SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO

YEZID CAMILO GUERRERO ANGULO
ROBERT MARCELO TABANGO GOYES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2014

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO

YEZID CAMILO GUERRERO ANGULO
ROBERT MARCELO TABANGO GOYES

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Director:
I.S. Esp. FRANCISCO SOLARTE SOLARTE

Co-Director:
I.S. Mg. MANUEL ERNESTO BOLAÑOS

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2014

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en el trabajo de grado, son responsabilidad exclusiva de los autores”.

Artículo primero del acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Acadèmico.

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma del Director de Tesis

_____
Firma del Jurado

_____
Firma del Jurado

San juan de Pasto, Octubre de 2014

AGRADECIMIENTOS

En primer lugar a Dios, por habernos guiado por el camino correcto durante estos años de estudio, darnos salud e iluminar nuestras mentes en esos difíciles momentosy por ponernos en la vida a cada una de esas personas incondicionales que contribuyeron al desarrollo de este proyecto.

Agradecer hoy y siempre a nuestros padres y familiares cercanos por el apoyo brindado y por sus consejos diarios que nos dan fortaleza para continuar formándonos integralmente día y día.

Un agradecimiento especial al Ingeniero Francisco Nicolás Solarte Solarte, director del proyecto, por su colaboración y disposición en el desarrollo de este trabajo, ya que por medio de su orientación, fue posible la consecución de cada uno de los objetivos propuestos y culminación de la investigación.

Y por último, al coordinador y a los administradores de la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño por su cooperación y suministro de información, fundamental para cada una de las fases del proyecto.

DEDICATORIA

Dedicamos este trabajo de grado a Dios que nos ha dado la vida y fortaleza para culminarlo. A nuestros padres quienes han velado por nuestro bienestar y educación, siendo apoyo incondicional en todo momento, y demás familiares por su ayuda y constante cooperación en el transcurso de nuestra carrera.

RESUMEN

Hoy en día la universidad cuenta con una módulo que está al frente de los servicios de administración de Red de Datos e internet, administración de Bases de Datos y Servidores, administración del Portal Web Universitario, servicios académicos y servicio de mantenimiento de quipos de cómputo. Dicha unidad es la Unidad de Informática y Telecomunicaciones (UIT), que es un organismo que depende de la Vicerrectoría Académica (ver figura 1), constituida como un laboratorio donde se desarrollan las actividades académicas de la Universidad que tienen que ver con la informática, la ingeniería de sistemas y las telecomunicaciones.

ABSTRACT

Today the university has a module that is leading management services Data Network and Internet, Management Databases and Servers, Web Portal Administration Degree, academic services and maintenance service quipos computer . This unit is the unit of Information Technology and Telecommunications (ITU) , which is an agency under the Academic Vice (see Figure 1) , incorporated as a laboratory where the academic activities of the University having to do with computers develop, systems engineering and telecommunications.

CONTENIDO

Pág.

INTRODUCCIÓN 14
1. MARCO DE REFERENCIA 18
1.1 ANTECEDENTES DE INVESTIGACIÓN 18
1.2 MARCO CONTEXTUAL 19
1.2.1 Estructura organizacional. 21
1.2.2 Funciones personal UIT: 34
1.3 MARCO TEÓRICO 40
1.4 MARCO LEGAL 59
1.5 MARCO CONCEPTUAL 62
2. METODOLOGÍA APLICADA 66
2.1 APOYO DE LA DIRECCIÓN 66
2.2 PLAN DE RECOLECCIÓN DE INFORMACIÓN 66
2.3 ANÁLISIS Y EVALUACIÓN DE RIESGOS 67
2.3.1 Definición y valoración de activos de información. 68
2.3.2 Identificación de amenazas a que están expuestos los activos de información. 68
2.3.3 Identificación de vulnerabilidades existentes para los activos de i nformación. 68
2.3.4 Estimación del impacto. 68
2.3.5 Estimación de la probabilidad. 68
2.3.6 Estimación del riesgo. 68
2.4 ANÁLISIS DE BRECHA 69
2.5 GESTIÓN DE RIESGOS 69
2.5.1 Plan de tratamiento de riesgos. 69
2.5.2 Establecer normativa para controlar el riesgo. 69
2.5.3 Plan de implementación. 70

3. CONCLUSIONES.....71
4. RECOMENDACIONES 72
BIBLIOGRAFÍA.....73
NETGRAFIA 74
ANEXOS.....76

LISTA DE FIGURAS

Pág.

Figura 1. Estructura orgánica - Universidad de Nariño 20
Figura 2. Estructura organizacional de la Unidad de Informática y Telecomunicaciones 22
Figura 3. Infraestructura Red de Datos e Internet de la Universidad de Nariño y municipios 27
Figura 4. Configuración principal red de datos sede principal Torobajo.....29
Figura 5. Dominios ISO 27002 44
Figura 6. Ciclo PHVA 49

LISTA DE TABLAS

Pág.

Tabla 1. Servidores alojados en la UIT 24
Tabla 2. Funciones – Coordinador aula de informática.....34
Tabla 3. Funciones – Administrador soporte y servicios tecnológicos 35
Tabla 4. Funciones – Administrador de red de datos e internet.....36
Tabla 5. Funciones - Administrador de sistemas 38
Tabla 6. Funciones – Administrador portal web 39
Tabla 7. Escala nivel de madurez COBIT 51
Tabla 8. Tipo de amenazas MAGERIT 55
Tabla 9. Tipos de activos 56
Tabla 10. Dimensiones de valoración de un activo.....56
Tabla 11. Valoración cualitativa 56
Tabla 12. Valoración cuantitativa 56
Tabla 13. Estimación del impacto 57
Tabla 14. Estimación de la probabilidad 57
Tabla 15. Tipo de amenazas MAGERIT 67
Tabla 16. Amenazas MAGERIT.....67
Tabla 17. Mapa de riesgos.....67

LISTA DE ANEXOS

Pág.

Anexo A. Inventario activos de información....78
Anexo B. Análisis y evaluación de riesgos....79
Anexo C. Ethical hacking....80
Anexo D. Entrevistas estructuradas....81
Anexo E. Verificación controles ISO 27002....82
Anexo F. Fotografías....83
Anexo G. Análisis de brecha....84
Anexo H. Plan de tratamiento de riesgos....85
Anexo I. Políticas de seguridad de la información....86
Anexo J. Plantillas y tablas....87
Anexo K. Plan para la implementación del SGSI....88

INTRODUCCIÓN

Cada día las instituciones de educación superior reconocen la importancia de la información como uno de los activos más significativos que debe ser manejado eficientemente, para garantizar ventajas dentro del campo administrativo y académico, por lo cual las instituciones incrementan su inversión en el uso de diferentes tecnologías tales como páginas web informativas, tecnologías de identificación por lector de huellas dactilares, llaves de hardware que permiten verificar identidades y otras herramientas como sistemas de alertas, cifrado de datos, etc.

Una de las tecnologías para el manejo de la información es los sistemas de información web, tales como portales web y sitios web que facilitan la interacción entre los usuarios y los servicios que pueden prestarse a través de ellos.

Es claro que en este contexto, el objetivo es el de proteger la información contra ataques internos y externos ya sean sabotajes informáticos para causar daños al hardware o al software del sistema. Este tipo de amenazas y vulnerabilidades pueden causar daños en la infraestructura física o en la información de varias formas, que van desde las más simples como desconectar el computador de la electricidad mientras se está trabajando, hasta las más complejas como el uso de programas lógicos destructivos, o el uso de los virus informáticos.

Hoy en día ninguna organización está exenta de esta clase de vulnerabilidades, amenazas o ataques, que deben ser detectados a tiempo para así diseñar una serie de controles que las contrarresten, para lograrlo se han creado diferentes normas, entre las cuales existe la norma ISO/IEC 27000 que proporcionan un marco de gestión de la seguridad de la información que puede adaptarse por cualquier organización pública o privada, grande o pequeña. En el proyecto se hizo uso de las normas ISO/IEC 27001:2005 de activos de información e ISO/IEC 27002:2005 de controles de seguridad.

Impulsados en lo anterior, se presenta un proyecto enfocado en un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, ya que la información es un factor clave de éxito y por lo tanto, su eficiente administración garantiza altos estándares de calidad y productividad.

El desarrollo de este proyecto implicó la definición de los activos que necesitan protegerse para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, junto con los riesgos, vulnerabilidades, amenazas y controles existentes para cada uno de ellos. Una vez hecho esto, se procedió a definir

nuevos controles necesarios para cada uno de los activos, y como resultado se obtuvo un sistema de gestión de seguridad de la información (SGSI), ajustado a las necesidades actuales y que permita gestionar de manera eficiente la información para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, asegurando la integridad, confidencialidad y disponibilidad de la misma y con esto la mejora continua de la institución.

PLANTEAMIENTO DEL PROBLEMA

Las universidades realizan en sus actividades diarias procesos de todo tipo, en los cuales la información juega el papel principal; el manejo de la información confidencial, integral y disponible es factor clave de éxito, por lo tanto, su eficiente gestión garantiza altos estándares de calidad y productividad.

Actualmente la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño no cuenta con un Sistema de Gestión de Seguridad de la Información integral y solamente se vienen implementando controles aislados de acceso físico a la misma, sistemas de cámaras en las aulas y acceso a la información contenida dentro de los sistemas. Algunos de los problemas que se presentan pueden ser de tipo físico tales como acceso no autorizado a datos y recursos informáticos o lógicos como interceptación de correos electrónicos que puede servir no solo para la obtención de información privada e importante, sino también para alterar o eliminar la misma, virus informáticos, entre otros.

Otro problema es la seguridad en las redes donde se han realizado pruebas y no existe ningún tipo de configuración para limitar el acceso en función de usuarios, además de que la clave de acceso a la red inalámbrica es fácilmente detectable y por lo tanto, con solo poseerla y configurar el protocolo de internet, se puede ingresar a la misma y navegar normalmente.

Se han evidenciado problemas en cuanto al ingreso a las aulas sin la debida autorización, ya que solo se cuenta con una asignación de horarios de clase para los docentes que requieran de la utilización de las mismas y en los momentos que se encuentran libres, cualquier persona sin autorización alguna puede ingresar fácilmente y sin una persona que la supervise, realizar algún tipo de acto delictivo en el hardware o en la información.

De continuar con esta situación, se verían afectados las instalaciones físicas, el hardware, los sistemas de información y la información contenida en ellos; lo que perturbaría el normal desarrollo de las actividades dentro de la unidad y la toma de decisiones por parte de sus directivos.

Finalmente, agregar que en la Universidad de Nariño se hace necesario la implementación e implantación de un sistema de seguridad de la información que se vea reflejado en las políticas organizacionales, en la gestión de todos sus

procesos y personal, y en el acceso físico y lógicos de los sistemas de información y datos.

FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de riesgos y la verificación de control de seguridad de la norma ISO 27001 e ISO 27002 pueden mejorar la gestión de la seguridad de la información para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño?

JUSTIFICACIÓN

Si bien es cierto que en muchas ocasiones, las Instituciones de Educación Superior tienen una forma informal de administrar su información, es preciso que se provean mecanismos bien estructurados para que esa administración sea útil, bajo fundamentos teóricos y prácticos. Preferiblemente, el análisis y evaluación de riesgos de seguridad de la información debería convertirse en una política con el fin de garantizar su cumplimiento; lastimosamente, este enfoque no es bien implementado y la información se encuentra dispersa, desorganizada, incompleta y no es confiable.

Los niveles de acceso a la información y los controles de usuario del sistema requieren mejoras ya que en este momento, no se encuentran muy bien definidos por lo que el sistema actual posee ciertas deficiencias, las cuales fueron revisadas y se hicieron las respectivas recomendaciones en cuanto al manejo de usuarios y demás.

El proyecto beneficiará a toda la Universidad de Nariño y ayudará a definir un sistema de control integral de seguridad de la información y de los activos informáticos para la Unidad de Informática y Telecomunicaciones tan fundamental hoy en día para lograr una utilización más eficiente y segura de la información.

También se beneficiaran los administradores y usuarios que hacen uso de los servicios informáticos y de la información que presta la Unidad de Informática y Telecomunicaciones, puesto que tendrán un control apropiado de las actividades y procesos de manejo de la información.

Si los directivos tanto de la Universidad como de la Unidad de Informática y Telecomunicaciones deciden implementar los controles y recomendaciones producto de este trabajo obtendrán ventajas relacionadas con la formalización de tareas y control de que se ejecuten oportuna y adecuadamente, mejora continua en la gestión de la seguridad, protección de los datos, en fin se minimizarían los riesgos en materia de confidencialidad, integridad y disponibilidad de la información.

En vista de la necesidad actual y dado que las Instituciones de Educación Superior de la región no se escapan a esta realidad, el proyecto consistió en la realización de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 e ISO 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, que aporte en el aseguramiento de la información como elemento clave en las actividades diarias y que en un futuro pueda ser replicado a las demás unidades.

OBJETIVOS

Objetivo general

Mejorar la gestión de la seguridad de la información mediante la aplicación del proceso de análisis de riesgos y la verificación de control de seguridad que permita estructurar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño.

Objetivos específicos

- Planear el proceso de recolección de la información de los activos, servicios y procesos que presta la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño a toda la Institución.

- Identificar, analizar y evaluar los riesgos, vulnerabilidades y amenazas presentes en la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño en cuanto a las características de confidencialidad, integridad y disponibilidad de la información.

- Estudiar los controles existentes en cuanto a seguridad de la información de acuerdo al estándar ISO 27002 para hacer un análisis de los controles que deberían implantarse en la unidad de Informática y Telecomunicaciones de la Universidad de Nariño.

- Estructurar el Sistema de Gestión de Seguridad de la Información para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño incluyendo los controles de seguridad en las políticas, procesos y procedimientos.

1. MARCO DE REFERENCIA

1.1 ANTECEDENTES DE INVESTIGACIÓN

Los proyectos sobre el sistema de seguridad de la información son relativamente nuevos, por lo cual no se ha encontrado ninguno en la Universidad de Nariño, y se tomará como referentes otros proyectos a nivel nacional e internacional que servirán de guía para enfocar mejor la investigación.

Dentro de los antecedentes se tomará en cuenta los siguientes:

El proyecto internacional desarrollado por Christian Miguel Cadme Ruiz y Diego Fabian Duque Pozo para la Universidad Politécnica Salesiana – Sede Cuenca (Ecuador) denominado: "AUDITORÍA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA LA EMPRESA DE ALIMENTOS "ITALIMENTOS CÍA. LTDA"[1]. En la empresa "ITALIMENTOS CÍA. LTDA." Existen vulnerabilidades para acceder a cierta información, para ello se ha realizado una auditoria de seguridad informática basada en un estándar internacional ISO 27001, que tiene como objetivo la confidencialidad, disponibilidad e integridad de los datos.

De este proyecto se tomará en cuenta la metodología utilizada para hacer un análisis de riesgos, vulnerabilidades, amenazas y el informe de recomendaciones presentado.

El proyecto desarrollado en la región por parte de José Daniel Guerra y Rafael Llerena, para la Institución Universitaria CESMAG – Sede Pasto, denominado: "DIAGNOSTICO DEL ESTADO DE LOS SGSI CON LA APLICACIÓN DE UN SOFTWARE EN LAS INSTITUCIONES DE EDUCACION SUPERIOR DE SAN JUAN DE PASTO"[2]. En este proyecto se desarrolló un software que evalúa el estado de madurez de los sistemas de gestión de la información, en donde se concluye que solo a nivel regional, la Institución Universitaria CESMAG y la Universidad Mariana, poseen sistemas de seguridad de información implantados que manejan un buen nivel de madurez. Sin embargo, aún existen muchas mejoras a los controles existentes sobre cada área de seguridad de la información.

[1]CADME, Christian y DUQUE, Diego. Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos CÍA. LTDA.". Tesis previa a la obtención del título de Ingeniero de Sistemas. Cuenca. Ecuador: Universidad politécnica salesiana, 2012.

[2]LLERENA, Rafael y GUERRA, José. Diagnóstico del estado de los SGSI con la aplicación de un software en las instituciones de Educación superior de san juan de Pasto. Tesis previa a la obtención del título de Ingeniero de Sistemas. Pasto. Colombia: Institución universitaria CESMAG, 2009.

De este proyecto se tomará como ejemplo los formatos de reportes que arroja el sistema y también se utilizarán los resultados obtenidos en esa época como parte de una base conceptual para dar nuestras respectivas recomendaciones y así se realice la implantación del Sistema de Gestión de Seguridad de la Información por parte de los directivos de laUnidad de Informática y Telecomunicaciones de la Universidad de Nariño**.**

1.2 MARCO CONTEXTUAL

La Universidad de Nariño es un ente universitario autónomo, de carácter oficial del orden departamental, creada mediante decreto No. 049 de noviembre 7 de 1904, con personería jurídica, autonomía académica, administrativa, financiera y patrimonio independiente que elabora y maneja su presupuesto de acuerdo con las funciones que le corresponde.

Los niveles de educación que se ofrecen en la Universidad de Nariño comprenden desde transición hasta último grado de bachillerato, programas de pregrado, diplomados, especializaciones, maestrías y doctorados. Todos sus programas cuentan con registro calificado y varios de ellos con acreditación en alta calidad.

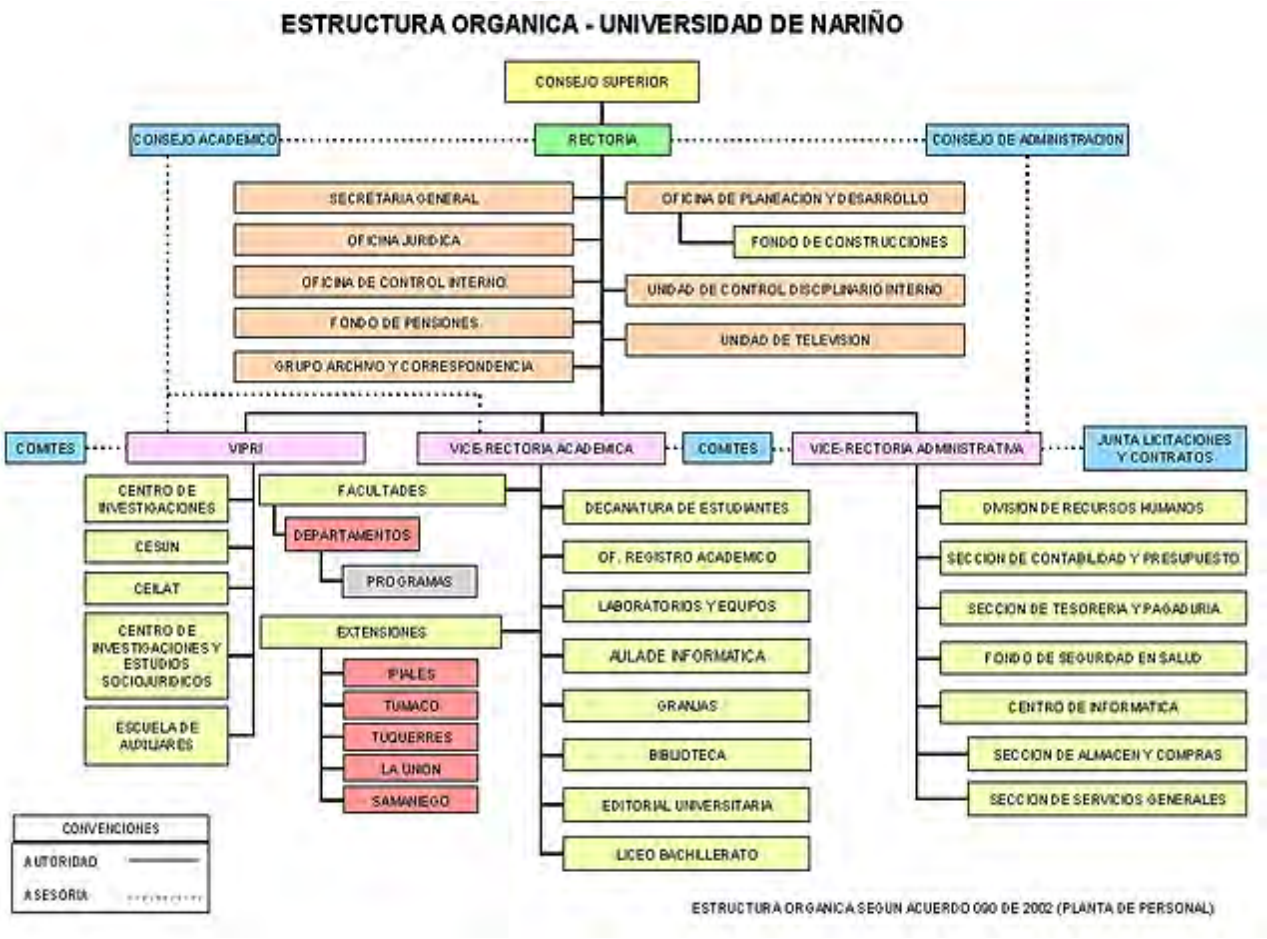
La Universidad de Nariño en el contexto social actual pretende ser una universidad con altos niveles de liderazgo regional y nacional, acreditada en alta calidad, investigativa y comprometida con la región y el país, moderna y eficiente con calidad y calidez humana, democrática y futurista

La Universidad de Nariño, está comprometida con el fomento de una cultura de investigación institucional básica y aplicada con miras a consolidarla como polo de desarrollo regional con impacto nacional e internacional.

Hoy en día la universidad cuenta con una módulo que está al frente de los servicios de administración de Red de Datos e internet, administración de Bases de Datos y Servidores, administración del Portal Web Universitario, servicios académicos y servicio de mantenimiento de quipos de cómputo. Dicha unidad es la Unidad de Informática y Telecomunicaciones (UIT), que es un organismo que depende de la Vicerrectoría Académica (ver figura 1), constituida como un laboratorio donde se desarrollan las actividades académicas de la Universidad que tienen que ver con la informática, la ingeniería de sistemas y las telecomunicaciones.

Asimismo, cuenta con un equipo de trabajo que está facultado para prestar una serie de servicios relacionados con la informática, la ingeniería de sistemas y las telecomunicaciones, en pro de colaborar con el desarrollo de las actividades de la Universidad de Nariño.

Figura 1. Estructura Orgánica - Universidad de Nariño



Fuente: http://www.udenar.edu.co/?page_id=16

Anteriormente esta unidad también desempeñaba funciones de desarrollo de software; que por recomendación del Comité de Sistemas se trasladaron al Centro de Informática.

El alcance de este proyecto, incluye:

- Definición de los activos en la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001.

- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño.

- Verificación de controles de seguridad de la información que se llevan a cabo en la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño teniendo en cuenta la norma ISO 27002.

- Estructuración del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño.

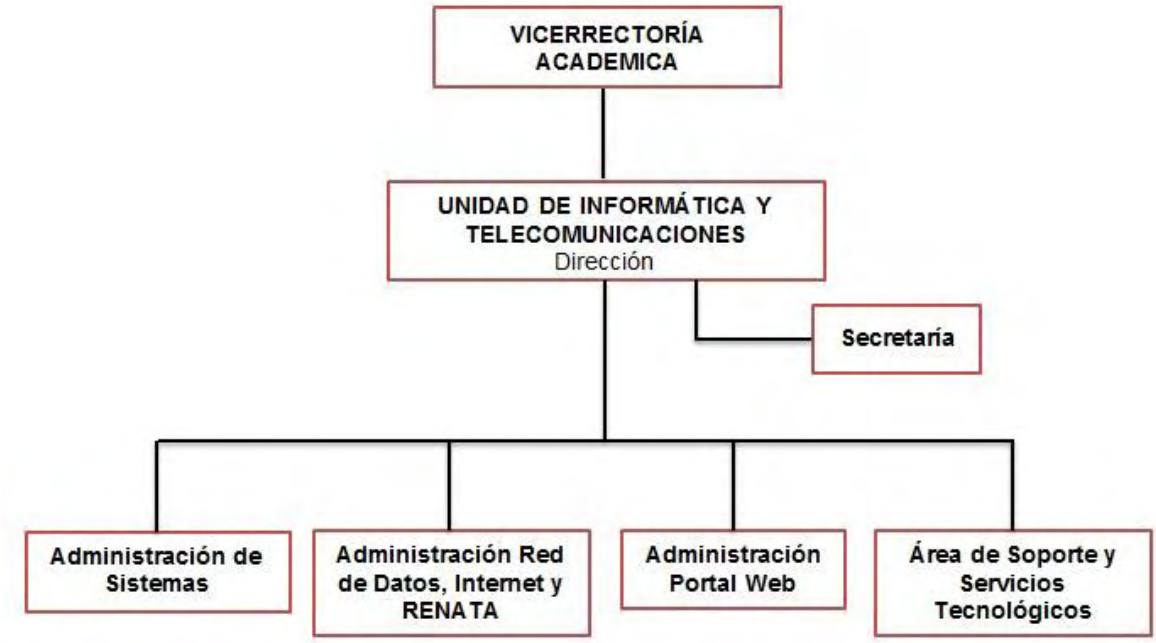
El proyecto contempla el análisis y evaluación de riesgos de seguridad de la información como herramienta clave para la revisión y evaluación de los controles, para lograr una utilización más eficiente y segura de la información.

1.2.1Estructura organizacional."La Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, en la actualidad se encuentra dividida por áreas de acuerdo a las necesidades que diariamente tiene la comunidad universitaria. Así mismo, cada área tiene asignado un determinado número de procesos y procedimientos, los cuales están interrelacionados entre las mismas dependencias para poder cumplir su labor"[3].

En la figura 2 se puede apreciar el esquema jerárquico de la unidad.

[3]UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES. Proyecto UIT. Pasto: Universidad de Nariño, Aula de informática, 2009. [en línea] Disponible en internet. http://uit.udenar.edu.co/. [citado febrero de 2014]

Figura 2. Estructura Organizacional de la Unidad de Informática y Telecomunicaciones



a. Administración de sistemas: El Aula de Informática de la Universidad de Nariño alberga servidores encargados de la administración y alojamiento de las bases de datos Oracle y Postgres principalmente, en donde se mantiene la información académica, también las bases de datos de los sistemas de información académicos y de todos los diferentes sistemas desarrollados como producto de investigación por parte de estudiantes y docentes.

Además de estos servidores, se cuenta con equipos destinados al alojamiento y administración del correo electrónico institucional, un servidor dedicado al control y distribución del canal de Internet de la Universidad (Proxy), un servidor encargado de alojar el portal institucional www.udenar.edu.co , un servidor de correo electrónico para estudiantes y un servidor dedicado al campus virtual UDENAR.

Estos servidores actualmente se encuentran trabajando a su máxima capacidad ya que los requerimientos tecnológicos de la institución crecen en manera exponencial presentando en muchas ocasiones saturación y bajo rendimiento debido a esta alta demanda de servicios.

El Aula de Informática ha adecuado uno de sus espacios para alojar estos servidores como también los sistemas de soporte eléctrico y refrigeración para brindar un lugar de condiciones similares a las adecuadas para este propósito.

En este espacio, también se han alojado servidores de otras dependencias que han sido aceptados por la dependencia para su aseguramiento lógico, y configuración, los cuales son administrados remotamente por sus responsables. Entre estos servidores se encuentran, el servidor de Bases de Datos y Publicación Web del proyecto Megalac de la Universidad de Nariño y COLACTEOS, el servidor del Centro Operador de la Universidad de Nariño COES, administrado por esta dependencia.

Los servidores alojados en el Aula de informática albergan diferentes plataformas y sistemas de información prestos a la parte administrativa y académica de la Universidad de Nariño. Dichos sistemas son desarrollados como trabajos de grado o de acuerdo a las necesidades de las diferentes dependencias, facultades o son adquiridos a los diferentes proveedores de Software.

A continuación, se presenta un listado de los diferentes servidores asociando los sistemas de información y su frecuencia de actualización.

Tabla 1. Servidores alojados en la UIT

NOMBRE DEL SERVIDOR	SISTEMA DE INFORMACIÓN (S.I)	SERVICIO	FRECUENCIA DE ACTUALIZACIÓN
AKANE – Dell PowerEdge R815	Idiomasra: S.I que lo manejan el Centro de Idiomas.	Sistemas basados en Apache: Portal Web Universitario, portales de Dependencias/Programas. Las Bases de Datos en MySQL y Postgresque contienen datos referentes a: Matriculas Centro de Idiomas, Convocatorias, Correspondencia y Sistemas que se manejan en la Universidad de Nariño.	Mensual
	Tusaber5: S.I (Modulo de aprendizaje) que lo maneja el Liceo de la Universidad, producto de un proyecto de grado.		Semestral
	Quejas, sugerencias y reclamos		Semestral
	Inscripciones Liceo: Formulario en el que se registran las personas que desean ingresar al Liceo de la Universidad.		Anual
	Correspondencia: S.I en donde se radican los documentos de archivo y correspondencia.		Anual
	Convocatorias		Semestral
	Herbun: S.I en el que se almacenan las colecciones del herbario de la Universidad de Nariño.		Semestral
SINDAMANOY – Sun V40Z	Interactiva: Moodle de cursos de informática.	Servidor DNS Bind, Servidor Correo Electrónico Postfix, AntiSpamSpamAssassin, Antivirus Amavis, Moodle para los cursos de informática.	Semestral
MAIL – Dell Power Edge R810	Correo Electrónico Institucional	Correo Electrónico institucional Exchange Server 2010.	Al liberar actualizaciones el fabricante
ARTHAS – Sun V40Z	Servicio de Comunicaciones Unificadas junto con Lync server 2010.		Al liberar actualizaciones el fabricante
CONFERENCIAS– Dell PowerEdge 2850	Servicio Livemeeting	Conferencias Live Meeting, office communication server 2007.	Al liberar actualizaciones el fabricante

Continuación tabla 1.

VACUNAS – Proliant ML 110	Antivirus Karspersky Business para los equipos de Tesorería y servidores de la UIT.		Diario
VIRTUAL – HP Proliant DL 380 G5	Zabbix y servicios de prueba, Mysql, Apache Tomcat.		Al liberar actualizaciones el fabricante
JUPITER – Dell PowerEdge 2800	Servidor de Backups, Aloja algunas páginas obsoletas que enlazan con el Portal de la Universidad de Nariño.	Sistemas de información basados en Microsoft Framework 2.0, 3.0 y 3.5., Internet InformationServices.	
ORION – HP Proliant DL 380 G5		DHCP, servidor proxy cache SQUID, servidor de nombres de domino BIND y analizador de acceso a la red SARG para el campus central.	
ENCUESTAS – HP ML 110	Limesurvey: Servidor de encuestas online.		Al liberar actualizaciones el fabricante
	OMTP (Observatorio del Mercado de Trabajo de Pasto): S.I con el objetivo de generar información estratégica para la toma de decisiones respecto a la formulación y gestión de la política de empleo a nivel local.		Semestral

Procedimientos administración de sistemas: el objetivo del área es mantener actualizadas, aseguradas y en óptimo funcionamiento las plataformas de infraestructura tecnológica de servidores y Sistemas de Información de la universidad para brindar el mejor servicio posible a la comunidad académica entre los principales procesos que maneja se encuentran:

- Administración, mantenimiento y aseguramiento del sistema de comunicación interna (Microsoft Lync) de la Universidad de Nariño.

- Creación de cuentas de correo institucional para Funcionarios, Docentes, Estudiantes.

- Administración de listas de correo para difusión de información en forma masiva.

- Montaje, aseguramiento y administración de sistemas de Información alojados en los servidores de la UIT.

- Apoyar en la implementación e investigación sobre nuevas tecnologías en comunicaciones, e internet.

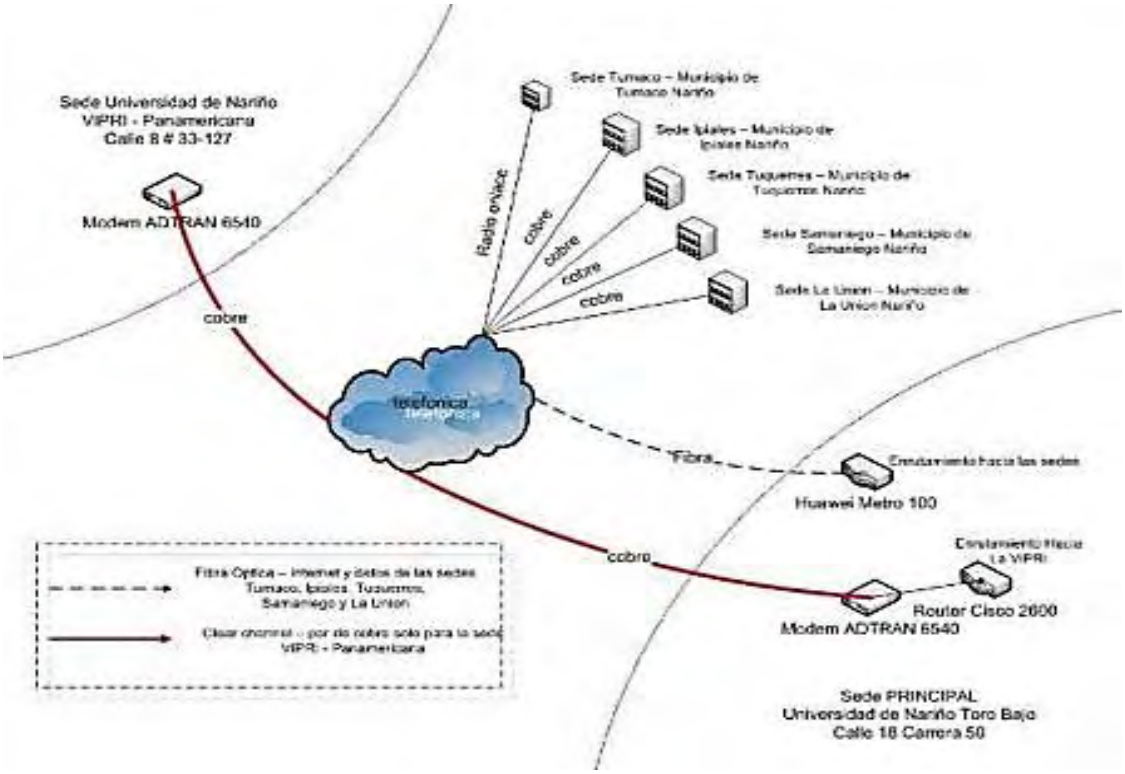
- Salvaguardar la confidencialidad de la información tanto de los usuarios de la red como de la información de las bases de datos de la Universidad.

- Participar, de acuerdo a su competencia, en el desarrollo de los planes estratégicos e informáticos de la Universidad, modernización tecnológica.

b. Administración red de datos e internet: comprende la red de datos e internet de la Universidad de Nariño, dentro de su sede principal y subsedes:

Dependencias a las que se presta el servicio: todo el campus universitario de Torobajo, sede VIPRI, liceo de la Universidad, sedes de los municipios de Tumaco, Ipiales, Tuquerres, Samaniego y La Unión. (ver figura 3)

Figura 3. Infraestructura red de datos e internet de la Universidad de Nariño y municipios



Se puede observar cada uno de los nodos alojados en las diferentes sedes de la Universidad, para el cual se hace la siguiente descripción:

- La red de datos tiene como nodo central un switch 3com 4500g el cual va directamente conectado a la servicio de Internet que provee telefónica, a este también está conectada la granja de servidores de la Universidad, entre los servidores se encuentra el servidor proxy, el cual a través de su otra interface de red a otro switch 3com 4500g equipo de conmutación principal para la red LAN, este se conecta a otro switch 3com 4900, el cual se encarga de interconectar a cada uno de los bloques de la universidad a través de fibra óptica. Todo lo anterior, se encuentra en el Aula de Informática.

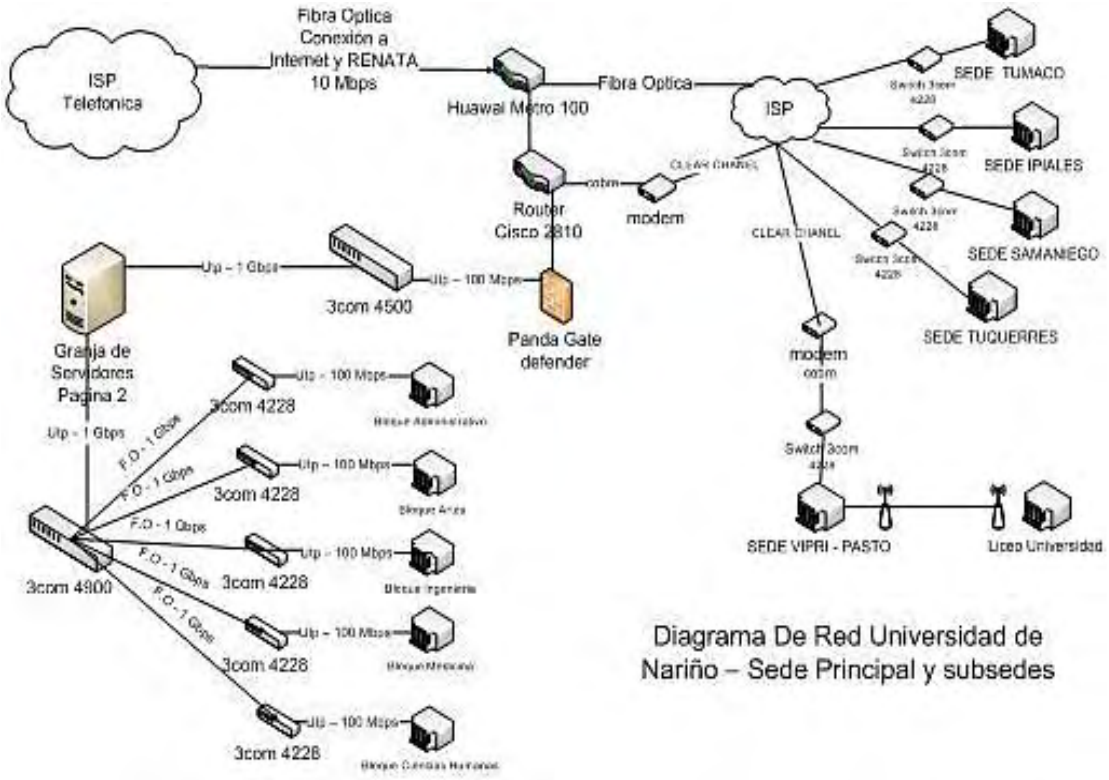
- En cada uno de los bloques de la universidad se encuentra un switch 3com 4228 encargado de recibir la fibra óptica que va desde el Aula de Informática y sirve de distribución ya sea a otros switchs o a los usuarios.

- Para interconectar a la sede de la VIPRI se utilizó como equipo enrutador un Cisco 2600 el cual va directamente conectado a un Modem Adtran 2000x, en enlace de las dos sedes se realiza a través de un clear 28ython que usa como medio de transmisión cobre, igualmente en la VIPRI existe un Modem Adtran 2000x y un router Cisco 2500, este se conecta a un switch NetGear, el cual distribuye fibra óptica a cada uno de los bloques. Todo lo anterior se encuentra en el bloque de Idiomas primer piso.

- Para el Liceo de la Universidad se cuenta con dos antenas Cisco Aironet 1300 las cuales sirven para enlazar a la VIPRI con el Liceo a través de una conexión wifi, igualmente el Liceo cuenta con 2 switchs 3com 4200 para distribución del cableado a cada puesto de trabajo y hacia las aulas de informática. Esto se encuentra en la oficina de psicología del liceo y en el bloque de idiomas en la VIPRI.

- Para interconexión hacia las sedes se dispone de equipo enrutador un Huawai metro 100, en cada una de las sedes se tiene un modem Adtran serie 2000, un router NetGear, y un switch 3com para la distribución del cableado hacia aulas de informática y usuarios finales y para observar el diagnostico de cómo se encuentra configurada la sede principal de Torobajo se presenta el siguiente diagrama; (ver figura 4)

Figura 4. Configuración principal red de datos sede principal Torobajo



En la figura 4, se puede observar la clase de equipos y su ubicación en cada uno de los bloques de la sede principal, además los canales de Internet que la Universidad tiene contratado con Telefónica.

Procedimientos administración de red de datos e internet: el objetivo es administrar, gestionar, mantener y operar efectivamente, la red lógica y física, de la Intranet e Internet, tanto en la sede principal como de las subsedes. Comprende red de datos e internet de la Universidad de Nariño, dentro de su sede principal y subsedes, entre los principales procesos que maneja se encuentran:

- Configuración de nuevos equipos que se conecten a la red, tanto cableada como inalámbrica.

- Solicitar e implementar servicios de RENATA, tales como: videoconferencias, oficina virtual y trasmisión vía *streaming*.

- Denegar y permitir servicios de red: messenger, puertos, páginas web, ftp, basándose en las peticiones de los usuarios y las políticas internas de la UIT.

- Regulación del uso de la INTRANET e INTERNET, con el fin de racionalizar y optimizar el uso de dichos recursos y servicios y asegurar una mayor calidad en el desarrollo de las funciones académicas y administrativas de la Universidad. Estas normas se fundamentan en valores como la responsabilidad, la eficiencia y la productividad en el uso de recursos internos.

- Mantenimiento físico preventivo de los equipos activos de red y cableado estructurado.

- Acceso a Internet e intranet de más de 1190 equipos a través de la red cableada, así como de más de 1270 equipos con acceso a Internet mediante la red inalámbrica en el campus principal, 200 equipos aproximadamente en la sede de la VIPRI, 55 equipos en la sede de Ipiales, 40 en la sede de Tumaco, 20 en la sede de Tuquerres, 20 en la sede de La Unión y 20 en la sede de Samaniego. El acceso se encuentra centralizado en la sede principal, para un total de más de 2450 equipos con servicio de Internet.

- Administración de la red de alta velocidad, que cuenta con un canal de acceso a Internet de 20 Mbps para la Universidad, un canal de fibra óptica entre las diferentes Universidades de la ciudad con un ancho de banda de 10 Mbps, un canal hacia la ciudad de Popayán con un ancho de banda de 40Mbps, un canal hacia las demás Universidades del país a 200 Mbps.

- El acceso a Internet se presta a través de un canal dedicado de fibra óptica el cual lo provee Telefónica Telecom, el ancho de banda de este canal de de 10 Mbps el cual se lo planea ampliar en los próximos meses del año 2014.

- El canal hacia las diferentes sedes de la Universidad lo provee Telefónica a través de un *Clear Channel Frame Relay* de cobre.

- Servicio de Video Conferencia hacia cualquier parte del mundo a través del sistema de video conferencia Polycom VSX 5500, soportado por un conjunto de IP públicas de la Universidad.

- Conexión de fibra óptica entre todos los bloques del campus principal y sede de la VIPRI, el cual esta soportado por swiches 3com con puertos de fibra óptica, lo que garantiza que el backbone de la red se encuentre a una velocidad de 1 Gbps y los accesos a los usuarios finales a 100 Mbps, este acceso se encuentra centralizado en el Aula de Informática de la Universidad.

- Acceso a Internet inalámbricamente mediante 8 antenas cisco Aironet 1300 en el campus principal de la Universidad, y 10 access point Lynksys en el campus principal y en las sedes de la VIPRI, Ipiales y Túquerres.

- Firewall físico Fortinet, los cuales protegen a la granja de servidores y en los accesos principales a Internet e intranet, lo que garantiza la seguridad de toda la red de la Universidad.

c. Administración portal web. El Portal Web Universitario www.udenar.edu.co se encuentra administrado bajo plataforma Microsoft en un servidor con sistema operativo Windows Server 2008 SP1 bajo el framework 3.5 de .Net, desarrollado en su gran mayoría en el lenguaje de programación ASP.Net con aplicaciones de Silverlight y Adobe Flash CS3.

Su diseño se encuentra establecido por una página maestra la cual cambia su contenedor según las opciones ofrecidas por los diferentes menús, manejando los colores institucionales como el verde y el amarillo.

En sus contenidos de información se encuentran las secciones de noticias y actualidad universitaria, eventos, convocatorias, correo electrónico, boletín de prensa, el espacio de interacción para la reforma universitaria y un menú donde se puede acceder a los principales recursos de la Universidad de Nariño, como sus programas académicos y las diferentes dependencias.

Algunas de las aplicaciones que se conectan a través del Portal Web se encuentran desarrolladas bajo lenguaje de programación PHP y están ubicadas en un servidor APACHE, un ejemplo de estas aplicaciones son el sistema de matrículas y el sistema Web Matías, el cual le permite administrar de manera independiente y autónoma la información general de cada programa académico; de igual manera, en dicho servidor se encuentran almacenadas las bases de datos de las diferentes aplicaciones manejados bajo los motores de PostgresSQL y MySQL.

Actualmente, el Portal Web Universitario se encuentra a cargo de un profesional en Licenciatura en Informática quien lo administra integralmente con la colaboración de un Monitor Técnico del programa de Licenciatura en Informática quienes brindan soporte en la actualización del Portal así como al desarrollo de nuevos sitios.

Procedimientos administración portal web:

- Administración, publicación, montaje y mantenimiento de los sitios Web existentes dentro del Portal Universitario.

- Desarrollo de las políticas de seguridad y accesibilidad del portal.

- Seguimiento, análisis, interpretación y evaluación estadística del tráfico del portal.

- Gestión y capacitación de los diferentes sistemas de publicación específicos (Gestores de contenidos) para las respectivas dependencias de la Universidad de Nariño.

- Mantenimiento el diseño Web del Portal de acuerdo con la definición de la estructura del mismo.

- Revisión y control de posibles errores existentes tanto en los links, estética como de contenido de la información.

- Coordinación de las comunicaciones con el Portal Web Universia y la Universidad de Nariño.

- Participar activa en el desarrollo de los planes estratégicos e informáticos de la Universidad.

d. Área de soporte y servicios tecnológicos: "El Área de Soporte y Servicios Tecnológicos brinda a las unidades Académicas y Administrativas de la Universidad de Nariño y sus respectivas sedes el soporte y la asistencia técnica en el mantenimiento preventivo y correctivo de los equipos de cómputo y ofimática"[4].

Para el servicio de soporte técnico y mantenimiento correctivo se dispone de un procedimiento que se describe en el formato AUI-SPM-PR-02 – Procedimiento Servicio de Mantenimiento y Apoyo en el Manejo de Hardware y Software

Asistencia y soporte técnico: el servicio de soporte técnico tiene como objetivo brindar solución a los problemas que presenten los equipos de cómputo y ofimática en hardware y software. Dentro de este servicio se encuentran tareas, tales como: configuración y conexión a la red de datos, instalación y configuración de periféricos como impresoras, cámaras, escáner, unidades ópticas y demás, recuperación y/o creación de copias de seguridad de la información, identificación, diagnóstico y eliminación de virus informáticos, asesorías en el uso del sistema operativo, software ofimático y aplicaciones básicas, así como también ensamblaje de equipos de cómputo, entre otras.

[4] Ibíd.

Formato: AUI-SPM-FR-07 Asistencia y Soporte Técnico Dependencias

Mantenimiento preventivo: la ejecución el plan de mantenimiento preventivo busca diagnosticar y corregir posibles fallas que estén afectando el normal funcionamiento de los equipos de cómputo.

En el mantenimiento preventivo se realizan las siguientes tareas:

- Registro en el Sistema ASST (inventario e historial de mantenimientos).
- Limpieza de hardware.
- Revisión, instalación y actualización de Software.
- Comprobación de errores de Disco Duro.
- Optimización del sistema operativo.
- Identificación, diagnóstico y eliminación de virus informáticos.

Para llevar a cabo este proceso es necesario que cada dependencia de acuerdo al cronograma establecido, reserve un espacio de tiempo seleccionando el día y la hora para realizar el mantenimiento, esta información será recolectada por el monitor técnico adscrito a la Unidad de Informática y Telecomunicaciones que visitará la dependencia el primer día de cada semana.

Formato: AUI-SPM-FR-10 Mantenimiento Preventivo Dependencias

Por otra parte la UIT tiene un Plan de Mantenimiento Preventivo de Equipos de Cómputo, Ofimática y Telecomunicaciones, en el cual se describen los procedimientos y tareas a realizarse.

Inventario y hoja de vida del hardware: para gestionar el inventario de hardware el ASST dispone de una aplicación de escritorio creada en Visual Basic .Net, la cual se conecta a una base de datos en Postgres. Este software permite el registro tanto del hardware como el historial de mantenimientos de preventivos, correctivos y servicio de soporte técnico.

1.2.2 Funciones personal UIT[5]:

Tabla 2. Funciones – Coordinador aula de informática

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Coordinador Aula de Informática**
No. De Cargos:	Uno (1)
Dependencia:	Unidad de Informática y Telecomunicaciones.
Cargo del Jefe Inmediato:	**Vicerrector Académico**
II. PROPOSITO PRINCIPAL	
Direccionar el proceso tecnológico de la Universidad de Nariño en todos sus campos, contribuyendo al desarrollo de las TIC´s, alineada con la planeación institucional y los adelantos técnicos.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Administrar eficientemente los recursos con el fin de atender las labores de docencia, investigación y proyección social, según parámetros establecidos. 2. Formular políticas, planes, programas y proyectos para el mejoramiento de los servicios que presta el Aula de Informática para su desarrollo y modernización, según procedimientos. 3. Dirigir y participar en los estudios e investigaciones que hagan eficiente la prestación de los servicios, de acuerdo con estrategias de gestión. 4. Implementar y ejecutar programas de telecomunicaciones con otros servicios y sistemas de información, teniendo en cuenta políticas, estándares y requerimientos. 5. Programar y ejecutar asesorías y asistencias técnicas a las dependencias académicas administrativas en los diferentes servicios que presta el Aula de Informática, según las necesidades de capacitación. 6. Programar y ejecutar los cursos de Lenguaje y Herramientas Informáticas, de acuerdo a las necesidades académicas. 7. Realizar procedimientos de inducción y reinducción sobre la utilización de tecnologías de comunicación, redes y mantenimiento de equipos de cómputo para el personal que labora en el Aula de Informática, según procedimientos establecidos. 8. Formar parte activa del Comité de Sistemas, dando cumplimiento a los lineamientos establecidos. 9. Administrar y manejar la caja menor, según procedimientos establecidos.	

[5]UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES. Manual especifico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

Continuación tabla 2.

10. Coordinar el estado de las instalaciones físicas y equipos y ordenar su mantenimiento, según procedimientos establecidos. 11. Programar la adquisición de elementos y equipos, garantizando su oportuna y transparente provisión. 12. Implementary mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Universidad. 13. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 14. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene.

Fuente. UNIDAD DE INFORMÀTICA Y TELECOMUNICACION. Manual específico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

Tabla 3. Funciones – Administrador soporte y servicios tecnológicos

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador soporte y servicios tecnológicos.**
No. De Cargos:	Uno (1)
Dependencia:	Unidad de Informática y Telecomunicaciones.
Cargo del Jefe Inmediato:	**Director Aula de Informática**
II. PROPOSITO PRINCIPAL	
Contribuir en la eficiencia e innovación de los procesos y servicios de la infraestructura tecnológica y comunicaciones de la Universidad de Nariño, a través de la gestión del soporte técnico y el mantenimiento preventivo en los equipos de cómputo de las diferentes dependencias académicas y administrativas.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Administrar y supervisar los procedimientos; de soporte y asistencia técnica en la solución de los problemas que presenten los equipos de cómputo y ofimática de las dependencias académicas y administrativas de la Universidad de Nariño. 2. Ejecutar los cronogramas y procedimientos del mantenimiento preventivo en los equipos de cómputo de la Universidad de Nariño. 3. Administrar y controlar el inventario de los equipos de cómputo y de	

Continuación tabla 3.

ofimática del Aula de Informática. 4. Diseñar e implementar el programa de mantenimiento preventivo en las salas de cómputo del Aula de Informática. 5. Instalar y configurar el hardware y software disponible en las salas de cómputo del Aula de Informática, acorde a las solicitudes de las unidades académicas o administrativas. 6. Apoyar el servicio de préstamo de recursos audiovisuales y multimedia. 7. Asesorar cuando se requiera a las diferentes dependencias en la adquisición de equipos de cómputo y ofimática. 8. Brindar asistencia y soporte técnico en las actividades o eventos programados por la Universidad de Nariño, dentro y fuera de las instalaciones, según sus requerimientos. 9. Seleccionar, capacitar y evaluar a los monitores técnicos adscritos al Área de Soporte y Servicios Tecnológicos del Aula de Informática. 10. Presentar informes cuando sean solicitados sobre el estado actual de los equipos de cómputo del Aula de Informática. 11. Investigar e implementar sobre nuevas tecnologías en software y hardware. 12. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Universidad. 13. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 14. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene.

Fuente. UNIDAD DE INFORMÀTICA Y TELECOMUNICACION. Manual específico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

Tabla 4. Funciones – Administrador de red de datos e internet

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador de red de datos e internet**.
No. De Cargos:	Uno (1)
Dependencia:	Aula de informática
Cargo del Jefe Inmediato:	**Director Aula de Informática**
II. PROPOSITO PRINCIPAL	
Asegurar que la red de datos funcione correctamente, dando servicio de internet, intranet y Renata a todas las dependencias de la Universidad de	

Continuación tabla 4.

Nariño, permitiendo la adecuada aplicación de las normas y procedimientos vigentes, con el fin de cumplir con las labores de Docencia, Investigación y Proyección Social de la Universidad de Nariño.
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES
1. Brindar soporte, operación, gestión y mantenimiento de la red privada e Internet, tanto de la sede principal como de las sedes (VIPRI, Centro, Liceo, Ipiales, Tumaco, Tuquerres, La Unión y Samaniego), finca botana, según requerimientos. 2. Realizar la configuración, gestión y mantenimiento de los equipos activos y pasivos de red, además refinamiento del servidor proxy y firewall, según especificaciones técnicas. 3. Realizar la instalación, configuración y mantenimiento de los servidores Proxy, Firewall, DHCP, DNS, FTP, según procedimientos establecidos. 4. Administrar la utilización del ancho de banda, para evitar su uso inadecuado, de acuerdo a lineamientos establecidos. 5. Participar en el desarrollo de los planes estratégicos e informáticos de la Universidad, dando cumplimiento a la modernización tecnológica. 6. Administrar la red nacional académica de tecnología avanzada (RENATA), según procedimientos establecidos. 7. Apoyar en la implementación e investigación sobre nuevas tecnologías en comunicación, telemática e Internet, videoconferencia red de alta velocidad, según metodología planteada. 8. Administrar lógicamente la red inalámbrica de la Universidad, de conformidad con los lineamientos fijados por el Aula de Informática. 9. Apoyar en la administración de sistemas de información y administración de servidores, según requerimientos. 10. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Universidad. 11. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 12. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad.

Fuente. UNIDAD DE INFORMÀTICA Y TELECOMUNICACION. Manual específico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

Tabla 5. Funciones - Administrador de sistemas

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador De Sistemas**
No. De Cargos:	Uno (1)
Dependencia:	Aula de informática
Cargo del Jefe Inmediato:	**Director Aula de Informática**
II. PROPOSITO PRINCIPAL	
Mantener actualizada y asegurada la plataforma de infraestructura tecnológica de servidores computacionales, que permiten a la comunicación universitaria, una fácil comunicación apoyando la agilidad de los procedimientos de las dependencias de la Universidad de Nariño.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Garantizar el aseguramiento lógico y administración de servidores, según metodologías y estándares de seguridad. 2. Administrar el sistema de correo electrónico de la Universidad de Nariño – Postmaster, según la normativa de la institución. 3. Montaje y Administración de sistemas de Información alojados en los servidores del Aula de Informática de la Universidad de Nariño, según requerimientos de usuarios, recursos disponibles y normatividad establecida. 4. Administrar Bases de Datos, asegurando la confidencialidad, la integridad y la disponibilidad de la información. 5. Apoyar en la implementación e investigación sobre nuevas tecnologías en comunicación, telemática e Internet. 6. Apoyar a la administración del portal web Universitario. 7. Salvaguardar la confidencialidad de la información tanto de los usuarios de la red como de la información de las bases de datos de la Universidad. 8. Administrar mantener y asegurar el sistema interno de mensajería instantánea, garantizando funcionalidad en el sistema. 9. Participar, de acuerdo a su competencia, en el desarrollo de los planes estratégicos e informáticos de la Universidad, contribuyendo a la modernización tecnológica. 10. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Universidad. 11. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 12. Adelantar, de acuerdo a su competencia y responsabilidad, las	

Continuación tabla 5.

actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene.

Fuente. UNIDAD DE INFORMÀTICA Y TELECOMUNICACION. Manual específico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

Tabla 6. Funciones – Administrador portal web

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador Del Portal Web**
No. De Cargos:	Uno (1)
Dependencia:	Aula de informática
Cargo del Jefe Inmediato:	Vicerrectora Académico
II. PROPOSITO PRINCIPAL	
Asegurar el correcto funcionamiento del Portal Web Institucional, en función del intercambio informativo entre la comunidad universitaria, sociedad y grupos de interés, con el fin de cumplir con las labores de Docencia, Investigación y Proyección Social de la Universidad de Nariño.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Administrar, actualizar, brindar soporte y mantenimiento al Portal Web Institucional conforme a procedimientos establecidos. 2. Desarrollar los sitios web de las unidades académicas y administrativas de la Universidad, realizando su publicación, montaje y mantenimiento, de acuerdo a los requerimientos institucionales. 3. Realizar capacitación en el manejo de los sistemas de publicación específicos (gestores de contenidos) a las unidades académicas y administrativas de la universidad, de acuerdo con prioridades establecidas y requerimientos institucionales. 4. Administrar el convenio Universia– Universidad de Nariño, según procesos y metodologías definidas. 5. Hacer el seguimiento, análisis, interpretación y evaluación estadística del tráfico del Portal Web Institucional, siguiendo especificaciones técnicas. 6. Desarrollar las políticas de seguridad y accesibilidad del portal teniendo en cuenta la normatividad vigente. 7. Investigar e implementar nuevas tendencias tecnológicas referentes al área de su desempeño, según necesidades. 8. Brindar respaldo al área de administración de sistemas, según requerimientos. 9. Participar de acuerdo a su competencia en el desarrollo de los planes	

Continuación tabla 6.

informáticos de la Universidad y modernización tecnológica, según necesidades. 10. Coordinar y supervisar las actividades de todos los integrantes que colaboran en el funcionamiento del Portal Web Institucional, según procedimientos establecidos. 11. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 12. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene. 13. Desempeñar las demás funciones que le asigne el superior inmediato de acuerdo con el nivel, la naturaleza, el área de desempeño, y el perfil del empleo.

Fuente. UNIDAD DE INFORMÀTICA Y TELECOMUNICACION. Manual específico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

1.3 MARCO TEÓRICO

Seguridad de la información: "Es la protección de los activos de información frente a diferentes amenazas, con el objetivo de preservar su disponibilidad, integridad y confidencialidad que permitan a la organización cumplir con su misión o continuidad del negocio, minimizar el riesgo de materialización de las amenazas potenciales y maximizar el retorno de inversiones y oportunidades"[6].

Las organizaciones que conocen los riesgos y los problemas que enfrentan relacionados con la seguridad de la información, ya sea por ataque deliberado de personal interno o externo, por un evento natural o un evento industrial, cuentan con personal certificado en prácticas de seguridad informática y gestionan varios recursos para la protección de la información y sistemas, lo que permite que dicha información sean menos vulnerable a ataques que hagan posible su distribución, modificación e incluso su eliminación[7].

[6]SEGURIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.ean.edu.co/index.php?option=com_content&view=article&id=2597&Itemid=1280. [citado marzo de 2014].

[7]CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado marzo de 2014].

Los principios básicos de la seguridad de la información, son los siguientes:

- Disponibilidad: es la capacidad de accesibilidad a la información cuando se la requiera utilizar. La disponibilidad protege al sistema contra intentos accidentales o intencionados de realizar una eliminación de información no autorizada, denegación del servicio o accesibilidad a la información y de intentos de utilizacióndel sistema o la información para propósitos no autorizados.

- Integridad: se encarga de garantizar que la información únicamente pueda ser modificada por personal autorizado y de manera controlada y así evitar la pérdida de consistencia. La violación de la integridad se presenta cuando un empleado, programa o proceso (por accidente o intencionalmente) modifica o elimina los datos que hacen parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y dicha modificación sea registrada, asegurando su precisión y confiabilidad.

- Confidencialidad: aseguramiento de que la información es accesible solo para personal autorizado.

Familia de normas ISO 27000: "La información es uno de los activos más importantes que debe ser manejado eficientemente, para garantizar ventajas dentro de los campos administrativos y académicos competidos en la actualidad, por lo que las organizaciones incrementan su inversión en el uso de diferentes tecnologías para su aseguramiento"[8].

Una adecuada gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y basado en objetivos claros de seguridad. Este proceso es el que conforma un Sistema de Gestión de Seguridad de la Información (SGSI), que podría considerarse por similitud con el Sistema de Calidad para la Seguridad de la Información basado en la norma ISO 9001.

Actualmente existe una serie de normas que proporcionan un marco de gestión para la seguridad de la información, las cuales pueden ser utilizadas por toda organización, cualquiera que sea su naturaleza y propósito. Estas normas son las que componen la serie ISO/IEC 27000 por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), donde se indica como estructurar e implantar un Sistema de Gestión de Seguridad de la Información basado en ISO 27001.

[8]EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado marzo de 2014].

Origen: Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British StandardsInstitution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas, como:

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001
- BS 8800. Publicada en 1996. Origen de OHSAS 18001

La norma BS 7799 de BSI apareció en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas. En la segunda parte (BS 7799-2), publicada en 1998, la que estableció los requisitos de un sistema de seguridad de la información para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin grandes cambios, como ISO 17799 en el año 2000.En 2002, se revisó la segunda parte para adecuarse a la filosofía de normas ISO de sistemas de gestión.En 2005, esta norma se publicó por ISO como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799 que se renombró como ISO 27002:2005 el 1 de Julio de 2007.

En 2006, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

De igual manera, ISO continúa desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001.

Serie 27000: Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO/IEC 27000**: Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.

- **ISO/IEC 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y comprende dos secciones. La primera sección contiene los requisitos del Sistema de Gestión de Seguridad de la Información para obtención de certificación.

Las cláusulas metodológicas definidas en el estándar son:

Sistema de Gestión de Seguridad de la Información:

Responsabilidad de la Dirección:

- Compromiso de la Dirección: Se debe proveer evidencia de su compromiso con el proyecto.
- Provisión de recursos

Auditorías Internas a intervalos planificados para determinar:

- Si el SGSI es conforme a ISO 27001
- Si el SGSI es conforme con otros requisitos
- Si el SGSI está implantado y mantenido de forma efectiva
- Si el SGSI funciona según lo esperado

Revisión de la Dirección de forma regular para garantizar:

- Que el alcance sigue siendo adecuado
- Que las mejoras del SGSI han sido debidamente identificadas

Mejora continua del SGSI:

- Deben tomarse acciones correctivas y preventivas
- Tener experiencias propias o de otras organizaciones
- Comunicar acciones y mejoras a todas las partes interesadas
- Asegurar que las mejoras alcanzan los objetivos buscados

La segunda sección correspondiente al Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

Desde el punto de vista de certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables.

- ISO/IEC 27002: “Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios”[9].

[9]ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado marzo de 2014].

Figura 5. Dominios ISO 27002

Fuente: Disponible en Internet. http://iso27002.es/

A5 Política de Seguridad

[5.1] Política de seguridad de la información:La Dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

A6 Organización de la Seguridad de la Información

[6.1]Organización interna: Gestionar la seguridad de la información dentro de la Organización. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.

[6.2] Terceros: Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de informaciónde la organización sean accesibles por terceros.

A7 Gestión de Activos

[7.1] Responsabilidad sobre los activos: Alcanzar y mantener una protección adecuada de los activos de la Organización.

[7.2] Clasificación de la información:.Asegurar que se aplica un nivel de protección adecuado a la información.

A8 Seguridad de los Recursos Humanos

[8.1]Seguridad en la definición del trabajo y los recursos: Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

[8.2] Seguridad en el desempeño de las funciones del empleo: Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

[8.3] Finalización o cambio del puesto de trabajo: Garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.

A9 Seguridad Física y del Entorno

[9.1] Áreas seguras: Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

[9.2] Seguridad de los equipos: Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

A10 Gestión de las Comunicaciones y Operaciones

[10.1]Procedimientos y responsabilidades de operación: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

[10.2] Supervisión de los servicios contratados a terceros: Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.

[10.3] Planificación y aceptación del sistema: Minimizar el riesgo de fallos en los sistemas.

[10.4] Protección contra software malicioso y código móvil: Proteger la integridad del software y de la información.

[10.5]Gestión interna de soportes y recuperación: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

[10.6] Gestión de redes: Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.

[10.7] Utilización y seguridad de los soportes de información: Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.

[10.8]Intercambio de información y software: Mantener la seguridad de la información y del software que se intercambian dentro de la organización o con cualquier entidad externa.

[10.9] Servicios de comercio electrónico: Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

[10.10] Monitorización: Detectar actividades de procesamiento de la información no autorizadas.

A11 Control de Acceso

[11.1] Requerimientos de negocio para el control de accesos: Controlar los accesos a la información.

[11.2] Gestión de acceso de usuario: Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

[11.3] Responsabilidades del usuario: Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

[11.4] Control de acceso en red: Impedir el acceso no autorizado a los servicios en red.

[11.5] Control de acceso al sistema operativo: Impedir el acceso no autorizado al sistema operativo de los sistemas.

[11.6] Control de acceso a las aplicaciones: Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

[11.7] Informática móvil y teletrabajo: Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

[12.1] Requisitos de seguridad de los sistemas: Garantizar que la seguridad es parte integral de los sistemas de información.

[12.2] Seguridad de las aplicaciones del sistema: Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

[12.3] Controles criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

[12.4] Seguridad de los ficheros del sistema: Garantizar la seguridad de los sistemas de ficheros.

[12.5] Seguridad en los procesos de desarrollo y soporte: Mantener la seguridad del software del sistema de aplicaciones y la información.

[12.6] Gestión de las vulnerabilidades técnicas: Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

A13 Gestión de los Incidentes de Seguridad

[13.1] Comunicación de eventos y debilidades en la seguridad de la información: Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

[13.2] Gestión de incidentes y mejoras en la seguridad: Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

A14 Gestión de la Continuidad del Negocio

[14.1] Aspectos de la gestión de continuidad del negocio: Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

A15 Cumplimiento

[15.1] Conformidad con los requisitos legales: Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

[15.2] Revisiones de la política de seguridad y de la conformidad técnica: Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.

[15.3] Consideraciones sobre la auditoría de sistemas: Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Sistema de Gestión de Seguridad de la Información:"La gestión de la seguridad de la información es necesaria que se realice mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso se puede constituir por el Sistema de Gestión de Seguridad de la Información(SGSI)"[10].

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se instituye ISO 27001, cuyo estándar ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, 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 correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar:

- Confidencialidad: aseguramiento de que la información es accesible solo para personal autorizado.
- Integridad: se encarga de garantizar que la información únicamente pueda ser modificada por personal autorizado y de manera controlada y así evitar la pérdida de consistencia.
- Disponibilidad: es la capacidad de accesibilidad a la información y los sistemas de tratamiento de la misma cuando se los requiera utilizar

Este modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en un análisis y evaluación de riesgos y en una medición de la eficacia de estos. Por lo tanto el SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

La aceptación de este estándar debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización.

[10]PARÁMETROS FUNDAMENTALES PARA LA IMPLANTACIÓN DE UN SGSI SEGÚN ISO 27001:2005. [en línea] Disponible en internet. http://www.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi. [citado marzo de 2014].

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional impulsa que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del Sistema de Seguridad de la Información.
- Mejoramiento contínuo en base a la medición del objetivo.

Beneficios de un SGSI:

- Involucrar a la Dirección en la seguridad de la información
- Desarrollar políticas formales de cumplimiento obligatorio
- Conocer realmente de qué activos dispone la organización
- Cumplir con la legislación vigente ligada al proyecto
- Realizar análisis de riesgos para el desarrollo del negocio
- Introducción de contratos de niveles de servicio
- Reforzar la seguridad ligada a personal
- Disponer de planes de contingencias ante incidentes
- Disponer planes de continuidad del negocio y recuperación ante desastres
- Desarrollo de indicadores del desempeño del SGSI
- Disminución de riesgos aniveles aceptables, etc.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, se adopta el ciclo de mejora continuaPHVA (Véase Figura 6).

Figura 6. Ciclo PHVA

Fuente: http://www.iso27000.es/sgsi.html

- **Planear**: Establecer el Sistema de Gestión de Seguridad de la Información. Es una fase donde se realiza el análisis y evaluación de riesgos, el Plan de Tratamiento de Riesgos y la definición de las políticas de seguridad.
- **Hacer**: Implementar y operar el Sistema de Gestión de Seguridad de la Información. Es una fase que envuelve la implementación y operación de los controles.
- **Verificar**: Monitorear y revisar el Sistema de Gestión de Seguridad de la Información. Es una fase de medición de resultados, auditoria interna y revisión por parte de la dirección de la organización.
- **Actuar**: Mantener y mejorar el Sistema de Gestión de Seguridad de la Información. Es una fase en la que se llevan a cabo acciones preventivas y correctivas para el Sistema de Gestión de Seguridad de la Información.

Llevar a cabo la implantación de un Sistema de Gestión de Seguridad de la Información, comprende las siguientes etapas:

- Identificar los objetivos del negocio
- Obtener el patrocinio de la alta dirección
- Establecer el alcance (algunos procesos del negocio)
- Diagnóstico / Análisis de brecha (Gap Analysis)

En esta etapa se determina la brecha con respecto al nivel de madurez de los requerimientos del estándar ISO/IEC 27001:2005, el cual dispone de unas cláusulas cuya finalidad es establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, en el contexto de los requerimientos de la organización.

El estándar comprende dos (2) secciones: en la primera se especifican cinco (5) cláusulas, de cumplimiento obligatorio para obtener la certificación, enfocadas a características metodológicas del SGSI. En la segunda, denominada Anexo A, se definen los controles mínimos para gestionar la seguridad de la información de manera adecuada. Desde el punto de vista de la certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables.

Las cláusulas metodológicas definidas en el estándar, son:

- Sistema de Gestión de Seguridad de la Información
- Responsabilidad de la Dirección
- Auditorías Internas
- Revisión de la Dirección
- Mejora continua del SGSI.

Los controles del Anexo A están organizados en once (11) dominios, denominados A5 hasta A15:

A5 Política de Seguridad
A6 Organización de la Seguridad de la Información
A7 Gestión de Recursos
A8 Seguridad de los Recursos Humanos
A9 Seguridad Física y del Entorno
A10 Gestión de las Comunicaciones y Operaciones
A11 Control de Acceso
A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
A13 Gestión de los Incidentes de Seguridad
A14 Gestión de la Continuidad del Negocio
A15 Cumplimiento

El diagnóstico se puede realizar por medio de una serie de entrevistas a los responsables de los temas contemplados en el estándar, las cuales pueden ser complementadas con una revisión documental de los procedimientos y políticas asociadas a la seguridad de la información.

Una vez relevada la información, se procede a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala definida por el estándar COBIT, consignada en la **Tabla 7. Escala nivel de madurez COBIT** contenida en el Anexo J – Plantillas y tablas.

- Asignar recursos y capacitar al equipo

- Análisis y evaluación de riesgos de activos de información:

- Definir método de análisis y evaluación: En el ámbito empresarial, toda organización, cualquiera que sea su naturaleza y propósito, se crea y se estructura en unas reglas y normas de comportamiento que permitan alcanzar unos objetivos propuestos.

  Existe un gran número de eventualidades que pueden perjudicar negativamente el cumplimiento de dichos objetivos, ya sean de origen interno o externo, intencionado o deliberado. De igual manera las innumerables medidas de protección contra este tipo de eventos son inabarcables por motivos de costo.

  Por tal razón, se hace necesario definir un proceso para identificar los riesgos más significativos, en oposición a los riesgos de bajo impacto, baja frecuencia o alto costo de control del mismo. Para este proyecto se utiliza la metodología MAGERIT.

- Preparar un inventario de los activos de información a proteger: En adición al inventario de activos, para la valuación de riesgos son de gran importancia los informes de vulnerabilidades, informes de seguimiento de riesgos y repositorio de incidentes para definir las amenazas y vulnerabilidades de cada activo de información.

- Análisis de riesgos: El análisis de riesgos es la herramienta por medio de la cual se puede identificar, clasificar y valorar los riesgos a los que la organización está expuesta y establecer los controles adecuados para minimizar la probabilidad de materialización o reducir el impacto de estos hasta un nivel tolerable o aceptable en caso de materializarse.

  En esta etapa se determina la frecuencia e impacto, se calcula el riesgo actual, y se determina el riesgo residual, resultante luego de que se implementen los controles.

- Evaluación de riesgos: En la medida en que el riesgo implica una eventual exposición a un impacto para la consecución de los objetivos de una organización, tiene una connotación negativa. No obstante, el riesgo es algo inherente a cualquier actividad y no puede considerarse un factor adverso, sino un factor que conviene conocer y gestionar adecuadamente para que se convierta en una ventaja competitiva para la unidad.

  Un mejor control del riesgo, en la medida en que se transmita a todos los grupos de interés (personal, proveedores, supervisores, etc.) puede proporcionar ventajas competitivas significativas. Esta característica del riesgo tanto como amenaza y como oportunidad se refleja tanto en la cantidad de riesgo que una organización es capaz de gestionar y la cantidad de riesgo que está dispuesta a gestionar para lograr los objetivos propuestos.Con los resultados obtenidos en el análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el *Informe de evaluación de riesgos TI*, el cual es utilizado para elaborar el *Plan de tratamiento de riesgos*.

- Gestionar el riesgo y elaborar un Plan de Tratamiento de Riesgos: Elaboración del Plan de Tratamiento de riesgos que contenga una serie de controles y recomendaciones básicas de seguridad para toda la organización que permita disminuir un alto grado de riesgo.

- Establecer la normativa para controlar el riesgo: Establecer las políticas de seguridad de la información que mejor se adapten a la organización.

- Monitorizar la implantación del SGSI: Con base en el informe de riesgos de TI, el plan de seguridad de TI y los informes de estado de la seguridad, se evalúa el avance de la implementación y la eficacia de los controles vigentes. La eficacia se mide a través de pruebas de vulnerabilidades o "ethical hacking", realizadas en forma coordinada.

- Prepararse para la auditoria de certificación

- Llevar a cabo auditorías internas periódicas.

Estándares y metodologías para el análisis y gestión de riesgos: "La gestión de riesgos de seguridad de la información es tal vez el proceso más significativo para la estructuración, mantenimiento y mejora de un sistema capaz de gestionar adecuadamente la seguridad de la información"[11].

Las metodologías de análisis y/o evaluación de riesgos ayudan a las organizaciones a acelerar este proceso. Algunas de las metodologías más utilizadas son:

- **ISO/IEC 27005:** Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Describe el proceso completo de gestión de riesgos dividiéndolo en 6 fases: Establecimiento del Alcance, Valoración de Riesgos (formada por las tareas de Análisis y Evaluación), Tratamiento de Riesgos, Aceptación de Riesgos, Comunicación de Riesgos y Monitorización y Revisión de Riesgos.

- **COBIT (*Control Objectives for Information and related Technology*): "**Es un modelo de gobierno para administrar el riesgo y controlar las Tecnologías de Información. Mantenido por ISACA (en inglés: *Information Systems Auditand Control Association*) y el IT *Governance Institute*, tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de Tecnologías de Información, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión"[12].

[11]SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado abril de 2014].

[12]¿Cuál es el mejor estándar de administración de riesgo para las TI? [en línea] Disponible en internet. http://www.emb.cl/gerencia/articulo.mvc?xid=1301. [citado abril de 2014].

La estructura del estándar COBIT, se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

En la actualidad se encuentra la versión 5, la cual proporciona una visión empresarial del Gobierno de Tecnologías de Información que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

- **MAGERIT: "**MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista"[13].

MAGERIT persigue los siguientes objetivos:

Directos:

a) Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
b) Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
c) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Actualmente se encuentra en la versión 3; durante el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997), el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La versión 2 y 3 de MAGERIT se ha estructurado en tres libros: "El Método", un "Catálogo de Elementos" y una "Guía de Técnicas".

[13]MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de InformaciónLibro I - Método. [en línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf. [citado abril de 2014].

El método: "Realización del análisis y de la gestión: En la Planificación del Análisis y Gestión de Riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto"[14].

Análisis de Riesgos: en el análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

Elementos del análisis de riesgos: aquí el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

a. Activos: El activo esencial es la información o dato.

b. Amenazas: determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.

Las amenazas según MAGERIT pueden ser de 4 tipos como se indicaen la **Tabla 8. Tipo de amenazas MAGERIT** contenida en el Anexo J – Plantillas y tablas.

c. Vulnerabilidades:Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

d. Impacto: Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto

e. Riesgo: Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia

f. Salvaguardas: Es un mecanismo de protección frente a las amenazas.

Catálogo de elementos: "Ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, escala de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información. Se persiguen dos objetivos[15]:

[14]Ibíd.

[15]Ibíd.

a. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

b. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Dicho catálogo está conformado por las siguientes tablas**: Tabla 9. Tipos de activos**, **Tabla 10. Dimensiones de valoración de un activo**,**Tabla 11. Valoración cualitativa** y **Tabla 12. Valoración cuantitativa** que pueden consultarse en el Anexo J – Plantillas y tablas.

Muchos Activos de información no son inventariables en sentido contable o como 'valor de cambio'; pero no por ello dejan de tener 'valor de uso' para la organización.

Controles: hay diferentes aspectos en los cuales puede actuar un control para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

[PR] Se requieren procedimientos tanto para la operación de los controles preventivos como para la gestión de incidencias y la recuperación tras las mismas.

[PER] política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.

Guía de técnicas: *"*Proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisisy gestión de riesgos"[16].

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la notación que desee, la que suele utilizar o la que ofrecen sus herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

Técnicas específicas: se han considerado de especial interés:

a. Uso de tablas para la obtención sencilla de resultados: La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

[16]Ibíd.

Estimación del impacto: se puede calcular el impacto con base a tablas sencillas de doble entrada. (Ver T**abla 13. Estimación del impacto** en el Anexo J – Plantillas y tablas)

Aquellos activos que reciban una calificación de impacto desastroso deberían ser objeto de atención inmediata.

Estimación de la probabilidad: por otra parte se modela la probabilidad de ocurrencia de una amenaza por medio de escalas cualitativas. (Ver **Tabla 14. Estimación de la probabilidad** en el Anexo J – Plantillas y tablas)

Estimación del riesgo: la estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

Este proceso de análisis de riesgos normalmente genera un MAPA DE RIESGOS, en el que se ubican los activos de información identificados y los cálculos realizados. (Ver Tabla 15. Mapa de riesgos en el Anexo J – Plantillas y tablas).

Con los resultados obtenidos con este análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el *Informe de evaluación de riesgos TI*, el cual es utilizado para elaborar el *Plan de tratamiento de riesgos*.

El objetivo general del análisis de riesgos, es identificar las causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para así tener suficiente información, optando por un diseño apropiadoe implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados.

Un minucioso análisis de riesgos; identificar, definir y revisar los controles de seguridad; determinar si se requiere incrementar las medidas de seguridad; y la identificación de los riesgos, los perímetros de seguridad, controles de acceso y los lugares de mayor peligro, pueden hacer el mantenimiento más fácilmente.

b. Técnicas algorítmicas para la obtención de resultados elaborados: dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos.

c. Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información:Los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e

incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Un árbol de ataque pasa revista a cómo se puede atacar un sistema, permitiendo identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y así lo que necesita saber y lo que necesita tener para realizar el ataque; de esta forma es posible refinar las posibilidades de que el ataque se produzca si se sabe a quién pudiera interesar el sistema y/o la información y se cruza esta información con las habilidades que se requieren.

Técnicas generales: son utilizadas en el desarrollo de un proyecto de análisis y gestión de riesgos. Se han considerado de especial interés:

b. Técnicas gráficas: histogramas, diagramas de Pareto y de tarta:

- Por puntos y líneas: Es la forma más clásica de presentación de resultados. Se limita a usar los ejes cartesianos usando las abscisas para recoger los datos y las ordenadas para mostrar su valor.
- Por barras: Los diagramas de barras disponen los elementos en unas coordenadas cartesianas convencionales: los elementos a considerar en un eje y los valores en el otro eje.
- Gráficos de 'radar': Estos gráficos representan las distintas variables o factores del fenómeno enestudio sobre ejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúanpara representar sus niveles y posibles umbrales en escala normal o logarítmica, según convenga.
- Diagramas de Pareto: Una gráfica de Pareto es utilizada para separar gráficamente los aspectos más significativos de un problema que el equipo sepa dónde dirigir sus esfuerzos para mejorar. Reducir los problemas más significativos (las barras más largas en una gráfica Pareto) servirá más para una mejora general que reducir los más pequeños.
- Diagramas de tarta: Estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360º de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica.

c. Sesiones de trabajo: entrevistas, reuniones y presentaciones:

- Entrevistas: Las entrevistas son reuniones con una persona o un grupo de personas con el objetivo de obtener cierta información. Las entrevistas se dicen estructuradas cuando se atiene a una serie de preguntas planificadas sin

margen para la improvisación. Las entrevistas se dicen libres cuando, existiendo un objetivo claro, no existe un formulario rígido.

- Reuniones: Las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.
- Presentaciones: El objetivo de las presentaciones es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

c. Valoraciones Delphi: La técnica Delphi es un instrumento de uso múltiple adecuada para MAGERIT que se utiliza con muy variados objetivos: Identificar problemas, desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles, identificar factores de resistencia en el proceso de cambio, establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector y contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.

1.4 MARCO LEGAL

Cada vez que se desee implementar un Sistema de Gestión de Seguridad de la Información, toda organización debe cumplir obligatoriamente con las leyes, normas y decretos aplicables en la consecución de los objetivos y desarrollo de actividades contenidas en un proyecto de este tipo.

“En lo que se refiere específicamente a Seguridad de la Información, algunas de las leyes y normas de la legislación colombiana tomadas de (Seguridad de la Información en Colombia, 2010)”[17]:

DECRETO 1377 DE 2013: “Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012”[18].

[17]SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea] Disponible en internet. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html. [citado mayo de 2014].

[18]DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado mayo de 2014].

LEY ESTATUTARIA 1581 DE 2012: "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional"[19].

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.
- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
- Crea una especial protección a los datos de menores de edad.
- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
- Crea el Registro Nacional de Bases de Datos.
- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

[19]LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado mayo de 2014].

DECRETO 2693 DE 2012: "Por el cual se establecen los lineamientos generales de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones"[20].

LEY 1341 DEL 30 DE JULIO DE 2009: "Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"[21].

LEY 1273 DEL 5 DE ENERO DE 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[22].

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008: "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[23].

LEY 603 DE 2000: "Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales"[24].

[20]DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado mayo de 2014].

[21]LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado mayo de 2014].

[22]LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado mayo de 2014].

[23]LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado mayo de 2014].

[24]LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado junio de 2014].

1.5 MARCO CONCEPTUAL

Enseguida se especifican algunos términos que serán citados y utilizados en el desarrollo del proyecto.

Activos de información: Los activos de información referentes a un nivel tecnológico, son todos los relacionados con los sistemas de información, redes, comunicaciones y la información en sí misma, Por ejemplo los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros[25].

Vulnerabilidad: Es una situación inherentes a los activos, o presente en su entorno, que facilita la materialización de las amenazas y las llevan a la condición de debilidad. Las vulnerabilidades son de diversos tipos como por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otras[26].

Amenaza: Es aquella situación que puede ocasionar resultados negativos en las operaciones cotidianas de la Unidad de Informática y Telecomunicaciones, generalmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas logran ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos[27].

Riesgo: Es aquel suceso que dificulta el cumplimiento de un objetivo de manera cuantitativa. Se puede considerar como una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva a dos tipos de consecuencias: Ganancias o pérdidas. Así mismo, el riesgo se plantea solamente como amenaza determinando el grado de exposición o el grado de una perdida (Por ejemplo el riesgo de que se pierdan los datos por el daño del disco duro, virus informáticos entre otros).

La organización internacional para la normalización (ISO), define riesgo tecnológico como:

"La probabilidad de que una amenaza se materialice, utilizando una vulnerabilidad existente de un activo o un grupo de activos, generándole pérdidas o daños"[28].

---

[25] POLITICAS DE SEGURIDAD DE ACTIVOS DE INFORMACION. [en línea] Disponible en internet: ww.utp.edu.com

[26] METODOLOGIA DEL ANALISIS DE RIESGO DE LA EMPRESA CASA DE LAS BETERIAS S.A DE C.V. [en línea] Disponible en internet: http://uplad.wikimedia.org

[27] EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado marzo de 2014].

[28] Ibíd.

Impacto: Es la consecuencia de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financieras, económicas, tecnológicas, físicas, entre otras[29].

Análisis de riesgos: Es un instrumento de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos mediante la identificación de sus elementos, lograr establecer el riesgo total y consecutivamente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos[30].

Probabilidad: Para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada[31].

Evaluación de riesgos: Este proceso incluye la medición del potencial de las pérdidas y la probabilidad de la pérdida, categorizando el orden de las prioridades[32].

Un conjunto de criterios puede ser usado para establecer una prioridad, enfocada en el impacto financiero potencial de las pérdidas, por ejemplo: riesgos críticos, que son todas las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota, riesgos importantes donde las exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones, riesgos no importantes que son las exposiciones a pérdidas que no causan un gran impacto financiero.

SGSI: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas *de Information Security Management System*. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización[33].

[29] Ibíd.
[30] Ibíd.
[31] Ibíd.
[32] Ibíd.
[33] Ibíd.

MAGERIT: La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Objetivos de control y riesgos: Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software.

Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran la conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.

Actividades de control: COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad; COSO discute los procedimientos y actividades de control utilizados en toda la entidad. COBIT clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente de procesamiento de información. SAC utiliza cinco esquemas de clasificación diferentes para los procedimientos de control de SI. COSO utiliza solo un esquema de clasificación para los procedimientos de control del sistema de información (SI). La discusión de COSO sobre las actividades de control enfatiza en quién realiza las actividades y en lo operativo más que en los objetivos de informes financieros. COSO también enfatiza la deseabilidad de integrar las actividades de control con la evaluación de riesgos.

Linux BackTrack: Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática[34].

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (*WhiteHat Knoppix*), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.Incluye una larga lista de herramientas de seguridad aptas para el uso, entre las que destacan numerosos escaneadores de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. Fue incluida en el puesto 7 de la famosa lista “Top 100 Network Security Tools” de 2006.

[34] BACKTRACK. [en línea] Disponible en internet: http://es.wikipedia.org/wiki/BackTrack. [citado junio de 2014].

SQLMAP: Es una herramienta desarrollada en PYTHON para realizar inyección de código SQL automáticamente. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web. Una vez que se detecta una o más inyecciones SQL en el host de destino, el usuario puede elegir entre una variedad de opciones entre ellas, enumerar los usuarios, los hashes de contraseñas, los privilegios, las bases de datos o todo el volcado de tablas y/o columnas específicas del DBMS (Sistema de gestión de base de datos), ejecutar su propio SQL SELECT, leer archivos específicos en el sistema de archivos y mucho más[35].

GOYSCRIPT WEP: Es un script de bash de Linux para poder realizar auditorías de redes WiFi con seguridad WEP (*Wired Equivalent Privacy*). Utilizado para encontrar debilidades en la clave de red de diferentes routers[36].

[35] SQLMAP HERRAMIENTOA AUTOMATICA DE LA INYECCION SQL. [en línea] Disponible en internet: www.dragonjar.org

[36] GOYSCRIPT (WEP, WPA Y WPS) [en línea] Disponible en internet: http//foro.seguridadwireless.net/live/wifislex/goyscriptwep-goyscripwap-y-goyscriptwps

2. METODOLOGÍA APLICADA

2.1 APOYO DE LA DIRECCIÓN

Uno de los principios fundamentales para iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la unidad. No sólo por ser un punto esencial contemplado en la norma sino porque el cambio de cultura yla concienciación que genera el proceso hacen necesario el impulso constante de la Dirección.

2.2 PLAN DE RECOLECCIÓN DE INFORMACIÓN

Una vez avalado el trabajo por parte de la Dirección, se procede con la recolección de toda la información necesaria para la consecución del proyecto.

Al final se conformó un inventario de activos actualizado y clasificado para cada una de las Áreas de la UIT:

Administración de sistemas: inventario conformado por 51 activos de información a proteger, entre los cuales se encuentran los principales servidores que alojan Sistemas de Información, el Portal web universitario, Bases de Datos, aplicaciones, etc. También el personal encargado de la administración del área, la sala de servidores, servicios y demás.

Administración de red de datos, internet y RENATA: inventario conformado por 37 activos de información a proteger, entre los que se encuentran los servidores por medio de los cuales se administra la Red de Datos, internet y RENATA, software para monitorización de la red, personal encargado de la administración del área y demás. Hay que aclarar que entre el área de Administración de Sistemas y el área de Administración de Red se comparten algunos activos de información como el servidor ORION y la sala de servidores.

Administración portal web: inventario conformado por 14 activos de información a proteger, entre los que se encuentran el servidor AKANE que lo administra el área de Sistemas pero al que también tiene acceso por FTP y SSH la Administradora del Portal web, ya que en este servidor está alojada la página web y demás portales de las diferentes dependencias y programas de la Universidad de Nariño que son de su responsabilidad. También se listan los equipos de escritorio, sus respectivos Sistemas Operativos y la oficina asignada para llevar a cabo las actividades de esta área.

Área de soporte y servicios tecnológicos: un inventario para la parte de Soporte Preventivo y otro inventario para la parte de Soporte Correctivo.

Soporte preventivo: inventario conformado por 12 activos de información a proteger, entre los que se encuentran el personal encargado de esta área, el Sistema de Información ASST para llevar un inventario de la Unidad de Informática y Telecomunicaciones, el Plan de mantenimiento preventivo de equipos de cómputo, ofimática y telecomunicaciones, etc.

Soporte correctivo: inventario conformado por 10 activos de información a proteger, entre los que se encuentran el personal encargado de esta área, el taller de soporte correctivo, la evaporadora de refrigeración para la sala de servidores, el Sistema de Alimentación Ininterrumpida (UPS), etc.

2.3 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Existen muchas metodologías de análisis y evaluación de riesgos aceptadas internacionalmente, la organización puede optar por una de ellas, hacer una combinación de varias o crear la propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla.

Por lo tanto la metodología que seutilizó fue MAGERIT ya que estando alineada con los estándares más conocidos para la gestión de riesgos como lo son ISO 27001 e ISO 31000, ofrece un método sistemático para analizar los riesgos derivados del uso de las Tecnologías de Información y Comunicaciones (TIC's), para así implementar los controles adecuados que permitan a una organización mitigarlos.

Esta metodología permite determinar el impacto sobre un activo de información, con la pérdida de confidencialidad, integridad y disponibilidad derivado de la materialización de las amenazas junto con las vulnerabilidades que pueden ser explotadas por esas amenazas, se determina la probabilidad de ocurrencia de dichas amenazas, se calcula el riesgo actual frente a las amenazas, y se determina el riesgo residual, resultante luego de que se implementen los controles.

Es necesario precisar que para efectos de este proyecto se determinó el riesgo residual **esperado**, ya que la implementación del Sistema de Gestión de Seguridad de la Información es decisión y responsabilidad de la Dirección de la Unidad de Informática y Telecomunicaciones.

El análisis de riesgos es una aproximación sistemática para determinar el riesgo siguiendo unos pasos:

2.3.1 Definición y valoración de activos de información. Por medio de un inventario conformado por los Activos de Información a proteger y cuyas dimensiones de valoración para cada uno de estos son: confidencialidad, integridad y disponibilidad.

2.3.2 Identificación de amenazas a que están expuestos los activos de información. Aquí se identifican y evalúan las amenazas que sufren los activos de información de la unidad. Se realizó la identificación de amenazas basándose en la clasificación de MAGERIT. (Ver **Tabla 15. Tipo de amenazas MAGERIT** en el Anexo J – Plantillas y tablas)

Cada una de las categorías presenta una serie de amenazas.(Ver **Tabla 16. Amenazas MAGERIT** en el Anexo J – Plantillas y tablas)

2.3.3 Identificación de vulnerabilidades existentes para los activos de información. Se identifican las vulnerabilidades que pueden ser explotadas por las amenazas potenciales por medio de inspección visual, listas de verificación, revisión de la información suministrada y *ethical hacking*.

2.3.4 Estimación del impacto. El objetivo es conocer el alcance del daño producido en la Unidad derivado de la materialización de las amenazas sobre los activos de información, mediante el uso de tablas de doble entrada para la obtención de resultados. (Ver **Tabla 13. Estimación del impacto** en el Anexo J – Plantillas y tablas)

2.3.5 Estimación de la probabilidad. El objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir. (Ver **Tabla 14. Estimación de la probabilidad** en el Anexo J – Plantillas y tablas)

2.3.6 Estimación del riesgo. La estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

Dicha estimación del riesgo se puede interpretar con mayor facilidad por medio de la utilización de la **Tabla 17. Mapa de riesgos** del Anexo J – Plantillas y tablas.

Con los resultados obtenidos en este análisis se procede a la evaluación de riesgos.

Para cada activo de información, el proceso concluye si el Nivel de Riesgo es aceptable, caso contrario, se define el tratamiento:

- Evitar: se evita el riesgo retirando el activo de información.
- Transferir: se transfiere el riesgo ejemplo por medio de un seguro.
- Mitigar: se reduce o mitiga el riesgo por medio de controles.

2.4 ANÁLISIS DE BRECHA

En esta etapa se determina la brecha con respecto al nivel de madurez de los requerimientos del estándar ISO/IEC 27001:2005 por medio de la verificación de los controles de seguridad de la información que se llevan a cabo en la Unidad.

Este proceso de diagnóstico junto con el análisis y evaluación de riesgos realizados anteriormente, hace posible la definición de nuevos controles para cada uno de los activos de información que lo requieran según su nivel de riesgo.

Al resultado de esta fase se le conoce como “Informe de análisis de riesgos”, que establece el modo de tratamiento y los controles necesarios para cada uno de los activos de información. Con este informe se elabora el “Plan de Tratamiento de Riesgos”.

2.5 GESTIÓN DE RIESGOS

2.5.1 Plan de tratamiento de riesgos. Contiene una serie de controles y recomendaciones básicas de seguridad para toda la organización que permita disminuir un alto grado de riesgo.

2.5.2 Establecer normativa para controlar el riesgo. La información es un activo que tiene valor para la comunidad universitaria y por consiguiente debe ser protegida y resguardada adecuadamente, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo así, a una mejor gestión de la universidad.

Por lo tanto, resulta necesario la elaboración de una Política de Seguridad de la Información que hagan parte de la cultura organizacional de la Universidad de Nariño y en este caso de la Unidad de Informática y Telecomunicaciones, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios

de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

2.5.3 Plan de implementación. Este plan incorpora todos los aspectos de la implementación del Sistema de Gestión de Seguridad de la Información, incluyendo estrategias descritas para lograr sus resultados, así como acciones de ejecución de las políticas que se diseñaron.

3. CONCLUSIONES

Con la aplicación de la norma ISO/IEC 27001 y 27002, se puede lograr un alto nivel de calidad en un proceso de seguridad de la información independientemente del tamaño y/o razón social de la organización, sin embargo, no hay garantía de seguridad absoluta puesto que siempre van a existir amenazas que vulneren las medidas de control adoptadas referentes a confidencialidad, integridad y disponibilidad de la información.

MAGERIT al presentar una guía completa y sistemática de cómo llevar a cabo el análisis de riesgos, facilita y acelera el proceso mediante la utilización de tablas de doble entrada; a diferencia de otras metodologías que utilizan formulas complejas que retardan los resultados en esta etapa.

Después de analizar la norma ISO/IEC 27001:2005 en conjunto con los niveles de madurez es posible determinar que cumpliendo la norma a un nivel GESTIONADO, se puede optar por la certificación.

4. RECOMENDACIONES

Organizar inventarios por áreas o dependencias que conforman la organización.

Revisar el Libro II – Catálogo de Elementos de MAGERIT que suministra una serie de tablas donde se indican las amenazas que pueden afectar determinados tipos de activos de información.

Ejecutar una evaluación de las políticas de seguridad de la información semestralmente, que posibilite mantenerse conforme a las necesidades de la Unidad de Informática y Telecomunicaciones mediante la aplicación de auditorías internas.

Apoyar la coordinación de acuerdo a la estructuración del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática y Telecomunicaciones, para posterior implementación del sistema por parte de los directivos de la Universidad de Nariño.

BIBLIOGRAFÍA

CADME, Christian y DUQUE, Diego. Auditoría de seguridad informática ISO 27001 para la empresa de alimentos “Italimentos CÍA. LTDA.”. Tesis previa a la obtención del título de Ingeniero de Sistemas. Cuenca. Ecuador: Universidad politécnica salesiana, 2012.

LLERENA, Rafael y GUERRA, José. Diagnóstico del estado de los SGSI con la aplicación de un software en las instituciones de Educación superior de san juan de Pasto. Tesis previa a la obtención del título de Ingeniero de Sistemas. Pasto. Colombia: Institución universitaria CESMAG, 2009.

UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES. Manual especifico de funciones y competencias laborales. Pasto: Universidad de Nariño, 2010.

NETGRAFIA

BACKTRACK. [en línea] Disponible en internet. http://es.wikipedia.org/wiki/BackTrack. [citado junio de 2014].

CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado marzo de 2014].

¿Cuál es el mejor estándar de administración de riesgo para las TI? [en línea] Disponible en internet. http://www.emb.cl/gerencia/articulo.mvc?xid=1301. [citado abril de 2014].

DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado mayo de 2014].

DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado mayo de 2014].

EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado marzo de 2014].

GOYSCRIPT (WEP, WPA Y WPS) [en línea] Disponible en internet: http//foro.seguridadwireless.net/live/wifislex/goyscriptwep-goyscripwap-y-goyscriptwps

ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado marzo de 2014].

LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado mayo de 2014].

LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado mayo de 2014].

LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado mayo de 2014].

LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado mayo de 2014].

LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado junio de 2014].

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [en línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf. [citado abril de 2014].

PARÁMETROS FUNDAMENTALES PARA LA IMPLANTACIÓN DE UN SGSI SEGÚN ISO 27001:2005. [en línea] Disponible en internet. http://www.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi. [citado marzo de 2014].

SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado abril de 2014].

SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea] Disponible en internet. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html. [citado mayo de 2014].

SQLMAP HERRAMIENTOA AUTOMATICA DE LA INYECCION SQL. [en línea] Disponible en internet: www.dragonjar.org

UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES. Proyecto UIT. Pasto: Universidad de Nariño, Aula de informática, 2009. [en línea] Disponible en internet. http://uit.udenar.edu.co/. [citado febrero de 2014]

ANEXOS

Los anexos del presente proyecto se encuentran almacenados en la carpeta general “ANEXOS” que acompaña este documento.

FAVOR REMITIRSE AL DOCUMENTO "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DENARIÑO"