DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE INFORMÁTICA, INGENIERÍA DE SISTEMAS Y TELEMÁTICA DE LA UNIVERSIDAD DE NARIÑO SOPORTADA EN LOS ESTÁNDARES MAGERIT E ISO/IEC 27001 Y 27002/2013

YEZID CAMILO GUERRERO ANGULO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2020

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE INFORMÁTICA, INGENIERÍA DE SISTEMAS Y TELEMÁTICA DE LA UNIVERSIDAD DE NARIÑO SOPORTADA EN LOS ESTÁNDARES MAGERIT E ISO/IEC 27001 Y 27002/2013

YEZID CAMILO GUERRERO ANGULO

Proyecto de grado presentado como requisito parcial para optar al título de Especialista en Seguridad Informática

Directora:
I.S. Esp. YENNY STELLA NUÑEZ ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2020

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en el trabajo de grado son responsabilidad exclusiva del autor”

AGRADECIMIENTOS

En primer lugar, a Dios por haberme guiado por el camino correcto durante estos años de posgrado, por fortalecerme, darme salud e iluminar mi mente en esos difíciles momentos y por ponerme en la vida a cada una de esas personas incondicionales que contribuyeron al desarrollo de este proyecto.

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

Un agradecimiento especial a la Ingeniera Yenny Stella Nuñez Alvarez, directora 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, Ingeniería de Sistemas y Telemática de la Universidad de Nariño por su cooperación y suministro de información, fundamental para cada una de las fases del proyecto.

DEDICATORIA

Dedico este proyecto de posgrado a Dios que me ha dado la vida y fortaleza para culminarlo. A mis 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 la especialización.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

INTRODUCCIÓN

Cada día las instituciones de educación superior reconocen la importancia de la información como uno de los activos más importantes que debe ser manejado eficientemente, para garantizar ventajas dentro del campo administrativo y académico competidos en la actualidad, por lo que 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 estas tecnologías para el manejo de la información son 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 27001:2013 de activos de información e ISO/IEC 27002:2013 de controles de seguridad.

Impulsados en lo anterior se presenta un proyecto enfocado en el diseño del Sistema de Gestión de Seguridad de la Información soportado en los estándares MAGERIT e ISO/IEC 27001 y 27002/2013 para la Unidad de Informática, Ingeniería de Sistemas y Telemática 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, Ingeniería de Sistemas y Telemática 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, Ingeniería de Sistemas y Telemática de la Universidad de Nariño, asegurando la integridad, confidencialidad y disponibilidad de la misma y con esto la mejora continua de la institución.

1. 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, integra 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, Ingeniería de Sistemas y Telemática 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 es fácilmente detectable y por lo tanto con solo poseerla y configurar el protocolo de internet, podemos 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.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de riesgos y la verificación de control de seguridad de la norma ISO 27001 e ISO 27002/2013 pueden mejorar la gestión de la seguridad de la información para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño?

2. JUSTIFICACIÓN

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 usuarios del sistema es preciso mejorarlos ya que actualmente, 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, Ingeniería de Sistemas y Telemática de la Universidad de Nariño tan fundamental hoy en día para lograr una utilización más eficiente y segura de la información.

También se beneficiarán los administradores y usuarios que hacen uso de los servicios informáticos y de la información que presta la Unidad de Informática, Ingeniería de Sistemas y Telemática, 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 las dependencias de la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño deciden implementar los controles y recomendaciones producto del 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 el diseño de un Sistema de Gestión de Seguridad de la Información soportado en la norma ISO 27001 e ISO 27002/2013 para la Unidad de Informática, Ingeniería de Sistemas y Telemática 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 aulas, departamentos y unidades.

3. OBJETIVOS

3.1 Objetivo general

Diseñar el Sistema de Gestión de Seguridad de la información mediante la aplicación del proceso de análisis de riesgos y la verificación de controles de seguridad soportado en la norma ISO 27001 y 27002 para la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño.

3.2 Objetivos específicos

- Planear el proceso de recolección de la información de los activos, servicios y procesos que presta la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño a toda la Institución.
- Identificar, Analizar y Evaluar los riesgos, vulnerabilidades y amenazas presentes en la Unidad de Informática, Ingeniería de Sistemas y Telemática 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 a la norma para hacer un análisis de los controles que deberían implantarse en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño.
- Estructurar el Sistema de Gestión de Seguridad de la Información para la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño incluyendo los controles de seguridad en las políticas, procesos y procedimientos.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES DE INVESTIGACIÓN

Los proyectos sobre sistemas de seguridad de la información en Nariño son relativamente nuevos 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.""**. 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, el cual 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".** 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.

De este proyecto se tomará como ejemplo los formatos de reportes que arroja el sistema y también se utilizaran 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 la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño**.**

El proyecto desarrollado bajo mi autoría y la del ingeniero Robert Marcelo Tabango Goyes para la Universidad de Nariño – Sede Pasto (Colombia) denominado: "**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002/2005 PARA LA UNIDAD DE**

INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO".
En la Universidad de Nariño a partir del año 2011 se empezó a desarrollar el proyecto basándonos en la última versión de la norma que en aquella época era la 2005. Por lo tanto, junto con los directivos e ingenieros de la unidad se decide actualizar el proyecto soportado en la reciente versión 2013 la cual contiene nuevos dominios, objetivos de control y controles.

4.2 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.

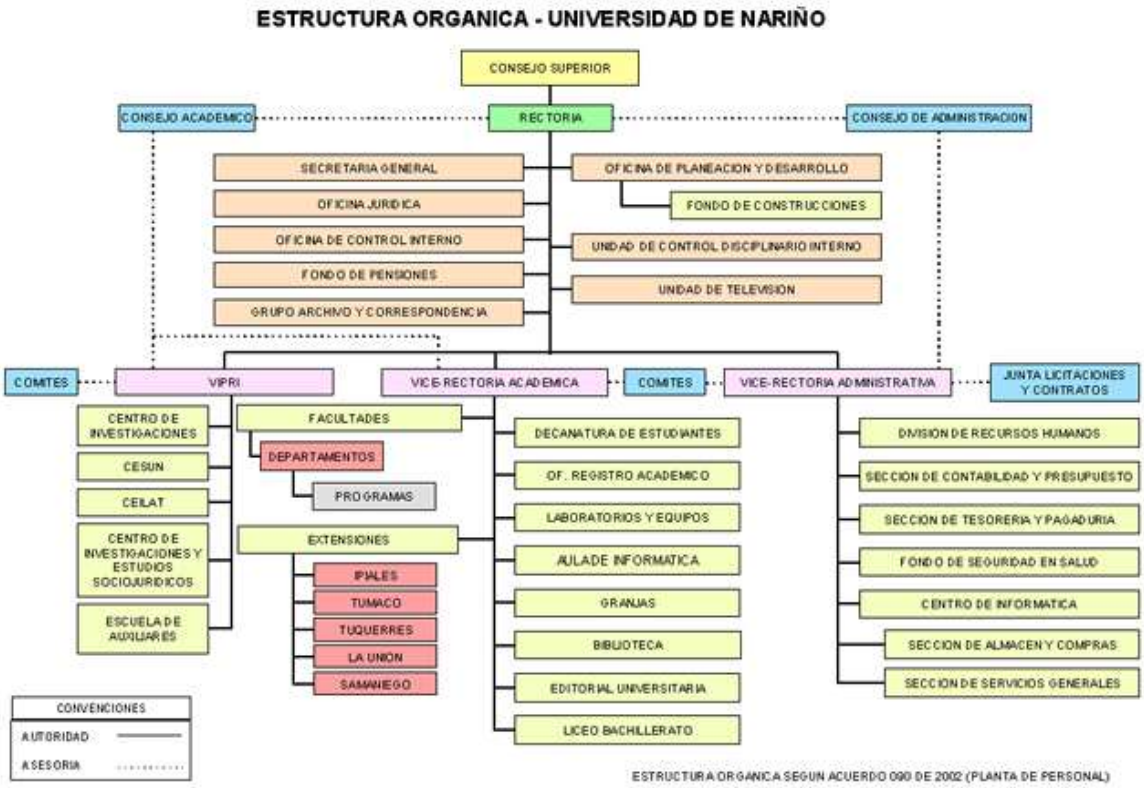
Los niveles de educación que se ofrecen en la Universidad de Nariño comprenden desde transición hasta último grado de bachillerato, programas de pregrado, diplomados, especializaciones, maestrías y doctorados. Todos sus programas cuentan con registro calificado y varios de ellos con acreditación en alta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

Figura 1. Estructura Orgánica - Universidad de Nariño



Fuente: Disponible en internet. http://uit.udenar.edu.co/.

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.

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, Ingeniería de Sistemas y Telemática de la Universidad de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001/2013.
- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño.

- Verificación de controles de seguridad de la información que se llevan a cabo en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño teniendo en cuenta la norma ISO 27002/2013.
- Estructuración del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática, Ingeniería de Sistemas y Telemática 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.

4.2.1. Estructura organizacional. La Unidad de Informática, Ingeniería de Sistemas y Telemática 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.

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

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

Fuente: Disponible en internet. http://uit.udenar.edu.co/.

a. Administración de sistemas: El Aula de Informática de la Universidad de Nariño tiene 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 nuestra 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 con 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 Power Edge R815	Idiomasra: S.I que lo manejan el Centro de Idiomas: Matriculas.	Sistemas basados en Apache: Portal Web Universitario, portales de Dependencias / Programas. Las Bases de Datos en MySQL y Postgres que 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, AntiSpam SpamAssassin, 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

Tabla 1. (Continuación).

NOMBRE DEL SERVIDOR	SISTEMA DE INFORMACIÓN (S.I)	SERVICIO	FRECUENCIA DE ACTUALIZACIÓN
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 Power Edge 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 Information Services.	
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.	
	Limesurvey: Servidor de encuestas online.		Al liberar actualizaciones el fabricante
ENCUESTAS – HP ML 110	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

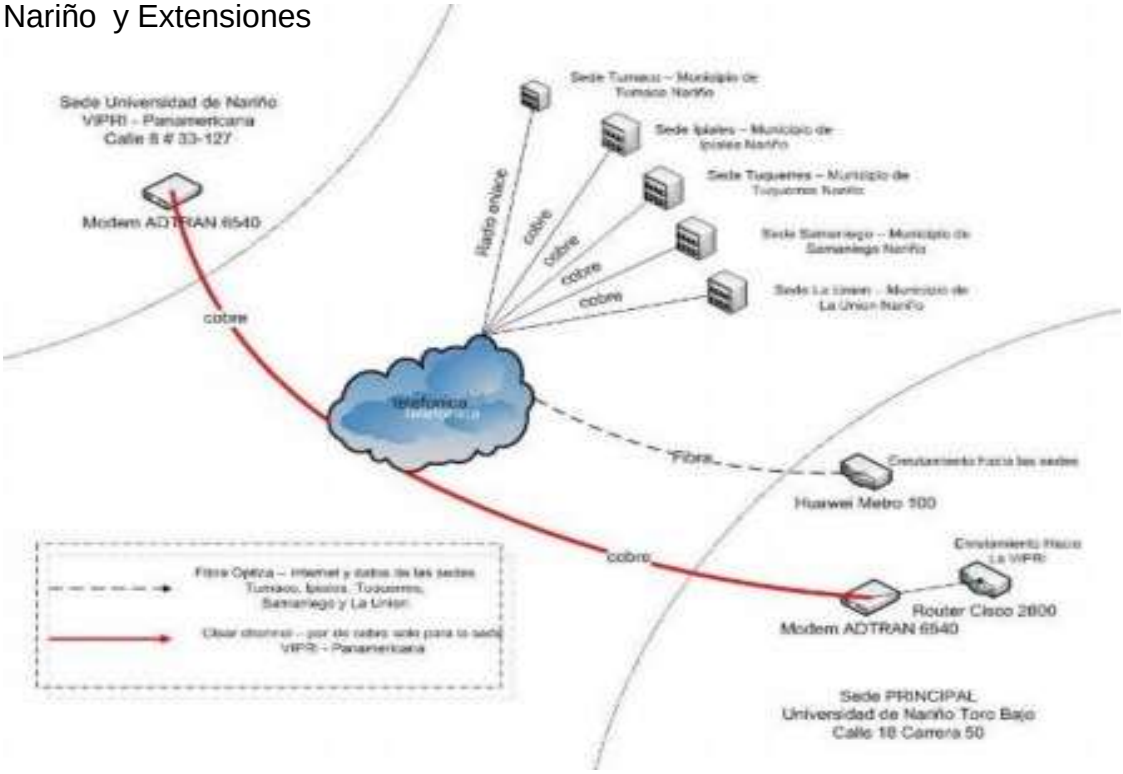
Procedimientos Administración Centro de datos: El objetivo del área es mantener actualizadas, aseguradas y en óptimo funcionamiento las plataformas de infraestructura tecnológica de servidores y Sistemas de Información de la universidad para brindar el mejor servicio posible a la comunidad académica 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 con su competencia, en el desarrollo de los planes estratégicos e informáticos de la Universidad, modernización tecnológica.

b. Administración red de datos e internet: Comprende 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 Extensiones



Fuente: Disponible en internet. http://uit.udenar.edu.co/.

En el cual se puede observar cada uno de los subnodos 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 nos 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.

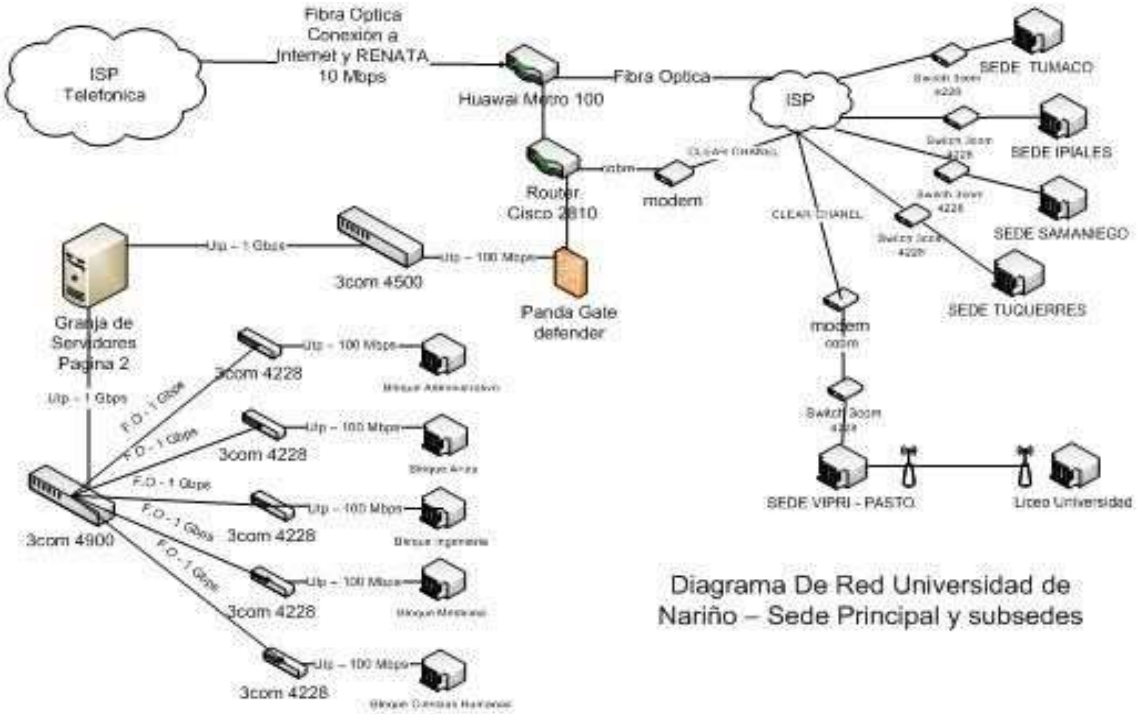
- Para interconectar a la sede de la VIPRI utilizamos como equipo enrutador un Cisco 2600 el cual va directamente conectado a un Modem Adtran 2000x, en enlace de las dos sedes se realiza a través de un clear channel que usa como medio de transmisión cobre, igualmente en el VIPRI existe un Modem Adtran

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 contamos con dos antenas Cisco Aironet 1300 las cuales sirven para enlazar a la VIPRI con el Liceo a través de una conexión wifi, igualmente en el Liceo contamos 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 tenemos como equipo enrutador un Huawai metro 100, en cada una de las sedes tenemos 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.



Fuente: Disponible en internet. http://uit.udenar.edu.co/.

En el diagrama 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, para la se 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 juego 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 CS.

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.

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.

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 unidad 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. (ver tablas 2-6)

4.2.2 Funciones personal UIT:

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, Ingeniería de Sistemas y Telemática
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.
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. 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 con 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.

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, Ingeniería de Sistemas y Telemática
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 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.

Tabla 3. (Continuación)

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.

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 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.

Tabla 4. (Continuación)

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.

Tabla 5. Funciones - Administrador de Sistemas

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador Centro de Datos**
No. de Cargos:	Uno (1)
Dependencia:	Aula de informática
Cargo del Jefe Inmediato:	**Director Aula de Informática**

II. PROPÓSITO 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.

Tabla 5. (Continuación)

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 con 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.

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.

Tabla 6. (Continuación)

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 con su competencia en el desarrollo de los planes 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.

4.3 MARCO TEÓRICO

4.3.1. 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" [1].

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[2].

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 utilización del 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.

[1] 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 febrero de 2018].

[2] CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado febrero de 2018].

4.3.2. 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" [3].

Una adecuada gestión de la seguridad de la información (El portal de ISO 27001, 2012) 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 existen 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.

Origen: Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, 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. Su última versión es la 2013.

[3] EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado febrero de 2018].

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:

4.3.3. 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 27002:2013, 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 2013 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 35 objetivos de control y 114 controles, agrupados en 14 dominios" [4]. (El anexo de ISO 27001 en español) (ver figura 5)

Figura 5.Dominios ISO 27002

Fuente: Disponible en internet.
https://portal.aenormas.aenor.com/revista/309/ciberseguridad2-2-309.html

[4] ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado febrero de 2018].

A5 Políticas

5.1 Directrices de la Dirección en seguridad de la información: La gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

A6 Organización

6.1 Organización interna: La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

6.2 Dispositivos para movilidad y teletrabajo: La protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo.

A7 Recursos humanos

7.1 Antes de la contratación: Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.
7.2 Durante la contratación: Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.

A8 Activos

8.1 Responsabilidad sobre los activos: Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.

8.2 Clasificación de la información: Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

8.3 Manejo de los soportes de almacenamiento: Los medios deberían ser controlados y físicamente protegidos.

A9 Accesos

9.1 Requisitos de negocio para el control de accesos: Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los

procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

9.2 Gestión de acceso de usuario: Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

9.3 Responsabilidades del usuario: La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

9.4 Control de acceso a sistemas y aplicaciones: Los medios deberían ser controlados y físicamente protegidos.

A10 Cifrado

10.1 Controles criptográficos: Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

A11 Física y ambiental

11.1 Áreas seguras: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

11.2 Seguridad de los equipos: Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

A12 Operativas

12.1 Responsabilidades y procedimientos de operación: Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados.

12.2 Protección contra código malicioso: El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

12.3 Copias de seguridad: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

12.4 Registro de actividad y supervisión: Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

12.5 Control del software en explotación: Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

12.6 Gestión de la vulnerabilidad técnica: Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

12.7 Consideraciones de las auditorías de los sistemas de información: Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde este proceso.

A13 Telecomunicaciones

13.1 Gestión de la seguridad en las redes: Se deberían controlar los accesos a servicios internos y externos conectados en red.

13.2 Intercambio de información con partes externas: Se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente.

A14 Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1 Requisitos de seguridad de los sistemas de información: El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

14.2 Seguridad en los procesos de desarrollo y soporte: Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

14.3 Datos de prueba: Se debería evitar la exposición de datos sensibles en entornos de prueba.

A15 Suministradores

15.1 Seguridad de la información en las relaciones con suministradores: La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.

15.2 Gestión de la prestación del servicio por suministradores: La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.

A16 Incidentes

16.1 Gestión de incidentes de seguridad de la información y mejoras: Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.

A17 Continuidad del negocio

17.1 Continuidad de la seguridad de la información: Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

17.2 Redundancias: Se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes.

A18 Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales: El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

18.2 Revisiones de la seguridad de la información: Se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

- ***ISO/IEC 27003****: Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.*

- ***ISO/IEC 27004****: Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.*
- ***ISO/IEC 27005****: Publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.*
- ***ISO/IEC 27006****: Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.*
- ***ISO/IEC 27007****: Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.*
- ***ISO/IEC TR 27008****: Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.*
- ***ISO/IEC 27009****: En estado de desarrollo. No certificable. Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte.*
- ***ISO/IEC 27010****: Publicada el 20 de octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.*
- ***ISO/IEC 27011****: Publicada el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005.*
- ***ISO/IEC 27013****: Publicada el 15 de octubre de 2012. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).*
- ***ISO/IEC 27014****: Publicada el 23 de abril de 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.*
- ***ISO/IEC TR 27015****: Publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.*
- ***ISO/IEC TR 27016****: En fase de desarrollo, con publicación prevista en 2014. Consistirá en una guía de valoración de los aspectos financieros de la seguridad de la información.*
- ***ISO/IEC TS 27017****: En fase de desarrollo, con publicación prevista en 2014. Consistirá en una guía de seguridad para Cloud Computing.*

- ***ISO/IEC 27018****: En fase de desarrollo, con publicación prevista en 2014. Consistirá en un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.*
- ***ISO/IEC TR 27019****: Publicada el 17 de Julio de 2013. Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.*
- ***ISO/IEC 27031****: Publicada el 01 de marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.*
- ***ISO/IEC 27032****: Publicada el 16 de Julio de 2012. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.*
- ***ISO/IEC 27033****: Parcialmente desarrollada. Norma dedicada a la seguridad en redes.*
- ***ISO/IEC 27034****: Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas.*
- ***ISO/IEC 27035****: Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información.*
- ***ISO/IEC 27036****: En fase de desarrollo, con publicación prevista a partir de 2013. Consistirá en una guía en cuatro partes de seguridad en las relaciones con proveedores.*
- ***ISO/IEC 27037****: Publicada el 15 de octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.*
- ***ISO/IEC 27038****: En fase de desarrollo, con publicación prevista en 2014. Consistirá en una guía de especificación para seguridad en la redacción digital.*
- ***ISO/IEC 27039****: En fase de desarrollo, con publicación prevista en 2014. Consistirá en una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).*
- ***ISO/IEC 27040****: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la seguridad en medios de almacenamiento.*
- ***ISO/IEC 27041****: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.*

- ***ISO/IEC 27042****: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía con directrices para el análisis e interpretación de las evidencias digitales.*
- ***ISO/IEC 27043****: En fase de desarrollo, con publicación prevista no antes de 2014. Desarrollará principios y procesos de investigación.*
- ***ISO/IEC 27044****: En fase de desarrollo, con publicación prevista no antes de 2014. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).*
- ***ISO 27799****: Publicada el 12 de junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.*

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)" [5].

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

[5] PARÁMETROS FUNDAMENTALES PARA LA IMPLANTACIÓN DE UN SGSI SEGÚN ISO 27001:2013. [en línea] Disponible en internet. http://www.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi. [citado febrero de 2018].

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.

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 continuo 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 a niveles 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 continua PHVA (Véase Figura 6).

Figura 6.Ciclo PHVA

Fuente: Disponible en internet. 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, auditoría 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 27001:2013, 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 (14) dominios, denominados A5 hasta A18:

A5	Políticas
A6	Organización
A7	Gestión de Recursos
A8	Activos
A9	Accesos
A10	Cifrado
A11	Física y ambiental
A12	Operativas
A13	Telecomunicaciones
A14	Adquisición, desarrollo y mantenimiento
A15	Suministradores
A16	Incidentes
A17	Continuidad del negocio
A18	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 siguiente tabla:

Tabla 7. Escala nivel de madurez COBIT

ESCALA	%	DESCRIPCIÓN
No Aplica	N/A	No aplica.
Inexistente	0	**Falta de un proceso reconocible.** La Organización no ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	Se evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. **Sin embargo, no hay procesos estandarizados.** La implementación de un control depende de cada individuo y es muchas veces es **reactiva.**
Repetible	40	**Los procesos y los controles siguen un patrón regular.** Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. Pero **no están formalizados, ni hay comunicación formal** sobre los procedimientos desarrollados. Hay un alto grado de confianza en los conocimientos de cada persona.
Definido	60	**Los procesos y los controles se documentan y se comunican.** No se han establecido mecanismos de monitoreo, para una detección de desviaciones efectiva.
Gestionado	80	Los controles se monitorean y se miden. Es posible **monitorear y medir el cumplimiento de los procedimientos** y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de **mejores prácticas**, basándose en los resultados de una **mejora continua**.

- 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 requiere definir un proceso para identificar los riesgos más significativos, en oposición a los riesgos de bajo impacto, baja frecuencia o alto costo de control de este. Para este proyecto se decidió utilizar 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" [6].

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 Audit and Control Association) y el IT Governance Institute, tiene una serie de recursos

[6] SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado febrero de 2018].

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" [7].

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 2019, 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" [8].

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.

[7] ¿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 febrero de 2018].
[8] 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 febrero de 2018].

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*".

***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" [9].

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: (ver tabla 8)

Tabla 8. Tipo de amenazas MAGERIT

TIPO DE AMENAZA	DESCRIPCIÓN
[N] Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Fallos deliberados causados por las personas.

[9] Ibíd.

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[10]:

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. (ver tablas 9-12)

Tabla 9. Tipos de activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, etc.
[HW] Hardware / Equipos informáticos	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
[M] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[10] Ibíd.

Tabla 9. (Continuación)

[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Personal relacionado con los sistemas de información.
[SI] Sistema de Información	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información para apoyar la toma de decisiones y el control en una organización.

Tabla 10. Dimensiones de valoración de un activo

CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION**
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso Interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	**INTEGRIDAD**	**DESCRIPCION**
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	**DISPONIBILIDAD**	**DESCRIPCION**
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Tabla 11. Valoración cualitativa

CÓDIGO	VALOR ACTIVO	DESCRIPCIÓN (Clasificación de información)
MA	Muy Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja
MB	Muy Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Baja

Tabla 12. Valoración cuantitativa

CÓDIGO	VALOR ACTIVO	VALOR	DESCRIPCIÓN
MA	Muy Alto	5	$5.000.001 o más
A	Alto	4	$3.001.000 a $5.000.000
M	Medio	3	$1.501.000 a $3.000.000
B	Bajo	2	$501.000 a $1.500.000
MB	Muy Bajo	1	0 a $500.000

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 análisis y gestión de riesgos" [11].

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.

Estimación del impacto: Se puede calcular el impacto en base a tablas sencillas de doble entrada: (ver tabla 13)

Tabla 13. Estimación del impacto

IMPACTO		***Degradación***		
		1%	50%	100%
Valor del activo	Muy Alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Degradación: Que tan perjudicado resulta el activo de información, debido a la materialización de las amenazas:

- 100%: Degradación total o muy considerable del activo

[11] Ibíd.

- 50%: Degradación medianamente considerable del activo
- 1%: Degradación poco considerable del activo

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.
Mayor (5): Impacta en la operatividad de los procesos.
Moderado (3): Impacta en la operatividad del macroproceso.
Menor (2): Impacta en la operatividad del proceso.
Insignificante (1): Impacta levemente en la operatividad del proceso

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)

Tabla 14. Estimación de la probabilidad

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

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 15-18)

Tabla 15. Estimación del riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	**5**	**5**	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	**5**	8
		1	**2**	**3**	**5**	**8**
		Impacto				

Tabla 16. Nivel de riesgo

	Nivel de Riesgo
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Tabla 17. Nivel de aceptación / tolerancia

Aceptable	Retenido.
Tolerable	Para activos no críticos, y tratado como intolerable en caso de críticos.
Intolerable	Atención inmediata y monitoreo permanente.
Extremo	Tratado en forma similar al intolerable, pero a nivel de Gerencia General.

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 P*lan de tratamiento de riesgos*.

Tabla 18. Tratamiento del riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Finaliza el proceso.
Tolerable Intolerable Extremo	Una de las tres opciones: a. Se transfiere el riesgo por ejemplo tomando un seguro. b. Se evita el riesgo retirando el activo de información. c. Se reduce o mitiga el riesgo por medio de controles.

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 apropiado e 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 y por tanto permite identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y por tanto 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 en estudio sobre ejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúan para 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.

4.4 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)" [12]:

DECRETO 1377 DE 2013: Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012"[13].

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" [14].

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.

[12] 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 febrero de 2018].
[13] DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [febrero de 2018].
[14] LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado febrero de 2018].

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.

DECRETO 2693 DE 2012: (MinTics, 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" [15].

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" [16].

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

[15] DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado febrero de 2018].
[16] LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado febrero de 2018].

las tecnologías de la información y las comunicaciones, entre otras disposiciones" [17].

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" [18].

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" [19].

4.5 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.[20]

Vulnerabilidad: Es unas situaciones 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.[21]

Amenaza: Es aquella situación que puede ocasionar resultados negativos en las operaciones cotidianas de la Unidad de Informática y Telecomunicaciones,

[17] LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado febrero de 2018].
[18] LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado febrero de 2018].
[19] LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado febrero de 2018].
[20] POLÍTICAS DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN. [en línea] Disponible en internet. http://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/politicas_sgsi.pdf. [citado febrero de 2018].
[21] METODOLOGIA DE ANALISIS DE RIESGO DE LA EMPRESA LA CASA DE LAS BATERIAS S.A DE C.V. [en línea] Disponible en internet. http://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf. [citado febrero de 2018].

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.[22]

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"[23].

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.[24]

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.[25]

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.[26]

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.

---

[22] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado febrero de 2018].
[23] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado febrero de 2018].
[24] Ibíd.
[25] Ibíd.
[26] Ibíd.

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.[27]

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.[28]

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.[29]

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.[30]

Actividades de Control: COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad; COSO discute los

---

[27] Ibíd.

[28] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado febrero de 2018].

[29] MAGERIT. [en línea] Disponible en internet. https://seguridadinformaticaufps.wikispaces.com/MAGERIT. [citado febrero de 2018].

[30] COMPARACIÓN DE CONTROLES INTERNOS: COBIT, SAC Y COSO. [en línea] Disponible en internet. http://www.netconsul.com/riesgos/cci.pdf. [citado febrero de 2018].

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.[31]

Linux BackTrack: Es una distribución GNU/Linux en formato Live CD 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.

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. [32]

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.[33]

[31] Ibíd.

[32] BACKTRACK. [en línea] Disponible en internet. http://es.wikipedia.org/wiki/BackTrack. [citado febrero de 2018].

[33] SQLMAP – HERRAMIENTA AUTOMÁTICA DE INYECCIÓN SQL. [en línea] Disponible en internet. http://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml. [citado febrero de 2018].

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.[34]

[34] GOYSCRIPT (WEP, WPA & WPS). [en línea] Disponible en internet. http://foro.seguridadwireless.net/live-wifislax/goyscriptwep-goyscriptwpa-y-goyscriptwps/. [citado febrero de 2018].

5. DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 APOYO DE LA DIRECCIÓN DE LA UNIDAD DE INFORMÁTICA, INGENIERÍA DE SISTEMAS Y TELEMÁTICA DE LA UNIVERSIDAD DE NARIÑO

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 y la concienciación que genera el proceso hacen necesario el impulso constante de la Dirección. Por tal razón se realizó una reunión previa en la que se confirmó el apoyo por parte de la dirección y los administradores de la unidad para el suministro de información, ingreso a las instalaciones de la unidad y demás actividades necesarias para la consecución del proyecto.

5.2 ALCANCE DEL PROYECTO

El alcance de proyecto incluye:

- Definición de los activos en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001/2013.
- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño.
- Verificación de controles de seguridad de la información que se llevan a cabo en la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño teniendo en cuenta la norma ISO 27002/2013.
- Estructuración del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática, Ingeniería de Sistemas y Telemática 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.

Los dominios, objetivos de control y controles que contempla la norma ISO 27002 son:

- Políticas
- Organización
- Recursos humanos
- Activos

- Accesos
- Cifrado
- Física y ambiental
- Operativas
- Telecomunicaciones
- Adquisición, desarrollo y mantenimiento
- Suministradores
- Incidentes
- Continuidad del negocio
- Cumplimiento

5.3 PLAN DE RECOLECCIÓN DE INFORMACIÓN

5.3.1. Información y documentación solicitada. A continuación, se describe la información y documentación solicitada y suministrada por parte de la unidad: (ver tabla 19)

Tabla 19. Información y documentación solicitada

DOCUMENTO	DESCRIPCION
Políticas de seguridad	Documento donde se plantea toda la normativa que deben seguir los funcionarios de la Unidad. El documento debe considerar aspectos generales y específicos sobre acceso a la información, responsabilidad y manejo de activos de información, procedimientos a seguir cuando se presente un incidente de seguridad. Nota: La Unidad de Informática, Ingeniería de Sistemas y Telemática no posee un documento de políticas de seguridad y controles. El documento suministrado y que más se asemeja es el: "REGLAMENTO Y POLÍTICAS DE USO DEL CORREO ELECTRONICO, SISTEMA UNIFICADO DE COMUNICACIÓN INTERNA, PORTAL WEB, RED DE DATOS E INTERNET Y SERVICIO DE SOPORTE TECNOLOGICO DE LA UNIVERSIDAD DE NARIÑO".
Manual de funciones y competencias laborales	La unidad facilitó el manual en el que se detallan las funciones esenciales de cada funcionario, desde el director hasta el último empleado y los resultados o criterios de desempeño esperados para cada cargo.
Procesos y procedimientos	La unidad proporcionó una serie de documentos que contienen diagramas de flujo, los cuales describen las actividades y su secuencia requerida en la realización de los procedimientos de la unidad. Además, incluyen

Tabla 19. (Continuación)

	objetivo, alcance y responsables que intervienen en el procedimiento. Los procedimientos son los siguientes: - AUI-GEC-PR-01: Publicación de información en la página web institucional. - AUI-GEC-PR-02: Creación de página web de unidades adscritas a la UDENAR. - AUI-REF-PR-01: Distribución de espacios físicos Aula de Informática. - AUI-SPM-PL-01: Plan de mantenimiento preventivo de equipo de cómputo, ofimática y telecomunicaciones. - AUI-SPM-PR-02: Servicio de mantenimiento correctivo y preventivo de hardware y software. - AUI-SPM-PR-03: Asesoría de servicio eléctrico. - AUI-SPM-PR-04: Desarrollo de cursos de lenguaje y herramientas informáticas. - AUI-SPM-PR-05: Administración servicio RENATA. - AUI-SPM-PR-09: Administración Bases de Datos. - AUI-SPM-PR-12: Cableado estructurado.
Inventario de activos	Cada administrador de la unidad suministró un inventario de su área de responsabilidad, en el que se recopilan los principales activos del área por medio de los cuales es posible la prestación de los servicios.
Portafolio de servicios	Disponible en la página web de la Unidad de Informática y Telecomunicaciones: http://akane.udenar.edu.co/siweb/ainfo/#home Contempla información general acerca de los servicios que presta cada área hacia las diferentes unidades académicas y administrativas de la Universidad de Nariño y a sus estudiantes.
Registro de problemas e incidentes	Información detallada acerca de un incidente, junto con su historial desde su registro hasta su resolución. Nota: La Unidad de Informática y Telecomunicaciones no posee documentos de registros de incidencias y problemas.

Tabla 19. (Continuación)

	Se proporcionó un conjunto de formatos que administran los empleados de la unidad dependiendo de sus funciones y responsabilidades. Los principales formatos son los siguientes: - AUI-GEC-FR-01: Registro de capacitación Portal Web. - AUI-GEC-FR-02: Información publicada en el Portal Web. - AUI-SPM-FR-02: Formato para mantenimiento de equipos. - AUI-SPM-FR-03: Préstamo de quipos. - AUI-SPM-FR-08: Redes y telecomunicaciones. - AUI-SPM-FR-10: Mantenimiento preventivo dependencias. - AUI-SPM-FR-11: Hoja de vida equipo. - AUI-SPM-FR-12: Servicios RENATA. - AUI-SPM-FR-14: Mantenimiento preventivo. - AUI-SPM-FR-15: Hoja de vida de equipos de redes y telecomunicaciones. - CNF-GIT-FR-07: Hoja de vida de mantenimiento de equipos de cómputo.
Hoja de vida equipos de computo	Formato que proporciona el historial de mantenimiento y cambios en los equipos esenciales de la Unidad de Informática y Telecomunicaciones. Hace referencia a los formatos: AUI-SPM-FR-11, AUI-SPM-FR-15 y CNF-GIT-FR-07.

5.3.2. Entrevista al personal responsable de los recursos informáticos y la información. Se llevaron a cabo una serie de entrevistas libres con cada uno de siguientes funcionarios:

- Administrador Centro de Datos
- Administrador Red de Datos
- Administrador Portal Web
- Administrador Área de Soporte y Servicios Tecnológicos: Mantenimiento preventivo
- Administrador Área de Soporte y Servicios Tecnológicos: Mantenimiento correctivo

Por medio de las cuales se pregunto acerca de la seguridad de la información relativo a gestión de activos, seguridad física, control de acceso (lógico), proceso de contratación del personal, cumplimiento y supervisión de las monitorias, licenciamiento software, funciones y características de los servidores, software y sistemas de información alojados en los servidores, copias de seguridad, etc.

Además, se aclararon interrogantes que surgieron de la revisión de la información y documentación suministrada, ya que estaba incompleta o se requería de una aclaración por parte del administrador.

5.4 ANÁLISIS Y EVALUACIÓN DE RIESGOS

5.4.1 Metodología de 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 se utilizó 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 se basa en analizar el impacto de una violación de seguridad sobre la organización, determinando las amenazas que pueden afectarla junto con las vulnerabilidades que pueden ser explotadas por esas amenazas, permitiendo así una clara identificación de controles y salvaguardas apropiados.

MAGERIT, está conformado por tres libros: El primero es el Método, en el que se describe la estructura del análisis y de la gestión de riesgos.

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

- Definir los activos de información importantes para la organización.
- Definir las amenazas y vulnerabilidades existentes para los activos de información seleccionados.
- Verificar los controles de seguridad de la información que se llevan a cabo en la organización.
- Estimar el impacto sobre un activo de información derivado de la materialización de una amenaza.
- Estimar el riesgo (Riesgo = Probabilidad x Impacto).

El segundo es un Catálogo de Elementos que 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. Y por último una Guía de Técnicas y ejemplos de cómo llevar a cabo el análisis de riesgos por medio de tablas, algoritmos, arboles de ataque, técnicas gráficas, etc. Este documento de técnicas convierte está metodología en un factor diferenciador con respecto a otras metodologías.

MAGERIT es muy útil para las organizaciones que inician con la gestión de seguridad de la información, porque permite enfocar esfuerzos en los riesgos que pueden ser más críticos.

6. DEFINICIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN A PROTEGER

Se formalizó un inventario de activos de información, el cual se puede consultar en su totalidad en la carpeta ***ANEXO A – INVENTARIO ACTIVOS DE INFORMACIÓN***. En la Tabla 20 se encuentran apartes del inventario en el que se definen y valoran los principales activos de información que conforman el Área de Administración de Sistemas. (ver tabla 20)

Tabla 20. Inventario parcial Área Administración Centro de Datos

ID	ACTIVO	CANT	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
UIT-AS-A-01	Administrador Centro de Datos	1	P	Uso Interno	Normal	Muy Alta	**Muy Alto**	**5**	…	…
UIT-AS-A-02	**Servidor Akane - Dell PowerEdge R815**	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-04	Código fuente Portal Web Universitario, Portales Dependencias/Programas.		D	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Portal Web
UIT-AS-A-05	Portal Web Universitario	1	SI	Uso Público	Sensible	Muy Alta	**Alto**	**4**	Coordinador UIT	Administrador Portal Web
UIT-AS-A-15	**Servidor Sindamanoy - Sun V40Z**	1	HW	Confidencial	Sensible	Alta	**Alto**	**4**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-18	**Servidor Mail - Dell PowerEdge R810**	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-20	Correo Electrónico institucional		S	Uso Interno	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-22	Base de datos Correo Electrónico Institucional		D	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-23	**Servidor Arthas – Sun V40Z**	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-25	Comunicaciones Unificadas (Lync Server 2010)		S	Uso Interno	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-26	**Servidor Conferencias - Dell PowerEdge 2850**	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-28	Servicio Livemeeting y de comunicaciones (Livemeeting y Office		S	Uso Interno	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos

ID	ACTIVO	CANT	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
	Comunications Server 2007)									
UIT-AS-A-29	**Servidor Vacunas – Proliant ML 110**	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-31	**Servidor Virtual – HP Proliant DL 380 G5**	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-35	**Servidor Jupiter – Dell PowerEdge 2800**	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-37	Internet Information Services: Páginas informativas obsoletas	1	SW	Confidencial	Baja	Baja	**Muy Bajo**	**1**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-38	**Servidor Orion – HP Proliant DL 380 G5 (Capus Central)**	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Red de Datos y Administrador Centro de Datos
UIT-AS-A-40	Analizador de acceso a la red SARG	1	SW	Confidencial	Normal	Media Baja	**Medio**	**3**	Coordinador UIT	Administrador Red de Datos
UIT-AS-A-41	**Servidor Encuestas - HP ML 110**	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-45	Monitor	2	P	Uso Interno	Baja	Media	**Medio**	**3**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-46	Oficina Administración Centro de Datos	1	L	Uso Interno	Sensible	Alta	**Alto**	**4**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-47	Sala de servidores	1	L	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Coordinador UIT	Administrador Centro de Datos
UIT-AS-A-50	Unidad LTO 5	1	Media	Confidencial	Sensible	Media Baja	**Alto**	**4**	Coordinador UIT	Administrador Centro de Datos

ID	ACTIVO	CANT	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
CNF-GIT-FR-07	Formato Mantenimiento servidores	1	Media	Confidencial	Normal	Media Baja	**Medio**	**3**	Coordinador UIT	Administrador Centro de Datos

El tipo de activo corresponde a la clasificación que presenta la metodología MAGERIT: (ver tabla 21)

Tabla 21. Tipo de activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, etc.
[HW] Hardware / Equipos informáticos	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
[M] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Personal relacionado con los sistemas de información.
[SI] Sistema de Información	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información para apoyar la toma de decisiones y el control en una organización.

Como ya se mencionó anteriormente, la seguridad de la información, según ISO 27001/2013, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento; por tal razón, las dimensiones de valoración de un activo que se utilizaron se describen a continuación: (ver tabla 22)

Tabla 22. Dimensiones de valoración de un activo

CODIGO	CONFIDENCIALIDAD	DESCRIPCION
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso Interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	**INTEGRIDAD**	**DESCRIPCION**
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	**DISPONIBILIDAD**	**DESCRIPCION**
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Para obtener esta valoración, se realizaron conversaciones con los administradores de la unidad; quienes conocen la importancia de cada activo dentro de la unidad, se revisó la información y documentación suministrada, para así determinar los niveles de confidencialidad, integridad y disponibilidad requeridos para cada procedimiento, que permitan cumplir con las operaciones normales de la unidad.

Ahora el valor total del activo de información depende de la escala de valoración de tipo cualitativa, como se muestra en la Tabla 23:

Tabla 23. Valoración cualitativa

CODIGO	VALOR ACTIVO	DESCRIPCION (Clasificación de información)
MA	Muy Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja
MB	Muy Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Baja

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

Administración Centro de Datos: 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: 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 Centro de Datos, 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.

7. ÁNALISIS DE RIESGOS

Como ya se mencionó, en esta etapa se determina el impacto sobre un activo de información, con la pérdida de confidencialidad, integridad y disponibilidad derivado de la materialización de las 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.

A continuación, se desarrollarán las actividades propuestas por la metodología MAGERIT para el análisis y gestión de riesgos.

7.1 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:

[N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[I] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.

[A] Ataques intencionados: Fallos deliberados causados por las personas.
Cada una de estas categorías presenta una serie de amenazas. Así: (ver tabla 24)

Tabla 24. Amenazas MAGERIT

[N]	**Desastres naturales**	
N01	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
N02	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
N.*	Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto.
[I]	**De origen industrial**	
I01	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
I02	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
I.*	Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, etc.
I03	Contaminación mecánica	Vibraciones, polvo, suciedad,
I04	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta,
I05	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
I06	Corte del suministro eléctrico	Cese de la alimentación de potencia
I07	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,
I08	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Tabla 24. (Continuación)

I09	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tonner, refrigerante,
I10	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
I11	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.
		Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
[E]	**Errores y fallos no intencionados**	
E01	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
E02	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación
E03	Errores de monitorización (logs)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,
E04	Errores de configuración	Introducción de datos de configuración erróneos.
E07	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.
E08	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
E09	Errores de [re]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.

Tabla 24. (Continuación)

E10	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
E14	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
E15	Alteración de la información	Alteración accidental de la información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E18	Destrucción de información	Pérdida accidental de información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E19	Divulgación de información	Revelación por indiscreción.
		Incontinencia verbal, medios electrónicos, soporte papel, etc.
E20	Vulnerabilidades de los programas	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
E21	Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E23	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
E24	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E25	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Tabla 24. (Continuación)

E28	Indisponibilidad del personal	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica
[A]	**Ataques intencionados**	
A03	Manipulación de los registros de actividad	Registros de actividad [D.log]
A04	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A05	Suplantación de identidad de usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
A06	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
A07	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A08	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
A09	Encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
A10	Alteración de secuencia (de mensajes)	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.

Tabla 24. (Continuación)

A11	Acceso no autorizado (aprovechando una debilidad)	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
A12	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.
A13	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
		Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.
		Repudio de recepción: negación de haber recibido un mensaje o comunicación.
A14	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
A15	Modificación de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
A18	Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
A19	Divulgación de información	Revelación de información.
A22	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A23	Manipulación de equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A24	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A25	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Tabla 24. (Continuación)

		El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
A26	Ataque destructivo	vandalismo, terrorismo, acción militar,
A27	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
A28	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos
A29	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A30	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero

MAGERIT nos facilita mucho esta actividad, debido a que indica que tipos de activos se pueden ver afectados por determinados tipos de amenazas. A continuación, se presenta un ejemplo: (ver tabla 25)

Tabla 25. Amenazas por tipo de activos

[N.1] Fuego	
Tipos de activos:	Descripción:
[HW] Hardware [Media] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	Incendios: Posibilidad de que el fuego acabe con recursos del sistema.

De esta forma se definieron las principales amenazas que se podrían presentar sobre cada uno de los activos de información de la UIT. Estas se pueden consultar en la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS.

A continuación, se dan a conocer las amenazas definidas para algunos de los principales activos de información de la unidad: (ver tabla 26-29)

Tabla 26. Amenazas Servidor Akane

Activo TI	**UIT-AS-A-02 Servidor Akane**
Administrador	**Administrador Centro de Datos**
Tipo activo	**Hardware**

Tipo	ID	Amenaza
Desastres naturales	N1	Fuego
	N2	Daños por agua
	N*	Desastres naturales
De origen industrial	I1	Fuego
	I2	Daños por agua
	I*	Desastres industriales
	I3	Contaminación mecánica
	I4	Contaminación electromagnética
	I5	Avería de origen físico o lógico
	I6	Corte del suministro eléctrico
	I7	Condiciones inadecuadas de temperatura o humedad
	I11	Emanaciones electromagnéticas
E	E2	Errores del administrador
	E23	Errores de mantenimiento/actualización de equipos
	E24	Caídas del sistema por agotamiento de recursos
	E25	Perdida de equipos
Ataques intencionados	A6	Abuso de privilegios de acceso
	A7	Uso no previsto
	A11	Acceso no autorizado
	A23	Manipulación de equipos
	A24	Denegación de servicio
	A25	Robo
	A26	Ataque destructivo

Tabla 27. Amenazas Portal Web Universitario

Activo TI	**UIT-AS-A-05 Portal Web Universitario**
Administrador	**Administrador Portal Web**
Tipo activo	**Sistema de Información**

Tipo	ID	Amenaza
I	I5	Avería de origen físico o lógico
Errores y fallos no intencionados	E2	Errores del administrador
	E8	Difusión de software dañino
	E9	Errores de [re-] encaminamiento
	E10	Errores de secuencia
	E15	Alteración accidental de la información
	E18	Destrucción de información
	E19	Fugas de información
	E20	Vulnerabilidades de los programas
	E21	Errores de mantenimiento/actualización de programas
Ataques intencionados	A5	Suplantación de la identidad del usuario
	A6	Abuso de privilegios de acceso
	A7	Uso no previsto
	A8	Difusión de software dañino
	A9	[Re-] encaminamiento de mensajes
	A10	Alteración de secuencia
	A11	Acceso no autorizado
	A15	Modificación deliberada de la información
	A18	Destrucción de información
	A22	Manipulación de programas

Tabla 28. Amenazas Administrador Centro de Datos

Activo TI	**UIT-AS-A-01 Administrador Centro de Datos**
Administrador	**Administrador Centro de Datos**
Tipo activo	**Personal**

Tipo	ID	Amenaza
E	E19	Fugas de información
	E28	Indisponibilidad del personal
A	A28	Indisponibilidad del personal
	A29	Extorsión
	A30	Ingeniería social

Tabla 29. Amenazas Base de Datos correo electrónico institucional

Activo TI	**UIT-AS-A-22 Base de datos Correo Electrónico Institucional**
Administrador	**Administrador Centro de Datos**
Tipo activo	**Datos / Información**

Tipo	ID	Amenaza
Errores y fallos no intencionados	E1	Errores de los usuarios
	E2	Errores del administrador
	E3	Errores de monitorización
	E4	Errores de configuración
	E15	Alteración accidental de la información
	E18	Destrucción de la información
	E19	Fugas de información
Ataques intencionados	A3	Manipulación de los registros de actividad
	A4	Manipulación de la configuración [D.log]
	A5	Suplantación de la identidad del usuario
	A6	Abuso de privilegios de acceso
	A11	Acceso no autorizado
	A15	Modificación deliberada de la información
	A18	Destrucción de la información
	A19	Divulgación de información

7.2 IDENTIFICACIÓN DE VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN ANTE LAS AMENAZAS POTENCIALES

Se llevó a cabo mediante una visita a las instalaciones de la unidad para realizar una inspección visual de los activos de información, entrevistas con los administradores, revisión de la información y documentación suministrada (Reglamento y políticas de uso, manual de funciones y competencias laborales, procedimientos, formatos y hojas de vida de los equipos) y utilización de herramientas de ethical hacking y análisis de vulnerabilidades.

7.2.1 Inspección visual de los activos de información. Inspección visual Sala de servidores. En las figuras 7 y 8 se observa la entrada a la Sala de servidores:

Figura 7. Entrada Sala de servidores

Fuente. Este ´proyecto.

Figura 8. Puerta Sala de servidores

Fuente. Este ´proyecto.

La entrada a la Sala de servidores no cuenta con una cámara de vigilancia.
El control de acceso a la sala de servidores en la puerta no dispone de un sistema biométrico o de seguridad, sino con una cerradura de llave que no permite identificar al personal autorizado para ingresar al sitio.

La puerta de la Sala de servidores tiene retardante para el fuego.

La UIT no cuenta con un protocolo de acceso a la sala de servidores, ni registro de entrada y salida, ni justificación de ingreso. Los únicos facultados para entrar sin previa autorización son: el Administrador Centro de Datos, el Administrador de la Red de Datos y el Administrador de Soporte correctivo.

En las figuras 9 y 10 se observa la entrada principal a las oficinas de Administración Centro de Datos, Administración Red de Datos y Sala de Servidores:

Figura 9. Perímetro oficina Administración de Sistemas

Fuente. Este ´proyecto.

Figura 10. Entrada principal oficinas UIT

Fuente. Este ´proyecto

Para ingresar a la Sala de servidores primeramente se debe pasar por la oficina del Administrador Centro de Datos, y luego por la oficina del Administrador de Red

cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola cerradura de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo.

En las figuras 11 y 12 se encuentran las ventanas de la Sala de servidores, ubicadas en la parte trasera. Estas ventanas son de vidrio normal polarizado con rejillas de metal, que, en caso de protestas en la Universidad de Nariño, no proporcionarían mayor protección a los equipos alojados en este cuarto.

Figura 11. Ventanas Sala de servidores

Fuente. Este proyecto

Figura 12. Ventanas Sala de servidores desde el exterior

Fuente. Este proyecto

La figura 13 nos muestra la cámara de seguridad dentro de la Sala de servidores.

Figura 13. Cámara de seguridad Sala de Servidores

Fuente. Este proyecto

Esta cámara de seguridad se encuentra deshabilitada hace aproximadamente un año por factores eléctricos.

Las figuras 14, 15 y 16 nos muestran el estado actual del cableado de datos y cableado eléctrico en la Sala de servidores:

Figura 14. Cableado 1 Sala de Servidores

Fuente. Este proyecto

Figura 15.Cableado 2 Sala de servidores

Fuente. Este proyecto

Figura 16. Cableado 3 Sala de servidores

Fuente. Este proyecto

No se utilizan paneles de obturación para el cableado en la sala de servidores.

No se encontró sistema de marquillas en los cables de datos y cables de energía. Los cables de datos se encuentran enredados con los cables de energía siendo esto uno de los generadores de ruido en el cableado de datos.

Se evidencia claramente que en la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad, que podría causar averías de origen físico o lógico en los servidores, UPS, evaporadora y demás.

En las figuras 17, 18 y 19 se observa que no existen planos, esquemas, avisos adecuados que indiquen que hay una fuente de energía y señales de estas mismas.

El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.

No están por separado los circuitos de la red regulada y normal.

Figura 17. Cableado 4 Sala de Servidores

Fuente. Este proyecto

Figura 18. Control eléctrico Sala de Servidores

Fuente. Este proyecto

La figura 19 nos muestra el sistema aire acondicionado para la sala de servidores.

En la actualidad se encuentra fuera de servicio, pero está en funcionamiento una evaporadora.

La unidad no cuenta con medidores de temperatura y humedad.

Figura 19. Aire acondicionado Sala de Servidores

Fuente. Este proyecto

Figura 20. Estado aire acondicionado Sala de servidores

Fuente. Este proyecto

Se observa claramente el deterioro que sufre el sistema de aire acondicionado generado por falta de mantenimiento por parte del personal del Área de Soporte y Servicios Tecnológicos.

Figura 21. Evaporadora Sala de servidores

Fuente. Este proyecto

En las figuras 22 y 23 se puede identificar que el espacio entre cada equipo es muy limitado para que fluya el aire. Se deberían separar un poco para mejorar la ventilación entre estos equipos y así evitar que los dispositivos se sobrecalienten, disminuyan su velocidad de procesamiento y por último que puedan apagarse por sobrecalentamiento.

Figura 22. Distribución equipos Sala de servidores

Fuente. Este proyecto

Se observan algunos equipos soportando cajas, las cuales deben estar ubicadas en un lugar adecuado y no sobre el hardware.

Figura 23. Distribución y orden Sala de servidores

Fuente. Este proyecto

Figura 24. Extintor de solkaflam (Clase C)

Fuente. Este proyecto

Importante recalcar que en la sala de servidores no existe un sistema de alarma para este tipo de amenaza.

La figura 25 hace referencia al Sistemas de Alimentación Ininterrumpida con que cuenta la Sala de servidores: UPS con baterías secas.

Figura 25. UPS Sala de Servidores

Fuente. Este proyecto

UPS ubicada en la parte inferior de los racks, expuesta al polvo y/o suciedad.

Las figuras 26, 27 y 28 nos permiten observar algunos de los equipos alojados en la Sala de servidores:

Figura 26. Servidores 1 Sala de servidores

Fuente. Este proyecto

Figura 27. Servidores 2 Sala de servidores

Fuente. Este proyecto

Figura 28. Servidores 3 Sala de servidores

Fuente. Este proyecto

Los racks en los que están ubicados los servidores no cuentan con aisladores de emanaciones electromagnéticas.

El sistema de marquillas en los servidores es el adecuado (Nombre servidor e IP fija).

En la Figura 29 se observa la consola para los racks y monitoreo de los servidores es una pantalla con teclado. La cual debería poseer una llave para poder ser abierta.

Figura 29. Control de servidores

Fuente. Este proyecto

Las figuras 30 y 31 ilustran el sistema de cámaras de vigilancia:

Figura 30. Cámara de vigilancia 1

Fuente. Este proyecto

Figura 31. Cámara de vigilancia 2

Fuente. Este proyecto

Estas cámaras de seguridad controlan específicamente el ingreso a la Biblioteca Alberto Quijano Guerrero, cuya puerta de entrada principal también es primer filtro hacia la oficina de Administración Centro de Datos, oficina de Administración de Red de Datos y Sala de servidores; por tal razón este par de cámaras contribuyen a la seguridad de la información de la unidad.

Inspección visual Taller de Soporte correctivo:

Figura 32. Puerta taller de Soporte correctivo

Fuente. Este proyecto

Figura 33. Entrada taller de Soporte correctivo

Fuente. Este proyecto

El Taller de soporte correctivo se encuentra ubicado en seguida a la entrada de la Biblioteca Alberto Quijano Guerrero.

No existe un sistema de cámaras de vigilancia dentro de la oficina.
Puerta metálica con una sola cerradura de seguridad.

Ventana con vidrio normal y adjunta a la puerta de entrada del lado de la cerradura de seguridad, que facilitaría el ingreso no autorizado al taller.

Todas las oficinas de la unidad tienen vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander.

Ahora en las figuras 34, 35 y 36 se observa una pésima distribución de los monitores, CPU´s, teclados, mouses y demás herramientas del Taller de Soporte correctivo. Este desorden facilitaría la perdida de información, equipos y herramientas necesarias para el adecuado desempeño de esta área.

Figura 34. Distribución 1 Taller de Soporte correctivo

Fuente. Este proyecto

Figura 35. Distribución 2 Taller de Soporte correctivo

Fuente. Este proyecto

Figura 36. Distribución 3 Taller de Soporte correctivo

Fuente. Este proyecto

Figura 37. Al aire libre se encuentra el radiador de la evaporadora; lugar adecuado para el buen funcionamiento de esta, pero es vulnerable a ataques deliberados por parte de personal interno o externo a la universidad que pretenda afectar el buen funcionamiento de la institución.

Figura 37. Radiador de evaporadora

Fuente. Este proyecto

Inspección visual Área de Soporte preventivo: En la figura 38 podemos ver que el armario localizado en el área de soporte preventivo no cuenta con una protección adecuada de las herramientas de trabajo, lo que facilitaría la perdida de estas.

Figura 38. Herramientas área soporte preventivo

Fuente. Este proyecto

En la siguiente figura se observa que el área de soporte preventivo no dispone de una cámara de seguridad desde hace aproximadamente un año y no existe un control para el personal que ingrese a esta oficina.

Figura 39. Inexistencia cámara de seguridad – Área soporte preventivo

Fuente. Este proyecto

En las figuras 40 y 41 se evidencia que el sistema de ventilación esta temporalmente desactivado debido a que genera un ruido excesivo que perjudica el ambiente de trabajo en esta oficina.

Figura 40. Estado Sistema de ventilación

Fuente. Este proyecto

Figura 41. Estado Sistema de ventilación

Fuente. Este proyecto

En la figura 42, se aprecia el sitio de trabajo del administrador de soporte preventivo conformado por un computador de escritorio, que no cuenta con la seguridad requerida para evitar accesos no autorizados, así como la pérdida del mismo.

Figura 42. Computador personal administrador soporte preventivo

Fuente. Este proyecto

7.2.2 Entrevista a los administradores de la UIT. Se estructuraron listas de verificación basadas en el Estándar EIA/TIA 568a, TIA 942 para Centros de Datos y el RETIE (Reglamento Técnico de Instalaciones Eléctricas) utilizadas para identificar las vulnerabilidades de los activos de información ubicados en las instalaciones de la unidad.

Lista de verificación para la sala de servidores: En la tabla se muestran los resultados de la entrevista al Administrador Centro de Datos: (ver tabla 30)

Tabla 30. Resultado entrevista Administrador Centro de Datos

SALA DE SERVIDORES		
ELEMENTO CON LOS QUE DEBE CONTAR	**SI**	**NO**
Altura de 2,50 metros en el cuarto de servidores se cumple.	X	
Ubicado lejos de fuentes electromagnéticas (Antenas, máquinas eléctricas, radar, iluminación, microondas, aparatos electrónicos).	X	
Esta cerca de Fuentes de inundación.		X
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	X	
Las puertas tienen retardante para el fuego.	X	
Iluminación adecuada.		X
Polvo en el medio ambiente.	X	
Cuenta con un equipo contra incendios al entrar a la sala.	X	
La sala es resistente al fuego.		X
Normas comunes de conservación y limpieza.		X
Se utilizan paneles de obturación para los cables.		X
Existe cableado bajo el piso elevado que no se utiliza y puede eliminarse.		X
Cuenta con aisladores (Ejemplo espuma) los racks.		X
Cuenta con un sistema de marquillas en los equipos dentro del cuarto.	X	
Equipos de respaldo para todos los elementos que interviene en el funcionamiento.		X
Accesibilidad para el suministro de equipos.	X	
SEGURIDAD EN EL AREA	**SI**	**NO**
Al Ingresar a la sala de servidores tiene un sistema de seguridad que le permita saber quién ingreso.		X
Cuenta con un sistema de seguridad de cámara de vigilancia.		X
Tiene sistema de alarma contra incendios.		X
Tienen el sistema de alarmas de control de temperatura y humedad.		X
AIRE ACONDICIONADO	**SI**	**NO**
Ventiladores en la parte superior de los racks de los servidores.		X

Tabla 30 (Continuación)

Existen fugas en el piso elevado o en el sistema de suministro de aire.		X
Los puntos de referencia de los aires acondicionados son apropiados.		X
Climatización para la sala de servidores y UPS.	X	
Controles de temperatura.	X	
Cuenta con deshumidificación y ventilación.		X
La configuración del sistema de retorno de aire es apropiada.		X
Tuberías de suministro y retorno invertidas.		X
Válvulas defectuosas.		X
Hay sistemas de enfriamiento que no fueron puestos en marcha.	X	

Lista de verificación cableado de red: En la tabla se muestran los resultados de la entrevista al Administrador de la Red de Datos, Internet y RENATA:

Tabla 31. Resultado entrevista Administrador de Red

CABLEADO DE RED	SI	NO
Categoría de cableado marque con una X: 5E X,6A X , 7A __.		
Los puntos de red dentro de las áreas son los adecuados.	X	
Cumple con el radio mínimo de curvaturas: 4x0 en funcionamiento.	X	
Diseño lógico de redes en el entorno marque con x: Anillo ___, Bus ___, Mixta ___, Malla ___, Doble anillo ___, Árbol ___, Estrella X.		
Utilizan canaletas metálicas o plásticas para la protección del cableado en el edificio.	X	
Dentro de las oficinas los puntos de red están dispuestos a la distribución de las áreas.	X	

Lista de verificación cableado eléctrico: En la tabla se muestran los resultados de la entrevista al Administrador del Área de Soporte correctivo: (ver tabla 32)

Tabla 32. Resultado 1 entrevista Administrador de Soporte correctivo

CABLEADO ELÉCTRICO	SI	NO
El cable esta con la conformidad con los estándares de seguridad contra incendios: UL VW-1, IEC 332-1.	X	
Estabilizadores de tensión	X	
Transformadores de aislación.	X	
Tableros de distribución.	X	
Los puntos eléctricos dentro de las áreas son los adecuados y están acordes.	X	
Cuenta con señales de seguridad donde advierta peligro de corto circuito.	X	
TIERRA CONFIABLES	**SI**	**NO**
Los gabinetes y los protectores de voltaje están conectados a una barra de cobre de polo a tierra.	X	
Estas barras se conectan al sistema de tierras (groundingbackbone) mediante un cable de cobre cubierto con material aislante	X	
ENERGIA ININTERRUMPIDA - UPS	**SI**	**NO**
Protección de energía para servidores de nivel de entrada, dispositivos pequeños de conexión en red y de más dispositivos.	X	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para servidores.	X	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para las redes de voz y datos	X	
Protección de energía trifásica diseñada para cumplir con requisitos de infraestructuras pequeñas y grandes y aplicaciones para salas de equipos	X	
Administración remota	X	
Fuentes de alimentación. Confiabilidad 24 x 7.	X	

Tabla 32 (Continuación)

AIRE ACONDICIONADO EN SALA DE SERVIDORES	SI	NO
Los puntos de referencia de los aires acondicionados son apropiados.		X
La configuración del sistema de retorno de aire es apropiada.		X
Tienen implementado un régimen de mantenimiento del sistema de enfriamiento.	X	
Sensores dañados o sin calibrar.		X
Tuberías de suministro y retorno invertidas.		X
Válvulas defectuosas.		X

Lista de verificación sistemas eléctricos y UPS: En la tabla se muestran los resultados de la entrevista al Administrador del Área de Soporte correctivo:

Tabla 33. Resultado 2 entrevista Administrador de Soporte correctivo

ELEMENTO CON LOS QUE DEBE CONTAR	SI	NO
Existencia de planos, esquemas, avisos que hay una fuente de energía y señales de estas mismas.		X
Identificación de los circuitos en toda la unidad	X	
Identificación de los conductores como Fase, Neutro y Tierra.	X	
Los materiales están acordes con las condiciones ambientales.	X	
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto directo en las áreas de trabajo.		X
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto indirecto en las áreas de trabajo.		X
El sistema eléctrico del edificio cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.		X
Cuentan con un sistema de protección contra rayos.		X
Están por separado los circuitos de la red regulada y normal además cuentan con los planos de cada una.		X
Los tomas de la red regulada y normal están marcados con naranja para regulada y blanco para normal en todas las oficinas del edificio.	X	

Tabla 33 (Continuación)

Las UPS son de batería: seca X, liquida ___.		
La capacidad de soporte de cada UPS está por circuitos.	X	
El mantenimiento de estas es cada: mes X, 3 meses ___, 6 meses ___, año ___, dos años ___.		
TIERRA CONFIABLES		
Continuidad de los conectores de tierra y conectores equipotenciales.	X	

7.2.3 Ethical hacking[35] y análisis de vulnerabilidades:

- **Pruebas servidor mail**

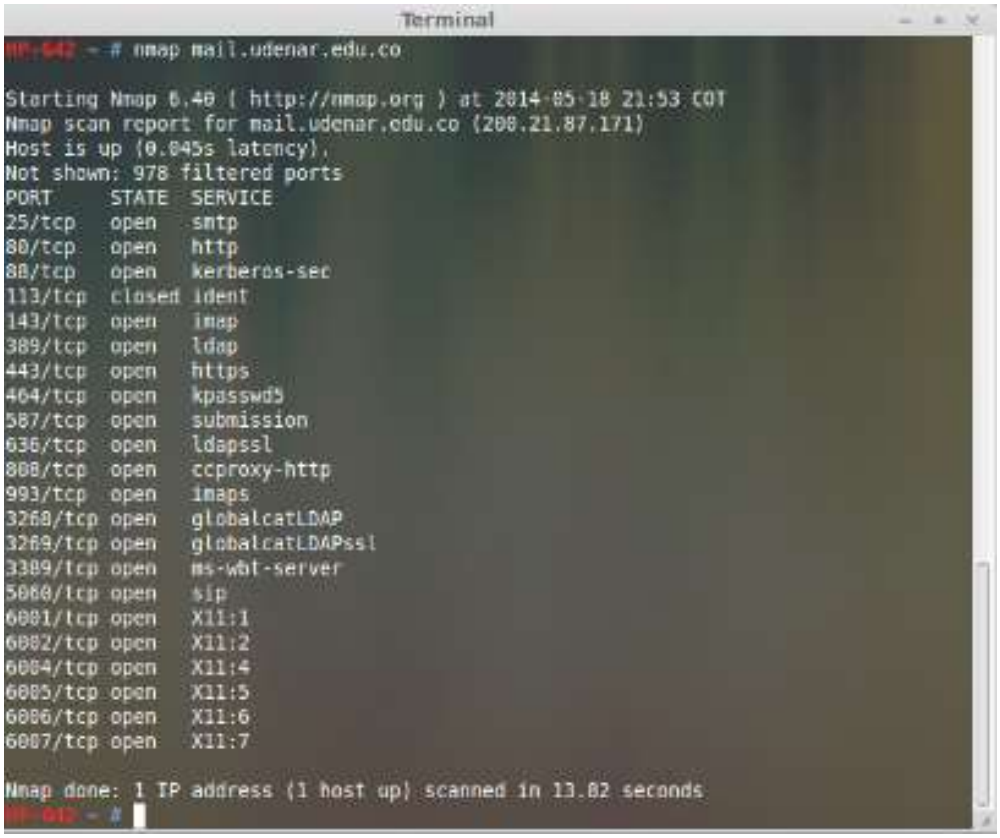
El servidor mail es un servidor muy importante para la unidad, por lo que en estas pruebas además de realizar el exhaustivo estudio de puertos y de sistema operativo, se tendrá en especial consideración el puerto 25 que corresponde al servicio SMTP[36], con el fin de identificar hasta donde se puede ingresar en la Shell del sistema con el objetivo de enviar correos electrónicos no deseados a través de la herramienta libre telnet.

La herramienta Telnet (TeLecommunication NETwork) es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.

Como primera medida, realizó un escaneo inicial con el fin de averiguar la dirección IP que tiene el servidor mail.udenar.edu.co así como los puertos que están abiertos. En la figura 43 se puede apreciar los resultados de dicho escaneo. (ver figura 43)

[35] Ataques a la red o Sistemas de Información sin fines destructivos.
[36] Protocolo simple de transferencia de correo

Figura 43. Escaneo inicial – Servidor Mail



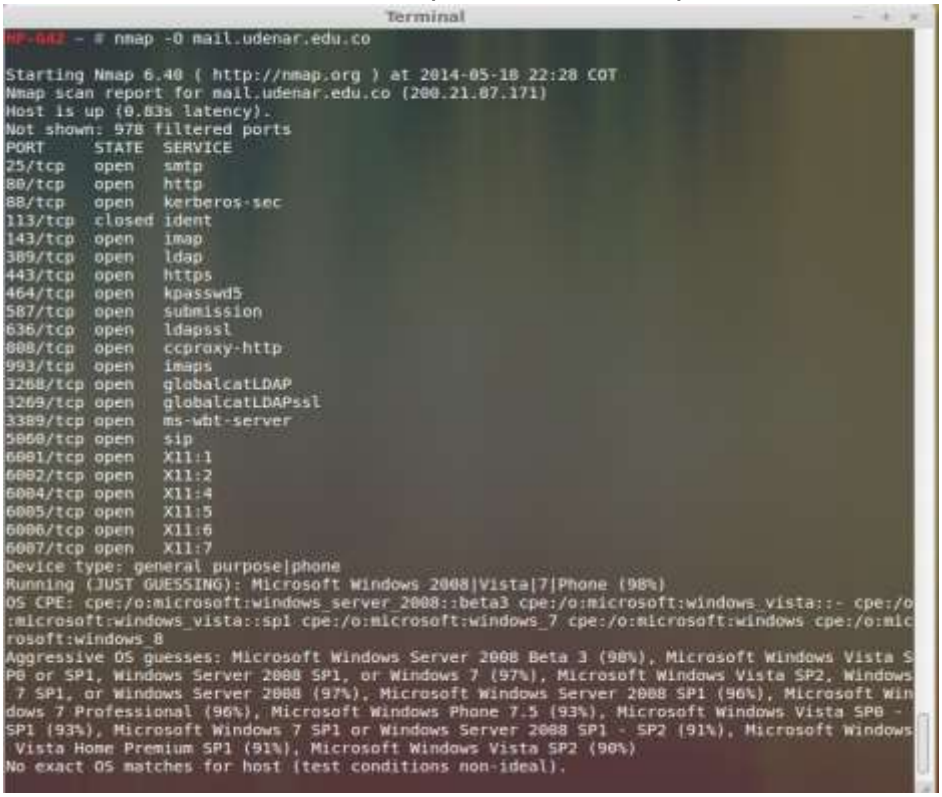
Fuente. Este proyecto

Al ser un servidor de suma importancia para la universidad, tiene puertos abiertos como kpasswd5 por el cual se podría acceder a los passwords desprotegidos con técnicas metasploit[37].

También se hizo un escaneo del sistema operativo con nmap obteniendo resultados no muy exactos (ver Figura 44), por lo que se decidió usar zenmap con un resultado de certeza de un 97% para Microsoft Windows Server 2008 SP1 (ver Figura 45). Esto denota que, frente a algún posible ataque al sistema operativo, se puede decir que se da un indicio importante al dar esa información con ese grado de exactitud.

[37] Proyecto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad.

Figura 44. Identificación del sistema operativo con nmap – Servidor Mail



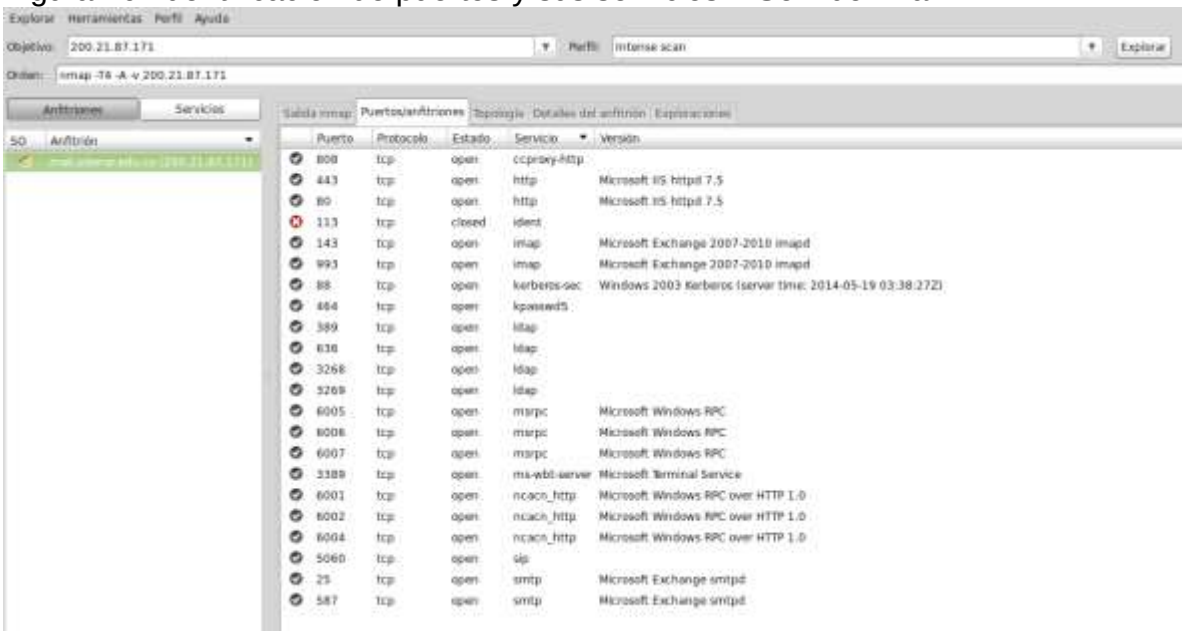
Fuente. Este proyecto

Figura 45. Identificación del sistema operativo con zenmap – Servidor Mail

Fuente. Este proyecto

Luego, se realizó la respectiva identificación de los servicios disponibles en los puertos que se encontraron abiertos (ver Figura 46), con lo que se evidencia nuevamente que algunos puertos están abiertos innecesariamente, así como repetidamente como en el caso del servicio RPC[38].

Figura 46. Identificación de puertos y sus servicios – Servidor Mail

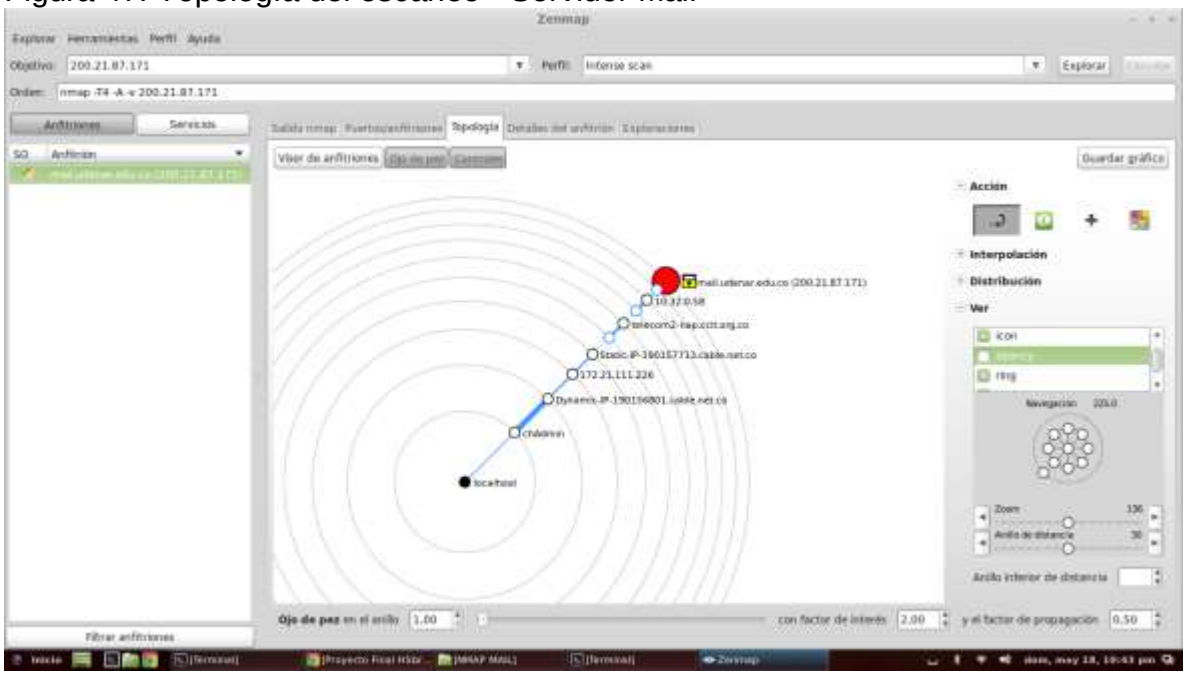


Fuente. Este proyecto

Asimismo, se realizó un gráfico de la topología utilizada en el escaneo del servidor mail (ver Figura 47).

[38] Llamada a procedimiento remoto

Figura 47. Topología del escaneo - Servidor Mail



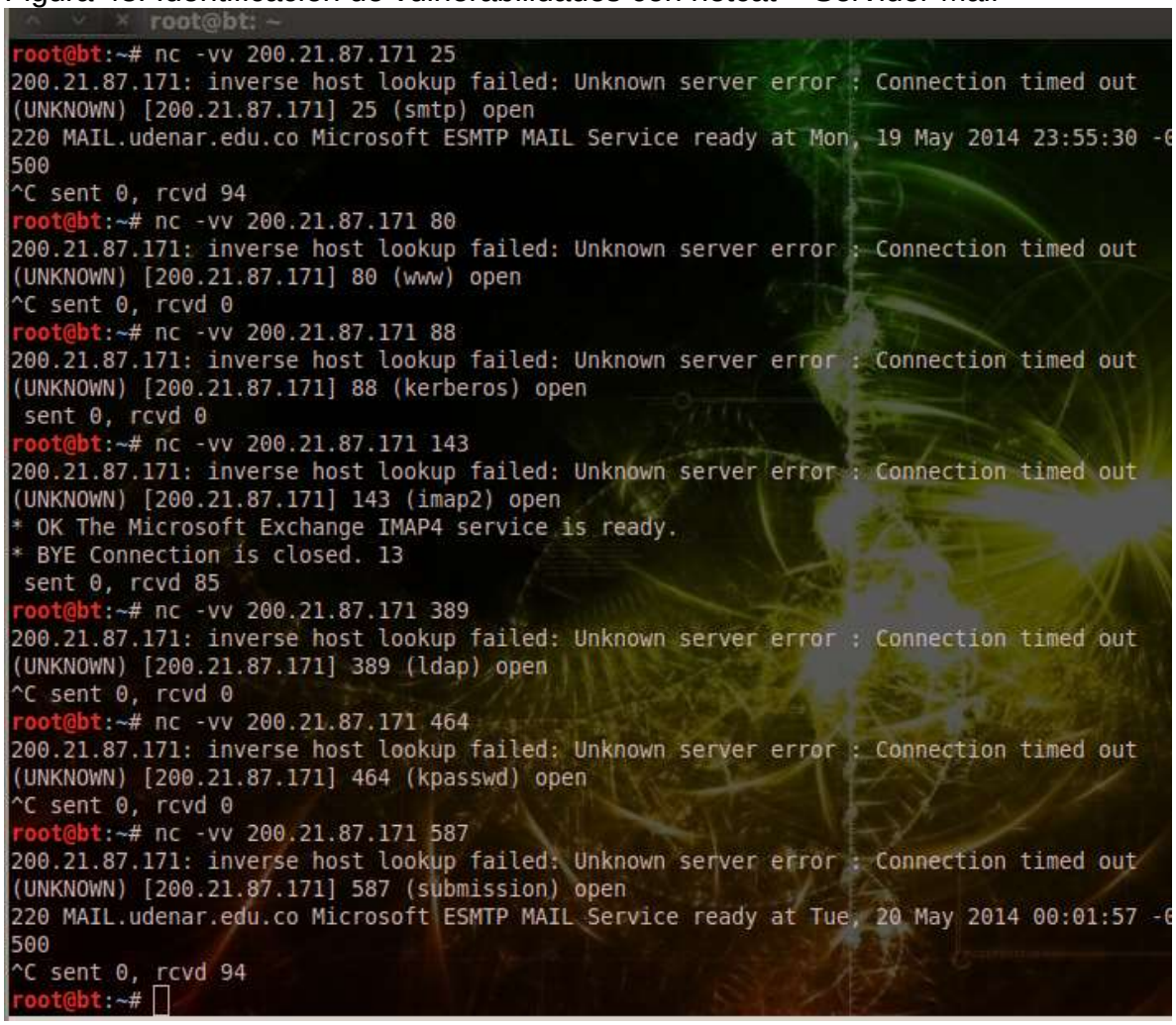
Fuente. Este proyecto

Se identificaron vulnerabilidades importantes en el servidor mail por medio del puerto 25 con su servicio smtp en donde con la herramienta NETCAT[39], (ver Figura 48), se pudo tener acceso a la Shell de Microsoft ESMTP[40] en donde posteriormente se hicieron pruebas con la herramienta TELNET[41] (ver figura 49), cuyos resultados nos dieron a conocer que se puede llegar hasta el punto de redactar un correo electrónico.

No obstante, aunque el correo no se envió al destinatario final, el servidor lo puso en cola de espera. Algo que con un ataque de tipo D.O.S (***D**enial **o**f **S**ervice – Denegación del Servicio*) dejaría fuera de línea al servidor en cuestión. Se recomienda tener mayor control en este punto para evitar posible correo spam y demás riesgos para la comunidad estudiantil.

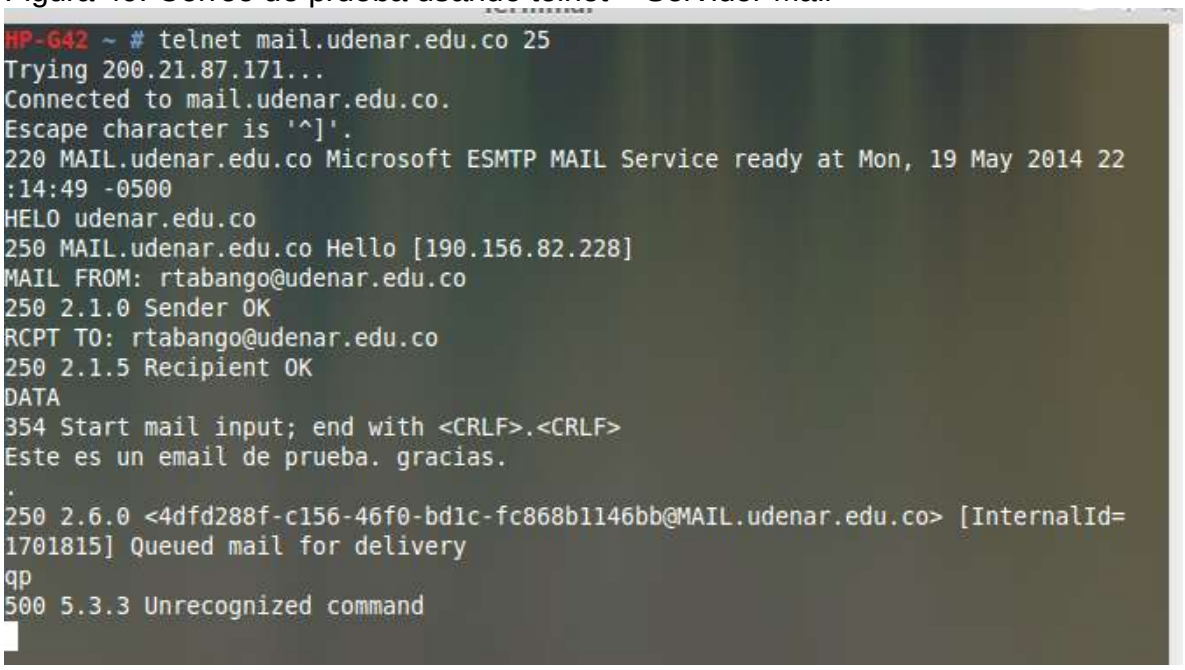
[39] Herramienta para depuración, análisis y manipulación de redes y servicios TCP/IP.
[40] Protocolo simple de transferencia de correo mejorado.
[41] Protocolo de red que permite viajar a otra máquina para manejarla remotamente.

Figura 48. Identificación de vulnerabilidades con netcat – Servidor Mail



Fuente. Este proyecto

Figura 49. Correo de prueba usando telnet – Servidor Mail



Fuente. Este proyecto

Pruebas al sistema de información de convocatorias: El sistema de información de convocatorias de la Universidad de Nariño está a cargo del área de administración portal web, en el cual se publican y se realizan algunas fases del proceso de contratación de personal de las diferentes dependencias universitarias. Cabe resaltar que es fuente de constante consulta por parte del personal tanto interno como externo a la universidad.

Debido a la gran importancia que tiene este sistema no solo dentro de la unidad, sino también en la comunidad universitaria se planteó realizar pruebas de penetración a su base de datos para que, en el peor de los casos, se pudiera tener acceso a las contraseñas de los administradores, así como también la posibilidad de modificar información publicada por este sistema. Esto, claro está, con pleno conocimiento y autorización por parte de la Licenciada Elizabeth Tobar, Administradora del Portal Web.

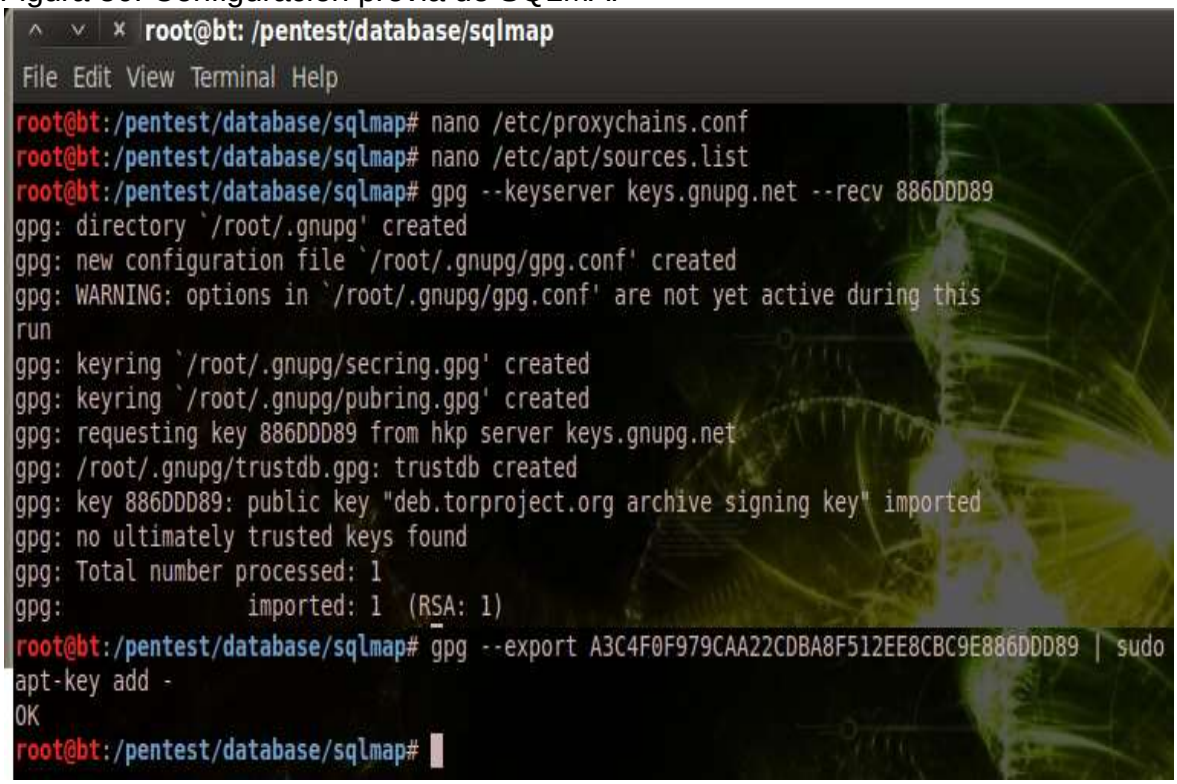
Esta prueba de penetración a la base de datos del sistema se realizó con la ayuda de la herramienta SQLMAP[42] incluida en el sistema operativo BackTrack rc3.

El primer paso que se realizo fue configurar la herramienta SQLMAP, agregando nuevas claves para su correcto funcionamiento (ver Figura 50). Estas claves vienen

[42] Técnica de ataques a páginas o aplicaciones para romper o acceder a la información.

proporcionadas en el manual de Backtrack que puede ser consultado en [http://n.pentest.jp/tmp/SQLMAPTutorial.pdf].

Figura 50. Configuración previa de SQLMAP

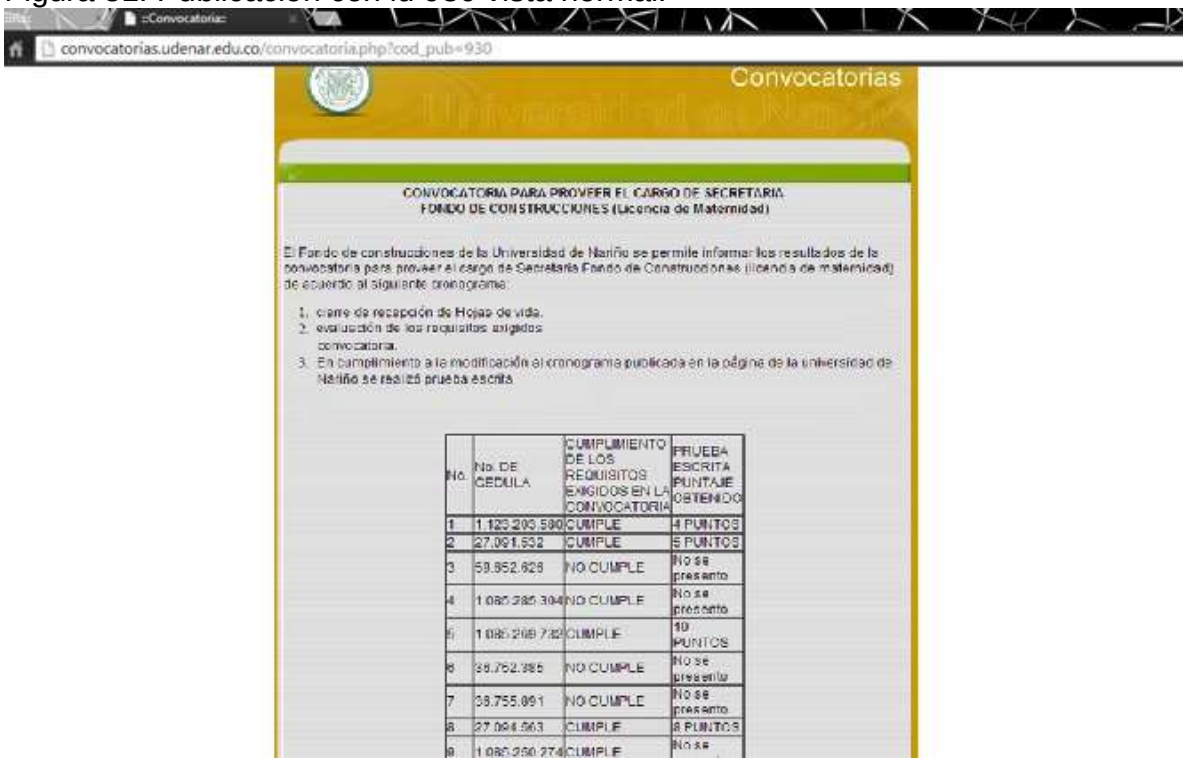


Fuente. Este proyecto

Después, se verifico en la página web del sistema de convocatorias (ver Figura 51) si estaba validado un error de sintaxis que es muy común y peligroso, se agregó una comilla al final de la url de una publicación cualquiera dando el error de sintaxis esperado (ver Figura 52).

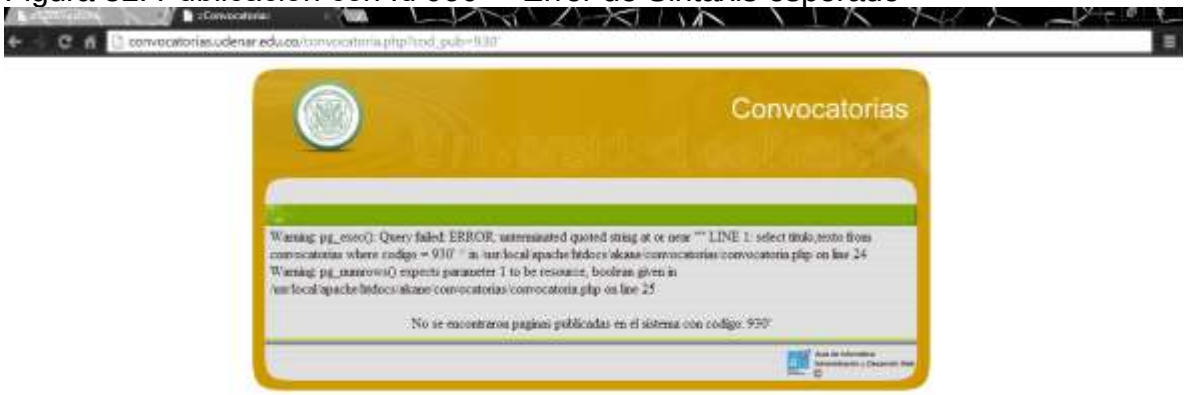
Sqlmap hace uso de este error para tratar de realizar una inyección sql con miras a explorar la base de datos.

Figura 51. Publicación con id 930 vista normal.



Fuente. Este proyecto

Figura 52. Publicación con Id 930’ – Error de Sintaxis esperado



Fuente. Este proyecto

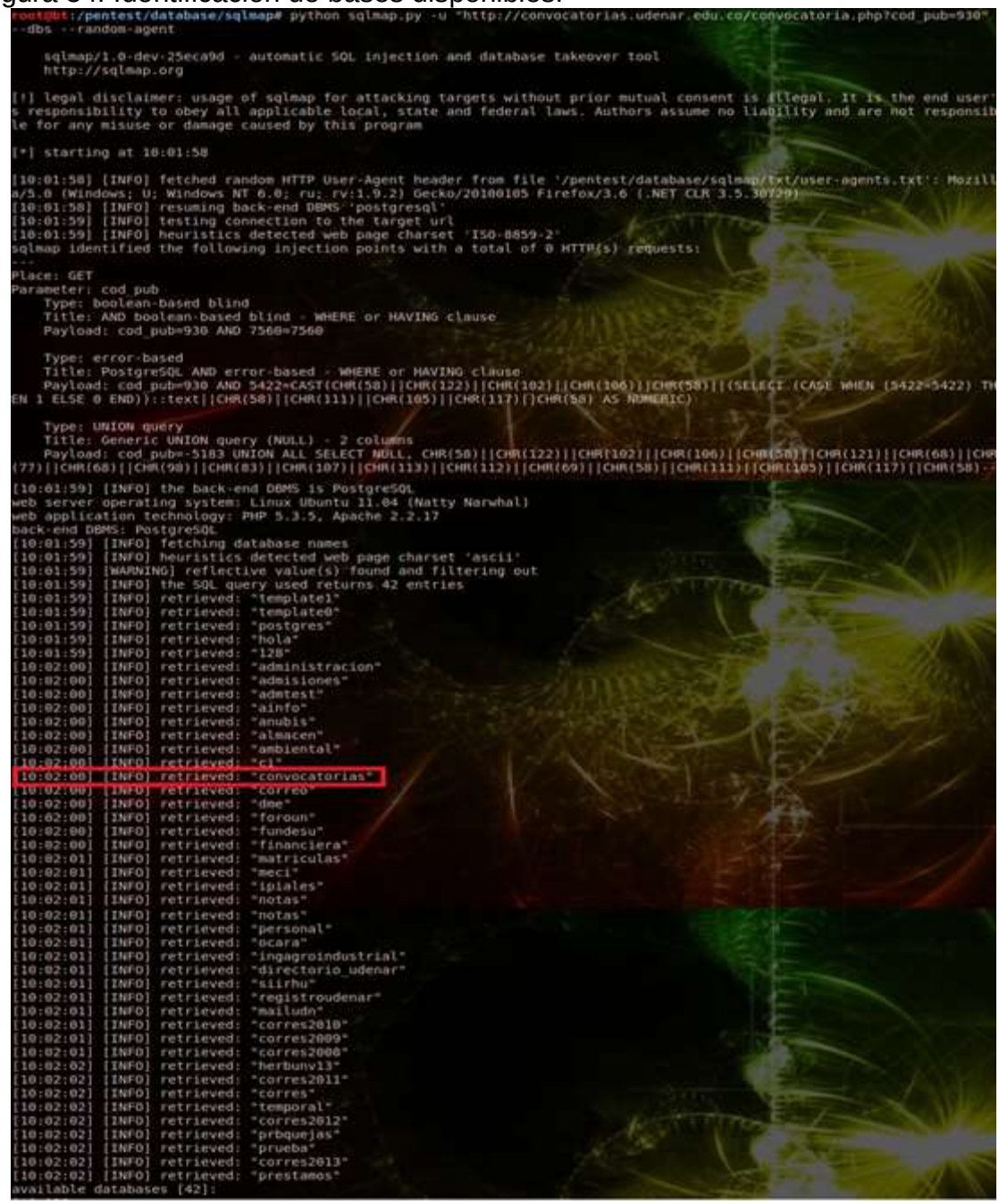
Al ver este error, se continuó con la prueba de penetración, primero haciendo una exploración inicial (ver Figura 53) para descubrir el gestor de base de datos dando como resultado Postgres 8.4 – 9.0.

Figura 53. Identificación del gestor de base de datos – Sistema Convocatorias

Fuente. Este proyecto

Luego, se realizó un escaneo de los nombres de las bases de datos administradas por el gestor postgres, esto con el fin de seleccionar la base de datos perteneciente al sistema de convocatorias, aunque con sqlmap se pudo identificar que no solo está disponible la base de convocatorias, sino que también 42 bases de datos más que están también expuestas (ver Figura 54).

Figura 54. Identificación de bases disponibles.



Fuente. Este proyecto

Como el objetivo de esta prueba es tratar de vulnerar el sistema de convocatorias de la universidad, nos centramos en la base de datos llamada “convocatorias”. El siguiente paso para seguir fue tratar de descubrir que tablas tiene la base de datos “convocatorias” y se descubrió que solamente son 3 tablas (ver Figura 55) con nombres que no siguen algún estándar de nomenclatura, algo sumamente grave porque fácilmente se pudo identificar la tabla “usuarios”.

Figura 55. Identificación de tablas base de datos convocatorias – Sistema Convocatorias

Fuente. Este proyecto

Al haber descubierto la existencia de la tabla “usuarios”, para poder hacer un volcado de datos (extracción de contraseñas), necesitamos conocer la estructura de la tabla, es decir, de que campos está compuesta, así como el tipo de dato al que está asociado cada campo (ver Figura 56).

Figura 56. Campos de la tabla usuarios – Sistema de Convocatorias

Fuente. Este proyecto

De igual manera, los campos de la tabla usuarios no utilizan una nomenclatura apropiada dejando ver que existe un campo llamado “clave” del cual se deduce que en dicho campo están las claves de acceso al sistema de convocatorias. Ahora el siguiente paso, es hacer el volcado de datos contenidos en la tabla usuarios para revisar si la clave utiliza algún tipo de cifrado o no (ver Figura 57). Dicho volcado se adjunta en la carpeta de anexos del proyecto para su posterior comprobación.

Figura 57. Volcado de datos de la tabla usuarios – Sistema de Convocatorias

Fuente. Este proyecto

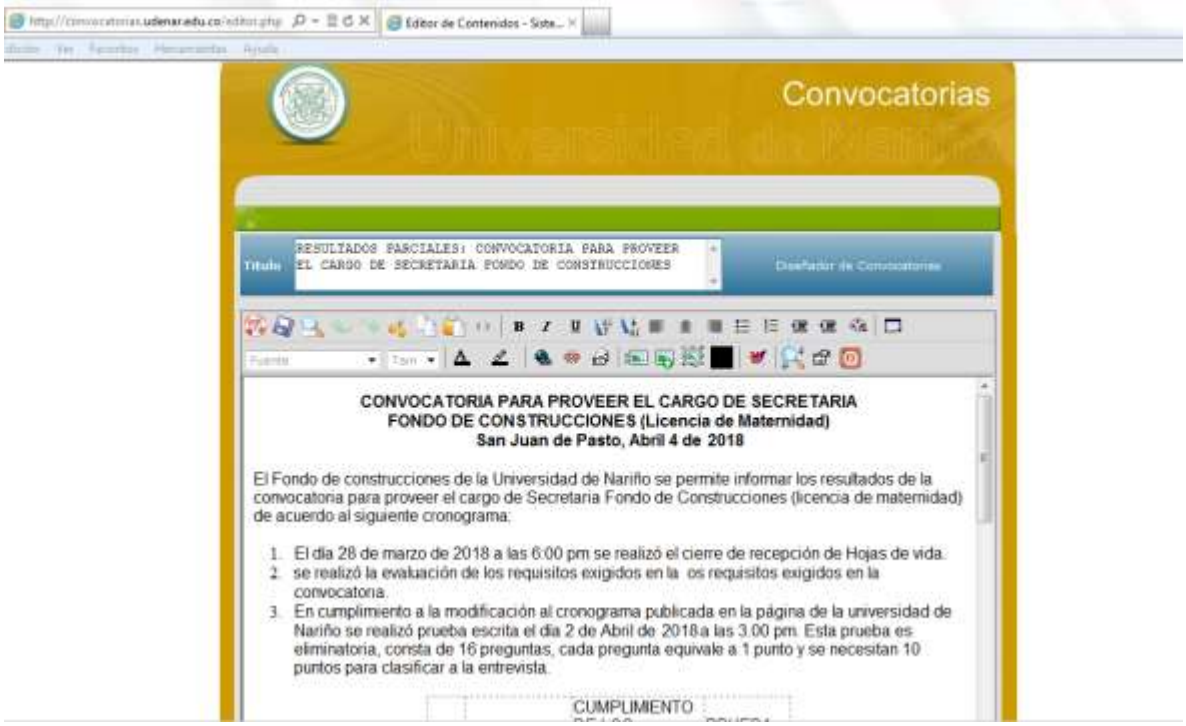
Luego de todo este proceso se descubrió que las claves de acceso no utilizan un método de cifrado como md5 o similares. Para el caso de la administradora Elizabeth se pudo establecer que su clave de acceso es “Masterudn2013”, además de que no se ha realizado una depuración de usuarios antiguos, los cuales con su clave podrían ingresar al sistema como tal. Por consiguiente, se recomienda actualizar las políticas de seguridad del sistema de convocatorias que están en un muy bajo nivel.

Luego, se procedió a realizar la conexión exitosa al sistema con los datos extraídos en esta exploración se ingresó a un menú de modificación total de las convocatorias (ver Figura 58, 59 y 60).

Figura 58. Inicio de sesión – Sistema de Convocatorias

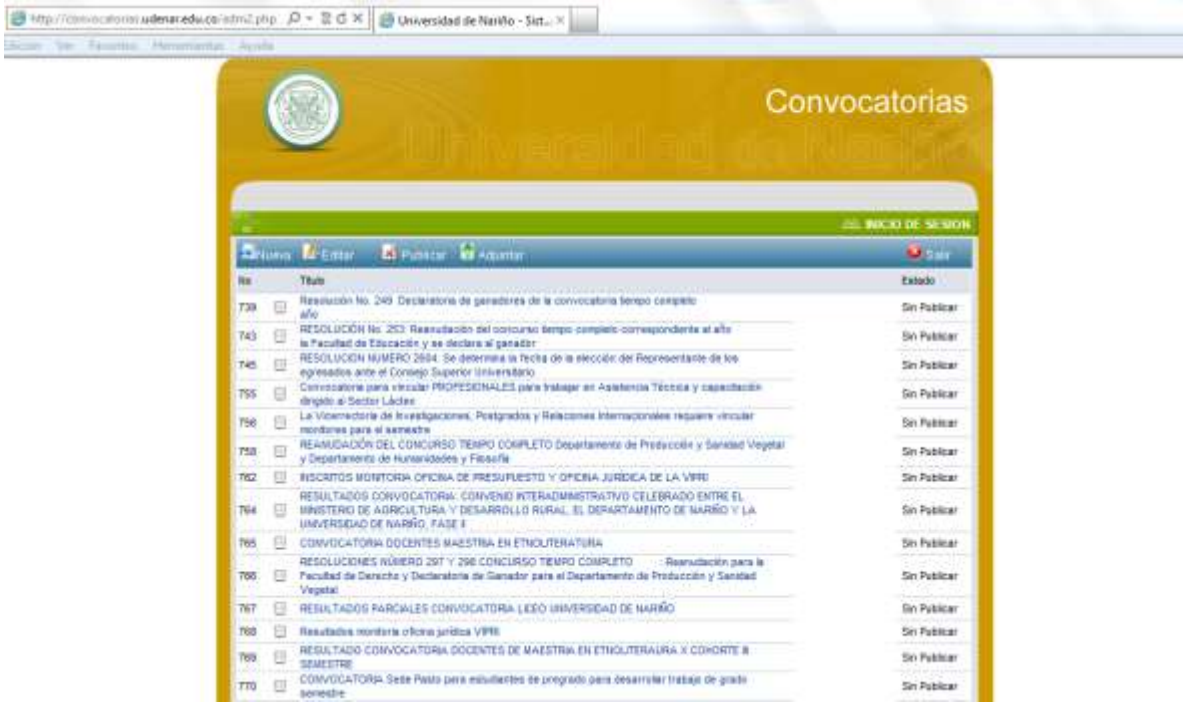
Fuente. Este proyecto

Figura 59. Página principal administración – Sistema de Convocatorias



Fuente. Este proyecto

Figura 60. Edición de publicaciones - Sistema de Convocatorias



Fuente. Este proyecto

- **Pruebas a la red inalámbrica universitaria OASI**

Para realizar esta prueba en busca de debilidades, se usó *GOYSCRIPT*, una herramienta basada en la suite Aircrack-ng para la explotación de vulnerabilidades en el cifrado WEP de la red inalámbrica de acceso a internet OASI de la Universidad de Nariño, la cual está a cargo el área de administración de sistemas de la unidad.

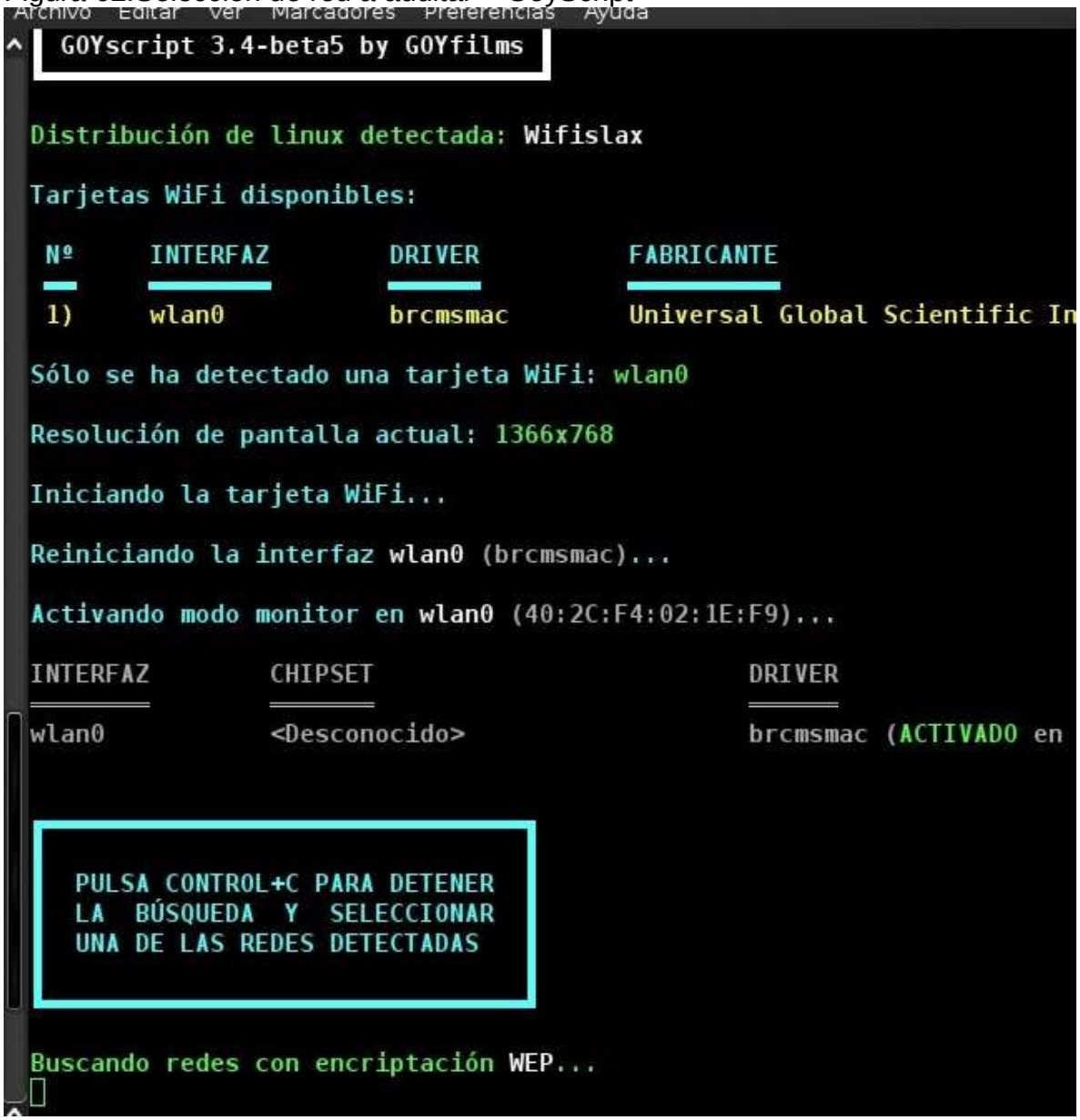
Su uso es muy simple, al ejecutar la herramienta, lo primero que nos pide, es seleccionar la interface de red que queremos montar en modo monitor para que nos pueda hacer el escaneo. Como se puede ver en la figura 61, en nuestro caso como solo tenemos una, el script nos selecciona la que tenemos disponible automáticamente.

Figura 61. Selección de interface de red - GoyScript

Fuente. Este proyecto

Una vez seleccionada, el solo script lanzara airodump-ng en el que se nos mostraran las redes con cifrado wep, que tenemos a nuestro alcance, cuando veamos nuestro objetivo en este caso la red oasi, cerraremos esta ventana, usando ctrl + c y a continuación nos mostrara un menú (ver Figura 62) con todas las redes disponibles, para que seleccionemos la que queremos auditar.

Figura 62.Selección de red a auditar – GoyScript



Fuente. Este proyecto

Al seleccionar la red número 8 que corresponde a la red oasi, automáticamente GoyScript lanzara todos los ataques de la suite Aircrack-ng (ver Figura 63), al mismo tiempo conforme vaya obteniendo vectores de inicialización (iv's) en donde esta encriptada la contraseña, ira probando con aircrack la obtención de la clave, cuando haya suficientes nos mostrara la clave en pantalla (ver Figura 64).

Figura 63. Auditando a la red oasi – GoyScript

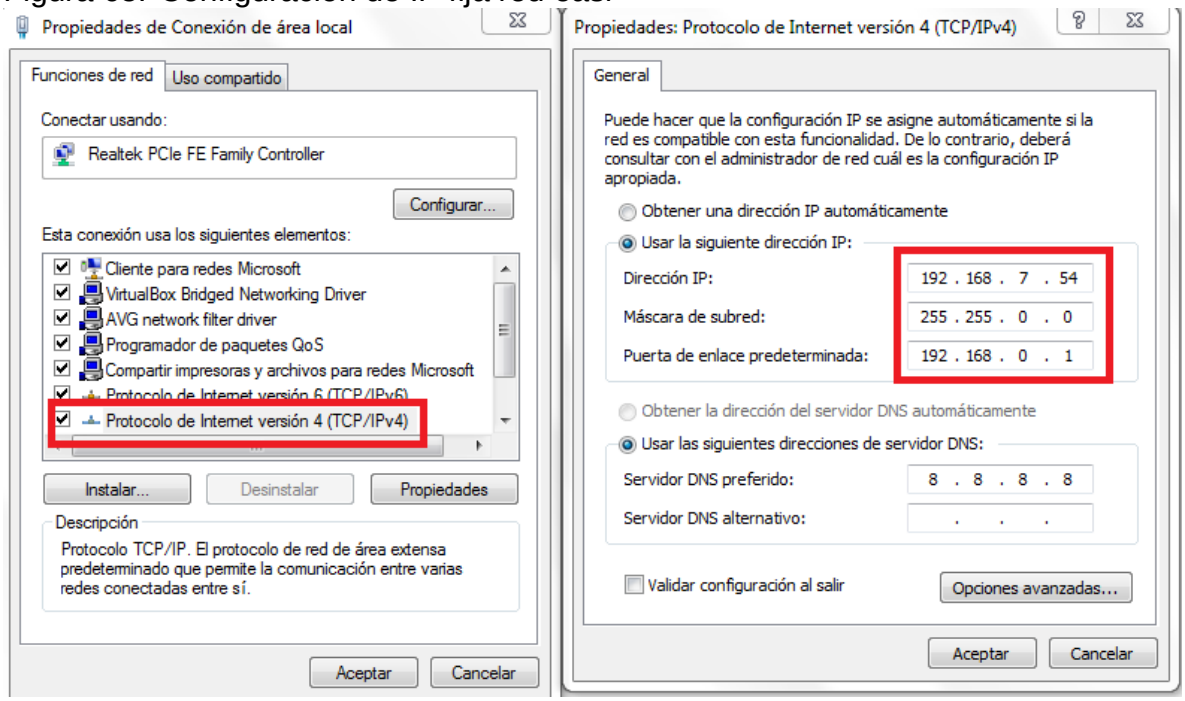
Fuente. Este proyecto

Figura 64. Clave de la red oasi obtenida – GoyScript

Fuente. Este proyecto

Como podemos observar, en menos de un minuto se pudo vulnerar la clave de acceso a la red inalámbrica oasi, evidenciando que se tiene una muy grave falencia en la restricción de acceso a internet en la red oasi. Además, se demuestra que no se requiere un registro obligado de los equipos por parte del personal del área de sistemas para acceder a la red. Basta con tener la clave (A1302B1302), y una dirección IP estática que se encuentra a la vista en cualquier equipo del aula de informática. Es cuestión de cambiar nuestra ip (ver Figura 65) para tener acceso a la red.

Figura 65. Configuración de IP fija red oasi



Fuente. Este proyecto

De igual manera se hizo una prueba de conexión desde un dispositivo Android con una dirección IP estática similar, demostrando que también se puede acceder a la red sin haber registrado el equipo previamente. Se puede ver en las figuras 66, 67 y 68 que luego de introducir la clave obtenida se realizó una conexión exitosa.

Figura 66. Conectado a la red oasi

Fuente. Este proyecto

Figura 67. Ajustes IP estática

Fuente. Este proyecto

Figura 68. Estado de conexión a la red oasi

Fuente. Este proyecto

En el documento ***ANEXO C – ETHICAL HACKING***, se pueden observar todas las pruebas realizadas de Ethical Hacking y análisis de vulnerabilidades.

Las vulnerabilidades encontradas para cada uno de los activos de información se registran en una tabla como la que se presenta en seguida: (ver tabla 34)

Tabla 34. Vulnerabilidades Servidor Akane

Activo TI	**UIT-AS-A-02 Servidor Akane**
Administrador	**Administrador de Sistemas**
Tipo activo	**Hardware**

Tipo	ID	Amenaza	Exposición / Vulnerabilidad
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N2	Daños por agua	

Tabla 34 (Continuación)

	N*	Desastres naturales	La Unidad de Informática y Telecomunicaciones se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I2	Daños por agua	
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. El sistema de aire acondicionado está fuera de servicio. La configuración del sistema de retorno del aire acondicionado no es apropiada. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.
	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS. No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Aire acondicionado fuera de servicio. La configuración del sistema de retorno de aire acondicionado no es apropiada.
	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.
E	E2	Errores del administrador	Falta de conocimiento del administrador.

Tabla 34 (Continuación)

	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor AKANE. Falta de conocimiento del administrador.
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio
	E25	Perdida de equipos	
Ataques intencionados	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander. Pruebas Lógicas: En los diferentes puertos escaneados, se observó actividad importante en el puerto 43 y 80. Y en el puerto 21 se puedo tener acceso a la Shell del programa vsFTP en su versión 2.3.2.
	A7	Uso no previsto	
	A11	Acceso no autorizado	
	A23	Manipulación de equipos	
	A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander.
	A26	Ataque destructivo	Al ser una universidad pública, periódicamente de se llevan a cabo marchas y protestas que podrían afectar los recursos de la unidad.

Los documentos completos del registro de vulnerabilidades se pueden revisar en la carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS***.

7.2.4 Estimación del impacto. El objetivo es conocer el alcance del daño producido en la UIT 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. A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto. (ver tabla 35)

El primer dato requerido es el “Nivel del activo”:

Tabla 35. Valor del activo

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
UIT-AS-A-01	Administrador Centro de Datos	1	P	Uso Interno	Normal	Muy Alta	**Muy Alto**	**5**
UIT-AS-A-02	Servidor Akane - Dell PowerEdge R815	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

El segundo dato necesario para la valoración del impacto es la “Degradación”, el cual nos indica que tan perjudicado resulta el [valor del] activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas:

- 100%: Degradación muy considerable del activo
- 50%: Degradación medianamente considerable del activo
- 1%: Degradación poco considerable del activo

Para el caso de Servidor Akane con nivel **Muy Alto** y un porcentaje estimado de degradación de **100%,** puesto que al ser de tipo hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres industriales y robo; lo afectarían o afectarían a la unidad considerablemente.

Al realizar el producto de ambos datos en la tabla X, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información: (ver tabla 36)

Tabla 36. Estimación del impacto Servidor Akane

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.
Mayor (5): Impacta en la operatividad de los procesos.
Moderado (3): Impacta en la operatividad del macroproceso.
Menor (2): Impacta en la operatividad del proceso.
Insignificante (1): Impacta levemente en la operatividad del proceso

El mismo procedimiento se realizó con cada uno de los activos de información a proteger de la UIT, cuyos resultados se puede evidenciar en la carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS***.

7.2.5 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 (a mayor número de vulnerabilidades, mayor probabilidad de ocurrencia de las amenazas) y se utilizó la siguiente escala: (ver tabla 37-38)

Tabla 37. Estimación de la probabilidad

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

En la Tabla 34, se visualiza el impacto y la frecuencia de materialización cada una de las amenazas sobre el Servidor Akane:

Tabla 38. Impacto y frecuencia Servidor Akane

Activo TI	**UIT-AS-A-02 Servidor Akane**	
Administrador	**Administrador Centro de Datos**	
Degradación	**100%**	
Impacto	**8**	**Desastroso**
Tipo	**Hardware / equipos**	

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2
	N2	Daños por agua		Raro	1
	N*	Desastres naturales	La Unidad de Informática y Telecomunicaciones se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2
	I2	Daños por agua		Raro	1
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. El sistema de aire acondicionado está fuera de servicio. La configuración del sistema de retorno del aire acondicionado no es apropiada. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.	Media	4

Tabla 38 (Continuación)

	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.	Muy baja	2
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS. No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.	Muy baja	2
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Aire acondicionado fuera de servicio. La configuración del sistema de retorno de aire acondicionado no es apropiada.	Baja	3
	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.	Baja	3
E	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor AKANE. Falta de conocimiento del administrador.	Baja	3
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3
	E25	Perdida de equipos		Muy baja	2
Ataques intencionados	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad	Baja	3
	A7	Uso no previsto		Baja	3
	A11	Acceso no autorizado		Baja	3

Tabla 38 (Continuación)

	A23	Manipulación de equipos	y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander. Pruebas Lógicas: En los diferentes puertos escaneados, se observó actividad importante en el puerto 43 y 80. Y en el puerto 21 se puedo tener acceso a la Shell del programa vsFTP	Baja	3
	A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander.	Muy baja	2
	A26	Ataque destructivo	Al ser una universidad pública, periódicamente de se llevan a cabo marchas y protestas que podrían afectar los recursos de la unidad.	Baja	3

De igual manera la estimación de frecuencia de materialización de las amenazas sobre cada uno de los activos de información de la UIT, se pueden examinar en la carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS***. (ver tabla 39)

7.2.6 Estimación del riesgo. Este valor se obtiene como resultado de la siguiente fórmula:

Riesgo (R)= Probabilidad (F) x Impacto

Tabla 39. Estimación del Riesgo Servidor Akane

Activo TI	**UIT-AS-A-02 Servidor Akane**	
Administrador	**Administrador Centro de Datos**	
Degradación	**100%**	
Impacto	**8**	**Desastroso**
Tipo	**Hardware / equipos**	

Tabla 39 (Continuación)

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual			
						3.91	Intolerable
				Frecuencia (F)	R	NR	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2 **16** 4		Extremo
	N2	Daños por agua		Raro	1 **8** 3		Intolerable
	N*	Desastres naturales	La Unidad de Informática y Telecomunicaciones se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2 **16** 4		Extremo
De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (Clase C) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2 **16** 4		Extremo
	I2	Daños por agua		Raro	1 **8** 3		Intolerable
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. El sistema de aire acondicionado está fuera de servicio. La configuración del sistema de retorno del aire acondicionado no es apropiada. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.	Media	4 **32** 4		Extremo
	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3 **24** 4		Extremo
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.	Muy baja	2 **16** 4		Extremo

Tabla 39 (Continuación)

	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3	**24**	4	Extremo
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS. No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. El sistema eléctrico de la unidad no cuenta con un proceso de certificación de los productos que se utilizan ni también de la red eléctrica.	Muy baja	2	**16**	4	Extremo
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Aire acondicionado fuera de servicio. La configuración del sistema de retorno de aire acondicionado no es apropiada.	Baja	3	**24**	4	Extremo
	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.	Baja	3	**24**	4	Extremo
E	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2	**16**	4	Extremo
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor AKANE. Falta de conocimiento del administrador.	Baja	3	**24**	4	Extremo
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3	**24**	4	Extremo
	E25	Perdida de equipos		Muy baja	2	**16**	4	Extremo
Ataques intencionados	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se	Baja	3	**24**	4	Extremo
	A7	Uso no previsto		Baja	3	**24**	4	Extremo

Tabla 39 (Continuación)

A11	Acceso no autorizado	debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander. Pruebas Lógicas: En los diferentes puertos escaneados, se observó actividad importante en el puerto 43 y 80. Y en el puerto 21 se puedo tener acceso a la Shell del programa vsFTP en su versión 2.3.2.	Baja	3	**24**	4	Extremo
A23	Manipulación de equipos		Baja	3	**24**	4	Extremo
A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3	**24**	4	Extremo
A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador de Sistemas, y luego por la oficina del Administrador de Red cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola chapa de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. Vigilancia compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander.	Muy baja	2	**16**	3	Extremo
A26	Ataque destructivo	Al ser una universidad pública, periódicamente de se llevan a cabo marchas y protestas que podrían afectar los recursos de la unidad.	Baja	3	**24**	4	Extremo

El valor **NR** (Nivel de Riesgo) obedece al Mapa de Riesgos: (ver tabla 40-41)

Tabla 40. Estimación del riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	5	**5**	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	**5**	8
		1	**2**	**3**	**5**	**8**
		Impacto				

Tabla 41. Nivel de riesgo

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Servidor Akane es de 3.91, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Este mismo análisis se realizó sobre cada uno de los activos de la UIT (Documentos completos ver carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS***).

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

8. 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, transferir o mitigar) y se establecen los controles necesarios. (ver tabla 42)

Tabla 42. Tratamiento del riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Finaliza el proceso.
Tolerable	Una de las tres opciones: a. Se transfiere el riesgo por ejemplo tomando un seguro.
Intolerable	b. Se evita el riesgo retirando el activo de información.
Extremo	c. Se reduce o mitiga el riesgo por medio de controles.

Para el Servidor Akane como el Nivel de Riesgo es Intolerable; es necesario definir el tratamiento a seguir.

Primeramente, se descarta la opción de evitar el riesgo, ya que este es un activo de Muy Alto valor y el retiro del mismo no permitiría la prestación de muchos servicios fundamentales para la universidad.

La opción de transferir el riesgo por medio de la adquisición de un seguro tampoco es la adecuada, puesto que los costos de las pólizas en la mayoría de los casos son muy elevados y la universidad por ser pública, no cuenta con los recursos necesarios para adquirirlos.

No obstante, el tratamiento a seguir consiste en la definición de nuevos controles de tipo preventivo y/o correctivo que hagan posible la mitigación de riesgos y así el Servidor Akane pase de un nivel Intolerable a un nivel tolerable, o en el mejor de los casos a un nivel aceptable; que es lo que se espera que suceda con los demás activos de información que tienen un Nivel de Riesgo similar o peor. Por lo tanto, se procede a realizar el diagnostico o Análisis de Brecha para verificar los controles existentes en la unidad con respecto al estándar ISO/IEC 27002:2013 y así poder determinar con mayor claridad el tratamiento a seguir para cada uno de los activos con Nivel de Riesgo tolerable, intolerable o extremo.

8.1 ANÁLISIS DE BRECHA

El diagnóstico se realizó por medio de entrevista estructurada (audios completos carpeta ***ANEXO D – ENTREVISTAS ESTRUCTURADAS***) al coordinador, administradores y secretaria de la UIT, para lo cual se diseñó un formato conformado por un conjunto de preguntas que permitieron verificar el estado actual de los controles que aplican para la unidad con relación al estándar ISO/IEC 27002:2013. Esto se complementó con revisión documental de los procedimientos, reglamento y políticas de uso, manual de funciones y competencias laborales, formatos, hoja de vida de los servidores y verificación visual.

Una vez relevada la información, se procedió 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.

La tabla 43 muestra un fragmento del formato que puede ser consultado en su totalidad en el documento ***ANEXO E – VERIFICACIÓN CONTROLES ISO 27002***: (ver tabla 43)

Tabla 43. Formato verificación controles ISO 27002

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A5 - Política de seguridad de la información				
5.1 – Directrices de la Dirección en seguridad de la información	A.5.1.1 Conjunto de políticas para la seguridad de información.	Administrador Soporte Preventivo: ¿En la UIT existe un documento de políticas de seguridad de la información?	No existe un documento de políticas de seguridad de la información	Inicial
		Coordinador UIT: ¿En la UIT existe un documento de políticas de seguridad de la información?	No existe un documento de políticas de seguridad de la información	
		Secretaria: ¿En la UIT existe un documento de políticas de seguridad de la información?	No existe un documento de políticas de seguridad de la información	
		Verificación de documento(s) relacionados con políticas de seguridad de la información.	Existe el documento: "REGLAMENTO Y POLÍTICAS DE USO DEL CORREO ELECTRONICO, SISTEMA UNIFICADO DE COMUNICACIÓN INTERNA, PORTAL WEB, RED DE DATOS E INTERNET Y SERVICIO DE SOPORTE TECNOLOGICO DE LA UNIVERSIDAD DE NARIÑO", el cual contiene controles, recomendaciones y prohibiciones relacionadas con la seguridad de la información. También existe un manual específico de funciones y competencias laborales en el que se definen las funciones esenciales para cada cargo, donde la seguridad de la información está implícita en la realización de las actividades diarias de los funcionarios.	

Tabla 43 Formato verificación controles ISO 27002

	5.1.2 Revisión de la política de seguridad de la información.	Coordinador UIT: ¿Se revisan frecuentemente los documentos de Reglamentos y políticas de uso y el Manual específico de funciones y competencias laborales?	El documento de Reglamentos y políticas de uso y el Manual específico de funciones y competencias laborales, no se revisan de manera regular. Generalmente cuando se inicia semestre, se planifican actividades y se habla en general de la seguridad en todos los campos, pero específicamente no se analiza cada documento.	Inicial

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
	11 - Seguridad física ambiental			
11.1 - Áreas seguras	11.1.1 Perímetro de seguridad física.	Fotografías perímetros de seguridad (paredes, seguridad puertas o entradas). Ver carpeta Anexo F - Fotografías	IMG_1 e IMG_2: Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Tampoco con una cámara de seguridad. IMG_3 e IMG_4: Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Administrador Centro de Datos, y luego por la oficina del Administrador de Red cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio esmerilado, donde cada puerta cuenta con una sola cerradura de seguridad y la llave principal la manejan los dos administradores y todos sus monitores a cargo. IMG_5 e IMG_6: La ventana trasera de la sala de servidores es de vidrio normal polarizado con rejillas de metal. La vigilancia es compartida entre el Aula de informática, el kiosko y el Auditorio Luis Santander.	Repetible

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
	11.1.2 Controles físicos de entrada.	Administrador de Red de Datos: ¿Qué tipo de controles físicos de entrada implementan para garantizar el acceso únicamente a personal autorizado?	Carnet que acredite que eres funcionario de la Universidad de Nariño. En el caso de los monitores necesitan autorización del administrador para ingresar a la sala de servidores. IMG_7: La cámara de la sala de servidores se quemó y esta deshabilitada hace aproximadamente un año. Control de puertas de oficinas y sala de servidores: 3 puertas con cerraduras y cuyas llaves disponen el director de la UIT, los administradores de sistemas y de red. Los monitores solo disponen de la llave de las dos primeras puertas de acceso a las oficinas. Vigilancia: Un vigilante que hace ronda cada hora durante todo el día y la noche.	Definido
		Administrador Soporte Preventivo: ¿Qué tipo de controles físicos de entrada implementan para garantizar el acceso únicamente a personal autorizado?	IMG_8 e IMG_9: Sistema de cámaras de vigilancia. En cuanto al uso de las aulas de informática se le presta al docente que tiene asignado su espacio sin embargo en aulas libres no existe control de cuantas personas ingresan. Vigilancia con un celador compartido entre el Aula de informática, el kiosko y el Auditorio Luis Santander.	
		Administrador Portal Web: ¿Qué tipo de controles físicos de entrada implementan para garantizar el acceso únicamente a personal autorizado?	La puerta principal de acceso a la oficina de administración del portal web tienes dos chapas. Manejan las llaves únicamente celaduría y el director de la UIT.	

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
			Cámara de vigilancia de la oficina de administración del portal web está en reparación y deshabilitada hace aproximadamente 6 meses. Existen 3 cámaras en control de acceso a esta oficina.	
	11.1.3 Seguridad de oficinas, despachos y recursos.	Verificación seguridad física para oficinas, despachos y recursos (ubicación tomas, corriente, refrigeración, etc.)	IMG_38 e IMG_39: Taller de soporte correctivo ubicado en seguida a la entrada de la Biblioteca Alberto Quijano Guerrero. No existe un sistema de cámaras de vigilancia dentro de la oficina. Puerta metálica con una sola chapa de seguridad. Ventana con vidrio normal y adjunta a la puerta de ingreso del lado de la chapa de seguridad. Las demás oficinas de la unidad cuentan con puertas de ingreso de madera con vidrio esmerilado y una sola chapa de seguridad. Todas las oficinas de la unidad tienen vigilancia compartida.	Repetible
	11.1.4 Protección contra amenazas	Administrador de Red de Datos: ¿Qué tipo de medidas físicas se aplicarían en la unidad en caso de algún desastre natural?	Extintores para prevenir incendios. Cableado por canaleta de 5.	Inicial

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
	externas y ambientales	Administrador Portal Web: ¿Qué tipo de medidas físicas se aplicarían en la unidad en caso de algún desastre natural?	No existe un manual. Salud ocupacional realiza capacitaciones para desastres naturales. En la Universidad de Nariño existe una Unidad de desastres que se encargan de hacer jornadas de capacitación para los funcionarios, pero son muy esporádicas.	
		Verificación de medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	No existe sistema de alarma contra incendios. IMG_10 e IMG_11: Un solo extintor de solkaflam (Clase C). IMG_12, IMG_13, IMG_14 e IMG_15: No se utilizan paneles de obturación para el cableado en la sala de servidores. IMG_16, IMG_17, IMG_18 e IMG_19: No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. IMG_20 e IMG_21: Se puede identificar que el espacio entre cada equipo es muy limitado para que fluya el aire. Se deberían separar un poco para mejorar la ventilación entre estos equipos y así evitar que los dispositivos se sobrecalienten, disminuyan su velocidad de procesamiento y que	

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
		llegado el caso que se puedan apagar por sobrecalentamiento. Se observan algunos equipos soportando cajas, las cuales deben estar ubicadas en un estante y no sobre el hardware.	
11.1.5 El trabajo en áreas seguras.	Administrador Soporte Correctivo: ¿Qué tipo de pautas y controles físicos lleva a cabo para trabajar en la sala de servidores y demás áreas?	No existe un procedimiento establecido. Protección industrial: Utilización de guantes bioeléctricos tipo ingenieril con impedancias para voltajes mayores o hasta 32500 voltios. Botas bioeléctricas con suela que brinda protección a 2500 voltios (Código Eléctrico Colombiano NTC 2050 y RETIE)	Repetible
	Verificación seguridad en la sala de servidores (UPS, sistema de refrigeración) y demás áreas y procedimientos relacionados.	IMG_12, IMG_13, IMG_14 e IMG_15: No se utilizan paneles de obturación para el cableado en la sala de servidores. IMG_16, IMG_17, IMG_20, IMG_22, IMG_18 e IMG_19: No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos.	

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
			No están por separado los circuitos de la red regulada y normal.	
	11.1.6 Áreas aisladas de carga y descarga.	No Aplica.	La UIT no se encarga de carga y descarga de equipos, herramientas, etc.	No Aplica

Las fotografías enumeradas en esta tabla se pueden ver en la carpeta ***ANEXO F – FOTOGRAFÍAS***.

Para los cálculos totales, se determinó el promedio de valores asignados a cada **control** para obtener la calificación del **objetivo de control** al cual pertenecen, los cuales a su vez se promediaron para calcular el nivel de madurez de cada **dominio**. En la tabla X se registran algunos de los resultados (documento completo ver documento ***ANEXO G – ANÁLISIS DE BRECHA***): (ver tabla 44)

Tabla 44 (Continuación)

Tabla 44. Formato Análisis de Brecha

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
5	**Política de seguridad de la información**		**2**		**20**
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.				
5.1.1 Conjunto de políticas para la seguridad de la información	5.1 Directrices de la Dirección en SI	20	1	Inicial	20
5.1.2 Revisión de la política de seguridad de la información			1	Inicial	20
11	**Seguridad física y ambiental**		**15**		**46,7**
	El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.				
11.1.1 Perímetro de seguridad física.	Áreas seguras	40	1	Repetible	40
11.1.2 Controles físicos de entrada.			1	Definido	60
11.1.3 Seguridad de oficinas, despachos y recursos.			1	Repetible	40
11.1.4 Protección contra amenazas externas y ambientales.			1	Inicial	20
11.1.5 El trabajo en áreas seguras.			1	Repetible	40

Tabla 44 (Continuación)

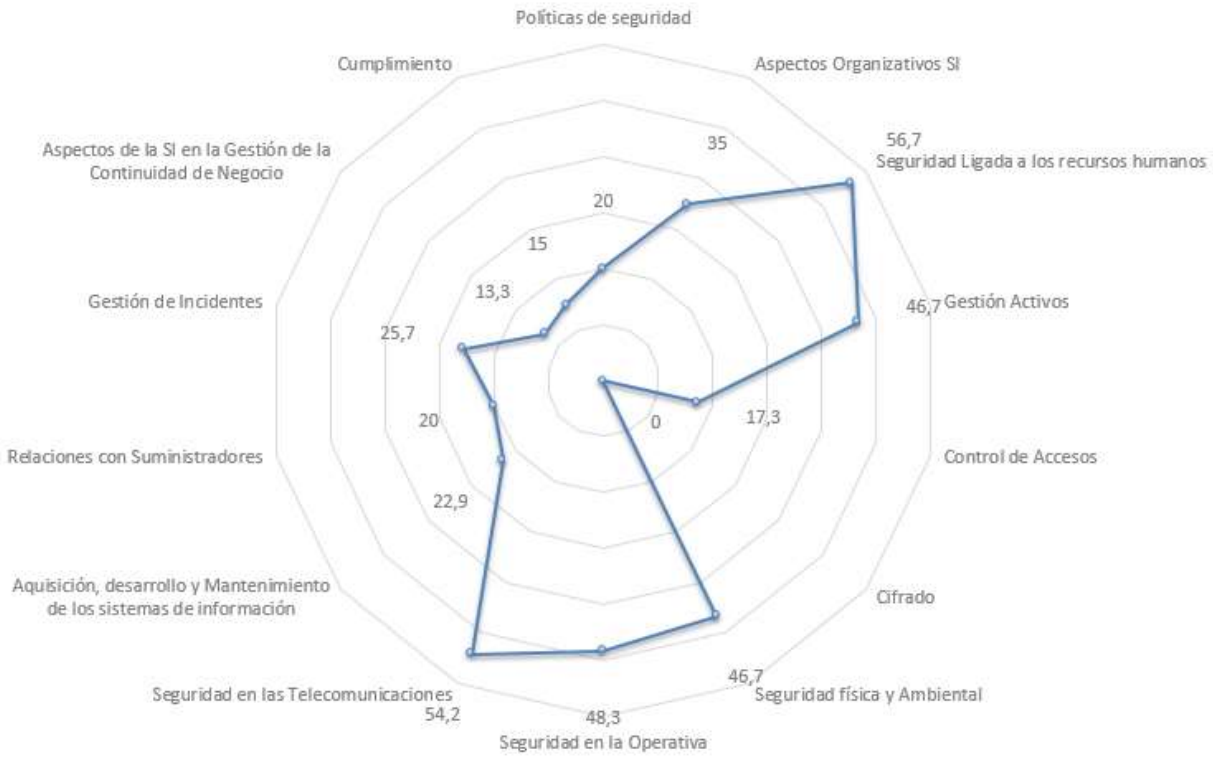
ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
11.1.6 Áreas aisladas de carga y descarga.			1	No Aplica	N/A
11.2.1 Emplazamiento y protección de equipos.	11.2 Seguridad del equipo	53,3	1	Repetible	40
11.2.2 Instalaciones de suministro.			1	Gestionado	80
11.2.3 Seguridad del cableado.			1	Repetible	40
11.2.4 Mantenimiento de los equipos.			1	Definido	60
11.2.5 Salida de activos fuera de las dependencias de la empresa			1	Definido	60
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones			1	Gestionado	60
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento			1	Definido	60
16	**Gestión de incidentes en la seguridad de información**		**7**		**25,7**
	El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.				
16.1.1 Responsabilidades y procedimientos	16.1 Gestión de incidentes de seguridad de la información y mejoras		1	Inexistente	0
16.1.2 Notificación de los eventos de seguridad de la información			1	Definido	60

Tabla 44 (Continuación)

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
16.1.3 Notificación de puntos débiles de la seguridad			1	Definido	60
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones			1	Inicial	20
16.1.5 Respuesta a los incidentes de seguridad			1	Inicial	20
16.1.6 Aprendizaje de los incidentes de seguridad de la información			1	Inexistente	0
16.2.3 Recopilación de evidencias			1	Inicial	20

Como resultado del promedio de los valores obtenidos para los 14 dominios, se concluye que frente a los controles de la norma, la Unidad de Informática, Ingeniería de Sistemas y Telemática se encuentra en un nivel de madurez **Repetible**; es decir, que se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no en todos los casos se han formalizado, ni existe comunicación formal y por lo tanto su ejecución depende de cada persona. Asimismo, no es posible detectar adecuadamente las desviaciones de la aplicación de estos ni gestionar su eficacia. (ver figura 69)

Figura 69. Nivel de madurez UIT por dominios de seguridad



Fuente. Este proyecto

Desde esta perspectiva, es necesario formalizar aquellos procedimientos que lo requieran, definir los faltantes, implementar los controles tecnológicos que se identifiquen como necesarios y establecer mecanismos que permitan llevar a cabo actividades de gestión sistemáticas enfocadas a la mejora de la seguridad de la información de 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.

Como ya hemos venido trabajando con el servidor Akane, a continuación, se indican los controles necesarios para este activo y se determina el riesgo residual esperado después de la implementación de dichos controles (ver carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS***): (ver tabla 45)

Tabla 45. Controles servidor Akane

Activo TI	**UIT-AS-A-02 Servidor Akane**	**Tipo**	**Hardware / equipos**
Administrador	**Administrador Centro de Datos**	**Degradación**	**100%**
Impacto	**8 Desastroso**	**Ubicación**	**UIT UDENAR**

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							3.91	Intolerable					2.61	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. Un solo extintor de solkaflam (Clase C).	Muy baja	2	**16**	4	Extremo	11.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	**3**	2	Tolerable
	N2	Daños por agua		Raro	1	**8**	3	Intolerable	11.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	**3**	2	Tolerable
	N*	Desastres naturales	La Unidad de Informática, Ingeniería de Sistemas y Telemática se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	**16**	4	Extremo	11.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas	Raro	1	**3**	2	Tolerable

Activo TI	**UIT-AS-A-02 Servidor Akane**	**Tipo**	**Hardware / equipos**
Administrador	**Administrador Centro de Datos**	**Degradación**	**100%**
Impacto	**8 Desastroso**	**Ubicación**	**UIT UDENAR**

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							3.91	Intolerable					2.61	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
									de desastre natural o humano.					
De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios. Un solo extintor de solkaflam (Clase C).	Muy baja	2	**16**	4	Extremo	11.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano. 11.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 11.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Raro	1	**3**	2	Tolerable

Activo TI	**UIT-AS-A-02 Servidor Akane**	**Tipo**	**Hardware / equipos**
Administrador	**Administrador Centro de Datos**	**Degradación**	**100%**
Impacto	**8 Desastroso**	**Ubicación**	**UIT UDENAR**

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							3.91	Intolerable					2.61	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
	I2	Daños por agua		Raro	1	**8**	3	Intolerable	11.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	**3**	2	Tolerable

Al resultado de esta fase se le conoce como “Informe de análisis de riesgos” equivalente a la carpeta ***ANEXO B – ANÁLISIS Y EVALUACIÓN 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”.

8.2 GESTIÓN DEL RIESGO

8.2.1 Plan de tratamiento de riesgos. El Plan de Tratamiento de Riesgos está conformado por los dominios y los controles contenidos en la ISO/IEC 27001 e ISO/IEC 27002/2013 junto con su descripción, los activos de la UIT sobre los cuales aplica cada control, la prioridad de aplicación y el estado actual del mismo. (ver tabla 46)

Tabla 46. Plan de tratamiento de riesgos

	CONTROL	ACTIVO DE INFORMACIÓN		ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad.	UIT-AS-A-05 Portal Web Universitario UIT-AS-A-06 Idiomasra UIT-AS-A-09 Inscripciones Liceo UIT-AS-A-10 Correspondencia	UIT-AS-A-12 Herbun UIT-AS-A-17 Interactiva UIT-MP-A-02 ASST	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.	Media	Definido
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	UIT-AR-A-04 BD MySQL UIT-AS-A-04 Código fuente Portal Web UIT-AS-A-13 B.D MySQL (S.I) UIT-AS-A-14 B.D Postgres (S.I)	UIT-AS-A-22 BD Correo Electrónico Institucional UIT-AS-A-33 BD MySQL (Páginas informativas) UIT-AS-MP-24 SGBD Postgres	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.	Media	Inexistente
	14.1.3 Protección de las transacciones por redes telemáticas	UIT-AS-A-05 Portal Web Universitario UIT-AS-A-06 Idiomasra UIT-AS-A-09 Inscripciones Liceo UIT-AS-A-10 Correspondencia	UIT-AS-A-11 Convocatorias UIT-AS-A-12 Herbun UIT-AS-A-17 Interactiva UIT-MP-A-02 ASST	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto.	Media	Inexistente
	14.2.2 Procedimientos de control de cambios en los sistemas	UIT-AS-A-05 Portal Web Universitario UIT-AS-A-06 Idiomasra UIT-AS-A-09 Inscripciones Liceo UIT-AS-A-10 Correspondencia UIT-AS-A-11 Convocatorias UIT-AS-A-12 Herbun UIT-AS-A-17 Interactiva UIT-MP-A-02 ASST	UIT-AS-A-50 Unidad LTO 5 UIT-AR-A-04 BD MySQL UIT-AS-A-04 Código fuente Portal Web UIT-AS-A-13 B.D MySQL (S.I) UIT-AS-A-14 B.D Postgres (S.I) UIT-AS-A-22 BD Correo Electrónico Institucional, etc.	En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.	Media	Repetible
	14.2.4 Restricciones en los cambios a los paquetes de software.	UIT-AS-A-05 Portal Web Universitario UIT-AS-A-06 Idiomasra UIT-AS-A-09 Inscripciones Liceo UIT-AS-A-10 Correspondencia	UIT-AS-A-11 Convocatorias UIT-AS-A-12 Herbun UIT-MP-A-02 ASST	Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible	Alta	Inicial

Para acceder al Plan de Tratamiento de Riesgos en su totalidad, ver ***ANEXO H – PLAN DE TRATAMIENTO DE RIESGOS***.

8.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 necesaria la implementación de una Políticas 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.

Objetivo: Proteger la información de la Unidad de Informática, Ingeniería de Sistemas y Telemática y los activos involucrados en el tratamiento de esta, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones de la Unidad.

Modelo estructura de la política de seguridad de la información

Este modelo se divide en dos partes, conformando la siguiente estructura:

- Tres temas introductorios.
- Capítulos que contienen diferentes cláusulas o dominios de seguridad de la información.

Cláusula: Dominio particular de Seguridad de la Información.
Categoría: Conjunto de controles de cada cláusula.

Cada cláusula contiene un número de categorías o conjunto de controles de seguridad. Las cláusulas (acompañadas por el número de categorías de seguridad incluidas dentro de cada cláusula).

Por último, por cada **categoría**, se establece un **objetivo** y contiene uno o más **controles** a realizar.

Resumiendo, se enuncia a continuación la estructura de cada uno de los capítulos de cada cláusula:

Capítulo de la cláusula o dominio:

- Generalidades
- Objetivos
- Alcance
- Política:
    - ✓ Categorías
        - ❖ Objetivo
    - ✓ Controles

Las Políticas de Seguridad se describen en el ***ANEXO I – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN***, proporcionando instrucciones sobre cómo mantener más seguros tanto el hardware, como la información almacenada en ellos y demás activos de información. La violación de dichas políticas puede conducir medidas disciplinarias.

9. CONCLUSIONES

La aplicación de la norma ISO/IEC 27001 y 27002 - 2013 fue útil porque proporcionó los mecanismos necesarios para identificar el nivel de madurez en seguridad de la información de la Unidad de Informática, Ingeniería de Sistemas y Telemática. Al igual que definir las recomendaciones que mejor se adapten a la organización.

La etapa de recolección de información y documentación es fundamental desarrollarla detalladamente obteniendo los datos necesarios, para evitar que posteriormente se deba recurrir a recuperar datos faltantes, que influyan presentando variaciones en el análisis y evaluación de riesgos afectando la confiablidad de los resultados.

MAGERIT es útil para las organizaciones que inician con la gestión de seguridad de la información, ya que permiten enfocar esfuerzos en los riesgos que pueden ser más críticos.

Una vez determinado el nivel de riesgo para cada activo de información de la Unidad de Informática, Ingeniería de Sistemas y Telemática se concluye que para activos de alto y muy alto valor y con un nivel de riesgo intolerable o extremo, el tratamiento recomendado para mitigación de riesgos es la definición de nuevos controles de tipo preventivo y/o correctivo.

Se hace necesario precisar que el hecho que una organización implemente un Sistema de Gestión de Seguridad de la Información no garantiza seguridad al 100%, ya que es imposible, por el contrario, si garantiza que se minimicen sus riesgos y de igual manera el impacto que tendrían si se materializará el riesgo.

Es de gran importancia crear una cultura de seguridad en cada uno de los empleados de la organización, ya que las transformaciones no siempre son aceptadas con facilidad, lo anterior encaminado a que el Sistema de Gestión de Seguridad de la Información genere un alto nivel de seguridad en los procesos.

La Unidad de Informática, Ingeniería de Sistemas y Telemática se encuentra en un nivel de madurez Repetible; es decir, se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no en todos los casos se han formalizado, ni existe comunicación formal y por lo tanto su ejecución depende de cada administrador.

10. RECOMENDACIONES

Es conveniente que el apoyo por parte de la Dirección de la organización donde se lleve a cabo un proyecto de este tipo se soporte mediante un documento escrito que especifique los niveles de acceso a la información e instalaciones de procesamiento para facilitar el ingreso y obtención de la documentación.

Para un adecuado manejo del inventario de activos de información, se recomienda organizarlo por áreas o dependencias que conforman la organización.

Para la identificación de amenazas es importante 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, Ingeniería de Sistemas y Telemática mediante la aplicación de auditorías internas.

Según el análisis de brecha realizado se debe hacer énfasis en el cifrado de la información pues no se aplica ningún tipo de controles y en la gestión de continuidad del negocio ya que se debe preservar la seguridad de la información durante las etapas de activación, desarrollo de procesos, procedimientos y planes para la continuidad y de retorno a la normalidad.

Realizada la estructuración del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática, Ingeniería de Sistemas y Telemática, es fundamental el apoyo de la coordinación y de todo el personal encargado, para posterior implementación del sistema por parte de los directivos de la Universidad de Nariño.

BIBLIOGRAFÍA

BELL Timothy, PEECHER Mark E, SOLOMON Ira, MARRS, Frank y THOMAS, Howard. Auditoría basada en riesgos. Perspectiva estratégica de sistemas: ECO Ediciones. 2008, 300p. ISBN 978-958-648-512-8.

BISIGROUP. Seguridad de la información ISO/IEC 27001. [en línea]. <http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001> [citado marzo de 2018].

CADME RUIZ C.M., DUQUE POZO, D.F: Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos Cía. Ltda"Quito, 2012, 120h. Trabajo de Grado (Ingeniero de Sistemas). Universidad Politécnica Salesiana. Facultad de Ingeniería. Programa de Ingeniería de Sistemas.

CANOSA Maximiliano. La importancia de los procesos de seguridad de la información. [en línea]<http://www.slideshare.net/foroglobalcrossing/la-importancia-de-los-procesos-de-seguridad-de-la-informacin-ventajas-y-eficiencia-de-aprovechar-la-experiencia-global> [citado mayo de 2018].

Estándar Internacional ISO/IEC 27001:20013

LOPEZ NEIRA Agustín. Iso 27001 en español [en línea]. <http://www.iso27000.es/index.html> [citado mayo de 2018].

MATUTE Macias, QUISPE Cando: Auditoría de la gestión de seguridad en la red de datos del Swissotel basada en COBIT. Quito, 2006, 90h. Trabajo de Grado (Ingeniero de Sistemas). Escuela Politécnica Nacional. Facultad de Ingeniería. Programa de Ingeniería de Sistemas.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT Versión 3.0

MINISTERIO DE LAS TIC. Gobierno en línea. Decreto 1151 de 2008. [en línea]. <http://programa.gobiernoenlinea.gov.co/apc-aa files/5854534aee4eee4102f0bd5ca294791f/Decreto1151Abril14de2008.pdf> [citado abril de 2018].

PIATTINI Velthuis, NAVARRO E, Ruiz M: Auditoría de tecnologías y sistemas de información. México: Grupo Editor Alfaomega. 692p. ISBN 9789701513781

UNIVERSIDAD DE OVIEDO. Seguridad en redes inalámbricas: Una guía básica. [en línea] <http://www.isa.uniovi.es/docencia/redes/Apuntes/tema8.pdf> [citado marzo de 2018].

NETGRAFIA

BACKTRACK. [en línea] Disponible en internet. http://es.wikipedia.org/wiki/BackTrack. [citado abril de 2018].

CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado abril de 2018].

¿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 2018].

DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado mayo de 2018].

DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado mayo de 2018].

EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado marzo de 2018].

ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado marzo de 2018].

LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado mayo de 2018].

LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado mayo de 2018].

LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado mayo de 2018].

LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado mayo de 2018].

LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado abril de 2018].

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 2018].

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 2018].

SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado abril de 2018].

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 2018].

UNIDAD DE INFORMÁTICA, INGENIERÍA DE SISTEMAS Y TELEMÁTICA. Proyecto UIT. Pasto: Universidad de Nariño, Aula de informática, 2009. [en línea] Disponible en internet. http://uit.udenar.edu.co/. [citado febrero de 2018]

ANEXOS

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

Anexo A - Inventario activos de información
Anexo B - Análisis y evaluación de riesgos
Anexo C - Ethical hacking
Anexo D - Entrevistas estructuradas
Anexo E - Verificación controles ISO 27002
Anexo F – Fotografías
Anexo G - Análisis de brecha
Anexo H - Plan de tratamiento de riesgos
Anexo I - Políticas de seguridad de la información
Anexo J - Plantillas y tablas
Anexo K - Plan para la implementación del SGSI