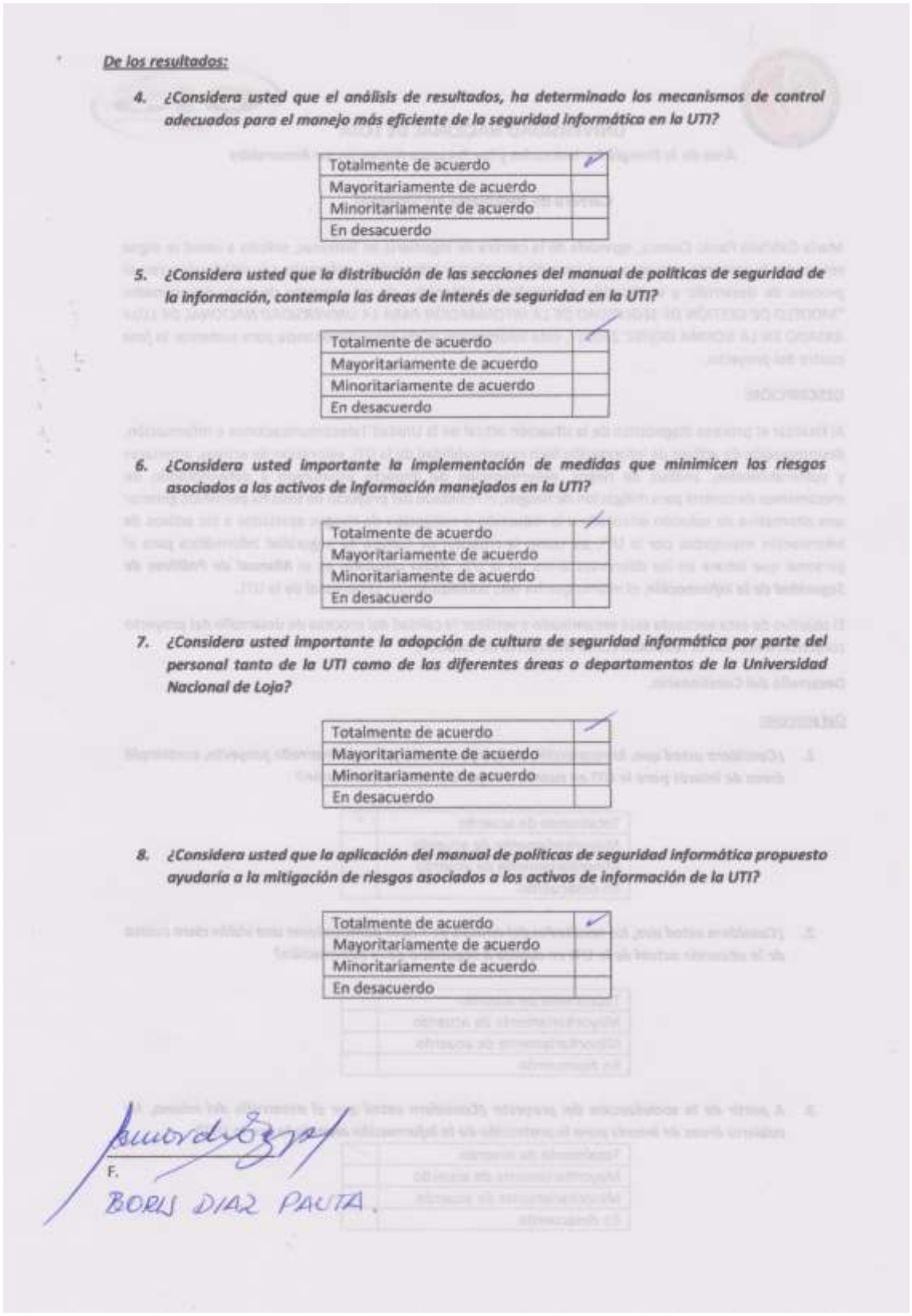
2. ***¿Considera usted que, los resultados del análisis de riegos permite tener una visión clara acerca de la situación actual de la UTI en cuanto a seguridad de la información?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

3. ***A partir de la socialización del proyecto ¿Considera usted que el desarrollo del mismo, ha cubierto áreas de interés para la protección de la información manejada por la UTI?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

Figura 34: Encuesta de satisfacción para el personal de la UTI (pag.1)



De los resultados:

4. ***¿Considera usted que el análisis de resultados, ha determinado los mecanismos de control adecuados para el manejo más eficiente de la seguridad informática en la UTI?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

5. ***¿Considera usted que la distribución de las secciones del manual de políticas de seguridad de la información, contempla las áreas de interés de seguridad en la UTI?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

6. ***¿Considera usted importante la implementación de medidas que minimicen los riesgos asociados a los activos de información manejados en la UTI?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

7. ***¿Considera usted importante la adopción de cultura de seguridad informática por parte del personal tanto de la UTI como de los diferentes áreas o departamentos de la Universidad Nacional de Loja?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

8. ***¿Considera usted que la aplicación del manual de políticas de seguridad informática propuesto ayudaría a la mitigación de riesgos asociados a los activos de información de la UTI?***

Totalmente de acuerdo	✓
Mayoritariamente de acuerdo	
Minoritariamente de acuerdo	
En desacuerdo	

F.

BORIS DIAZ PAUTA.

Figura 35: Encuesta de satisfacción para el personal de la UTI (pag.2)

ANEXO 15: Certificado de conformidad con el proyecto emitido por la Dirección de la UTI.

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD DE TELECOMUNICACIONES E NFORMACIÓN

Ing. Milton Ricardo Palacios Morocho
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

CERTIFICA.

Que la Srta. Egresada María Gabriela Pardo Cuenca, con ced. 1104616576, cuyo proyecto de titulación versa sobre el tema *"MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE LOJA BASADO EN LA NORMA ISO/IEC 27001"*, ha culminado con éxito el desarrollo de dicho proyecto, incluyendo la socialización con el Director y Responsables de la Unidad de Telecomunicaciones e Información, el día 12 de febrero de 2015, donde se ha dado por validada la información procesada y los resultados obtenidos, incluyendo en ello la propuesta del **Manual de Políticas de Seguridad de la Información para la Unidad de Telecomunicaciones e Información**, el cual fue elaborado a partir de las necesidades de seguridad de la información, análisis de riesgos de activos de información y resultados obtenidos en el desarrollo del proyecto.

LO CERTIFICO, para los fines pertinentes.

Loja, 25 de febrero de 2015

Ing. Milton Ricardo Palacios Morocho
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN.

CIUDAD UNIVERSITARIA "GUILLERMO FALCONÍ ESPINOSA" La Argelia, Loja-Ecuador
PBX: (593 07 2) 547252 Casilla: Letra "S" E-mail: telecomunicaciones@unl.edu.ec Sitio Web: www.unl.edu.ec

Figura 36: Certificado de Conformidad con los resultados obtenidos en el proyecto por parte de la Dirección de la Unidad de Telecomunicaciones e Información.

ANEXO 16: Tabla comparativa entre UNE 71502:2004 e ISO 27001:2005

Tabla comparativa entre UNE 71502:2004 e ISO/IEC 27001:2005

	UNE 71502:2004	ISO/IEC 27001:2005
Título	Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)	Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos
Editada por	AENOR	ISO / IEC
Fecha de publicación	Febrero de 2004	Octubre de 2005
Idioma	Español	Inglés
Ámbito	Español	Internacional
Elaborada por	AEN/CTN 71	ISO/IEC JTC 1 SC 27
Nº de páginas	12 (+ 4 de anexos)	12 (+ 30 de anexos)
Equivalencia de apartados y cláusulas		Prólogo
		0. Introducción
		0.1 Generalidades
		0.2 Enfoque por procesos
		0.3 Compatibilidad con otros sistemas de gestión
	1. Objeto y campo de aplicación	1. Alcance
		1.1 Generalidades
		1.2 Aplicación
	2. Normas para consulta	2. Referencias normativas
	3. Términos y definiciones	3. Términos y definiciones
	4. Marco general del SGSI	4. SGSI
	4.1 Requisitos generales	4.1 Requisitos generales
	4.2 Planificación y diseño del SGSI	4.2 Establecer y gestionar el SGSI
		4.2.1 Establecer el SGSI
	(5. Implantación del SGSI)	4.2.2 Implantar y utilizar el SGSI
		4.2.3 Monitorizar y revisar el SGSI
		4.2.4 Mantener y mejorar el SGSI
	4.3 Selección de controles	(4.2.1 Establecer el SGSI)
	4.4 Documentación	4.3 Requisitos de documentación
		4.3.1 Generalidades
	4.5 Control documental	4.3.2 Control de documentos
	4.6 Registros	4.3.3 Control de registros
	4.7 Responsabilidad de la Dirección	5. Responsabilidad de la Dirección
	4.7.1 Compromiso de la Dirección	5.1 Compromiso de la Dirección
	4.7.2 Política de seguridad de la Organización	(4.2.1 Establecer el SGSI)
	5. Implantación del SGSI	(4.2.2 Implantar y utilizar el SGSI)
	5.1 Implantación de los controles	
	5.2 Eficacia de los controles	
	6. Explotación	
	6.1 Gestión de los recursos	5.2 Gestión de los recursos
	6.1.1 Provisión de recursos	5.2.1 Provisión de recursos
	6.1.2 Recursos humanos	5.2.2 Formación, toma de conciencia y competencia
	6.1.2.1 Generalidades	
	6.1.2.2 Competencia, toma de conciencia y formación	
	(7.2 Auditorías internas)	6. Auditorías internas del SGSI
	7. Revisión del SGSI	7. Revisión del SGSI por la Dirección
	7.1 Generalidades	7.1 Generalidades
		7.2 Entradas de la revisión
		7.3 Salidas de la revisión
	7.2 Auditorías internas	(6. Auditorías internas del SGSI)
	8. Proceso de mejora	8. Mejora del SGSI
	8.1 Mejora continua	8.1 Mejora continua
	8.2 Acción correctiva	8.2 Acción correctiva
	8.3 Acción preventiva	8.3 Acción preventiva
	9. Bibliografía	Bibliografía
	Anexo A. Relación de procedimientos para establecer un SGSI	Anexo A. Objetivos de control y controles
		Anexo B. Principios de la OCDE
		Anexo C. Correspondencia con ISO 9001:2000, ISO 14001:2004

Figura 37: Comparativa entre UNE 71502:2004 e ISO/IEC 27001:2005

ANEXO 17: Certificación Traducción Summary

Loja, martes 3 de marzo de 2015

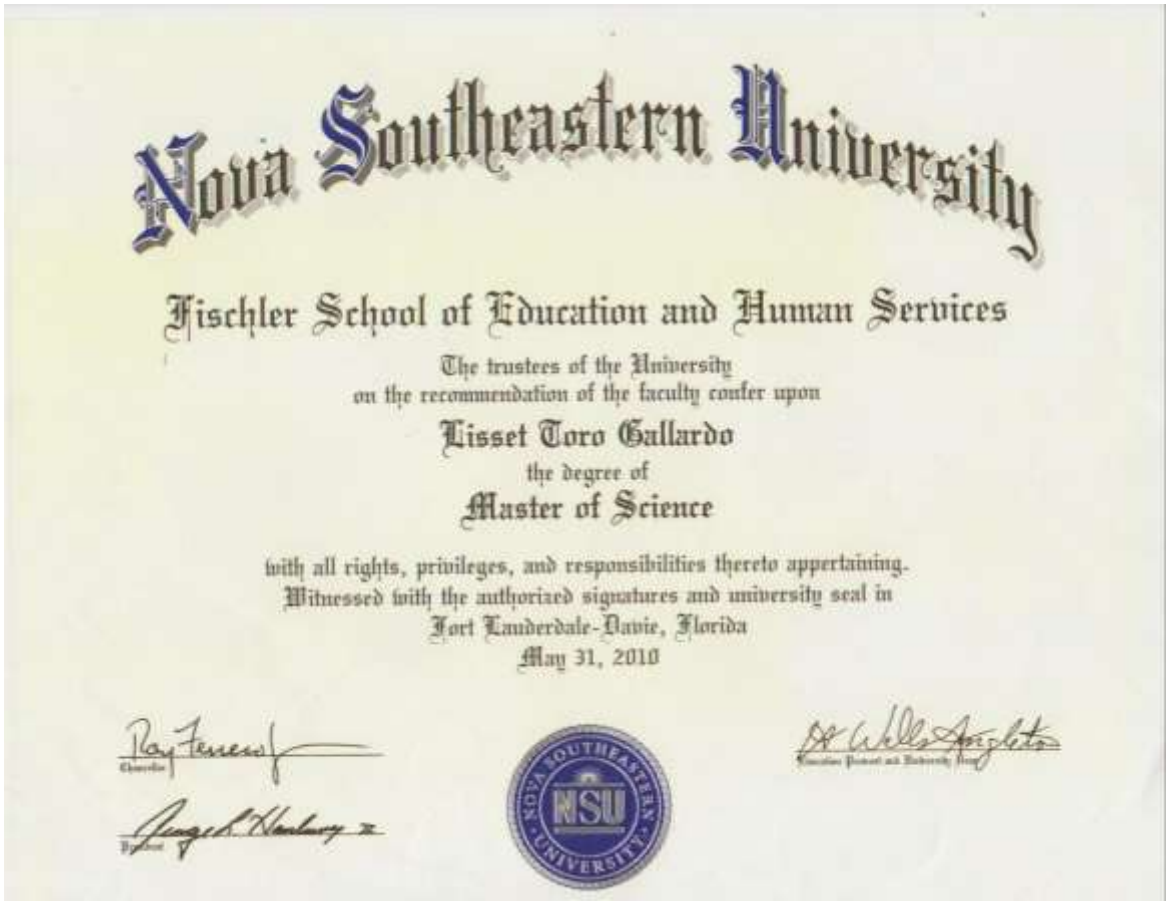
Ciudad

Yo, Lisset Vanessa Toro Gallardo, con cédula N. 1104074842 con estudios de posgrado en la enseñanza del idioma inglés en NOVA Southeastern University respaldo que el resumen del trabajo de titulación es fiel traducción de su original en español por lo que su contenido puede ser interpretado de forma correcta.

Por su atención le expreso mi agradecimiento

Atentamente,

Mgs. L. Vanessa Toro Gallardo



Nova Southeastern University

Fischler School of Education and Human Services

The trustees of the University
on the recommendation of the faculty confer upon

Lisset Toro Gallardo

the degree of

Master of Science

with all rights, privileges, and responsibilities thereto appertaining.
Witnessed with the authorized signatures and university seal in
Fort Lauderdale-Davie, Florida
May 31, 2010

ANEXO 18: ARTÍCULO CIENTÍFICO

ANEXO 19: LICENCIA CREATIVE COMMONS