DISEÑO DE UN PLAN DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD FÍSICO Y LÓGICO DE ACUERDO CON MODELOS DE GESTIÓN DE LA INFRAESTRUCTURA DE REDES APLICABLE A UNA INSTITUCION EDUCATIVA

CRISTIAN CAMILO JAIME BATANERO

CÓDIGO 1400481

DIEGO ALEJANDRO BELTRAN MUÑOZ

CÓDIGO 1400459

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

BOGOTÁ D.C. 2012

DISEÑO DE UN PLAN DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD FÍSICO Y LÓGICO DE ACUERDO CON MODELOS DE GESTIÓN DE LA INFRAESTRUCTURA DE REDES APLICABLE A UNA INSTITUCION EDUCATIVA

CRISTIAN CAMILO JAIME BATANERO

CÓDIGO 1400481

DIEGO ALEJANDRO BELTRAN MUÑOZ

CÓDIGO 1400459

Trabajo de grado presentado como requisito para optar por el título de Ingeniero en Telecomunicaciones

DIRECTOR

Ing. Ricardo Alfonso Pinto García

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

BOGOTÁ D.C. 2012

Luis Eduardo Tabares
Jurado

Luis Fernando González
Jurado

Bogotá D.C 16 de Mayo del 2012
Ciudad y Fecha

A Dios,

A nuestros padres y familiares,

A nuestros compañeros,

A nuestros docentes,

A nuestra Universidad,

A la Academia Nacional de Sistemas,

A los que creyeron en nosotros siempre y nos dieron fuerzas para seguir adelante.

AGRADECIMIENTOS

La culminación de este proyecto no habría sido posible sin el constante apoyo y colaboración de aquellas personas e instituciones que aportaron desinteresadamente de una u otra manera a nuestro crecimiento personal y profesional, durante nuestros estudios y durante el desarrollo de este proyecto. Especialmente queremos agradecer:

- ***A Dios**, por brindarnos la fe y la esperanza en momentos de desiertos, por poner en nuestro camino pruebas en donde no siempre se gana, enseñándonos a levantarnos y continuar con nuestro camino, como también pruebas donde salimos victoriosos, para aprender a valorar todo lo que tenemos a nuestro alrededor: la familia, los amigos y nuestra propia vida.*
- ***A Nuestros Padres,** por su esfuerzo constante para poder suplir todas nuestras necesidades, por enseñarnos el camino correcto, por estar ahí cuando se presentaron adversidades, por sus buenos consejos y porque todo lo que somos se lo debemos a ellos.*
- ***A Nuestros Hermanos,** por ser nuestros compañeros, por sacarnos una alegría en momentos de tristeza, por ser nuestro apoyo y demostrarnos todo su amor día tras día.*
- ***A Nuestro Director De Proyecto, Ricardo Pinto,** quien demostró un gran compromiso e interés con nuestro proyecto brindándonos sus conocimientos, experiencias y opiniones para la culminación de este trabajo y nuestra carrera.*
- ***A Nuestros amigos, Mónica Alejandra Macías, Germán Fabián Ochoa, Leonardo y Miguel Ángel Barriga,** por haber estado con nosotros en este largo camino, por brindarnos momentos de alegría, por todas las experiencias que compartimos y que aunque pasara lo que pasara nos demostraron que siempre podíamos contar con ellos.*
- ***A Nuestros Compañeros, Juan Carlos Sarmiento, David Saboya, Cristian Rivera, William Reyes, Iván Mendoza y Andrés Pardo** y a todos nuestros otros compañeros, de quienes aprendimos muchas cosas útiles a lo largo de estos años, fue un gran honor haber compartido con ellos.*
- ***A nuestros Docentes Y A La Universidad Militar Nueva Granada,** quienes nos inculcaron los conocimientos necesarios para terminar con la formación profesional competente, con ética, con valores y con responsabilidad.*

TABLA DE CONTENIDO

LISTA DE ANEXOS

LISTA DE DIAGRAMAS E IMÁGENES

LISTA DE TABLAS

1. INTRODUCCION

Con la evolución de la tecnología, los grandes avances en los sistemas y su relación con los objetivos de competencia entre organizaciones, se hace necesario aumentar los niveles de protección de uno de los activos más valiosos que estas poseen, la información, la cual se encuentra dentro de un universo de amenazas y vulnerabilidades que con el tiempo aumentan, todo esto con el fin de garantizar siempre la disponibilidad, la confidencialidad e integridad de la misma. Una de las formas más adecuada para la protección de la información es mediante una correcta gestión del riesgo, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos.

Esto, ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de los activos de información para obtener el mayor provecho y evitar la vulnerabilidad de estos. Es así, por lo que la seguridad lógica surge como una herramienta que ayuda a la organización a tomar sensibilidad sobre la importancia de la información y los servicios que permiten que la empresa se desarrolle y se mantengan dentro del mundo de los negocios.

De acuerdo con lo anterior, la implementación del sistema de seguridad requiere un alto compromiso con la organización, destreza y experimentación técnica que permita determinar las fallas y debilidades que se presentan en la organización, y constancia por parte de los miembros de esta para la renovación y actualización del sistema de seguridad, para así, entrar en el ambiente de las organizaciones modernas.

1.1 TITULO

El titulo de este proyecto responde a la necesidad de mejorar y ampliar los niveles de seguridad física y lógica de una institución educativa de la ciudad de Florencia Caquetá, mediante la integración de los sistemas de control de acceso e intrusión, sistemas de video, vigilancia inteligente y seguridad para el acceso a las redes de datos, teniendo en cuenta modelos de gestión de la infraestructura de red.

Específicamente, el proyecto atiende la necesidad de seguridad de la ACADEMIA NACIONAL DE SISTEMAS de Florencia Caquetá, cuyo objeto social es la formación

técnica y profesional de los habitantes de la región, con lo cual el proyecto permitirá elevar la calidad y oportunidad de su objetivo. Por lo descrito anteriormente el proyecto se titula "DISEÑO DE UN PLAN DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD FÍSICO Y LÓGICO DE ACUERDO CON MODELOS DE GESTIÓN DE LA INFRAESTRUCTURA DE REDES APLICABLE A UNA INSTITUCION EDUCATIVA"

1.2 PLANTEAMIENTO DEL PROBLEMA

El sector educativo, más específicamente la Academia Nacional de Sistemas, maneja una gran volumen de información a diario dentro de sus bases de datos como lo son: El registro de notas y control académico en línea, el control de pagos de matriculas, las bibliotecas virtuales y la página Web, estos procesos son soportados por una infraestructura de hardware que se encuentran al alcance de cualquier usuario sin ninguna restricción. Es por esto, que la institución se ve en la necesidad de mejorar el sistema de seguridad físico e informático que maneja actualmente. Dentro de las falencias encontradas están: un circuito cerrado de televisión sin protección, una base de datos desprotegida y un sistema de red inseguro, incrementado por el rápido crecimiento de la planta física de la institución.

Todo esto denota que la institución no presenta estudios de seguridad que contemplen lo anteriormente descrito, lo cual crea una necesidad de disponibilidad para crear políticas de seguridad que salvaguarden la información tanto lógica como física. A raíz de estos requerimientos se plantea la siguiente pregunta:

¿El diseño e implementación de un plan de mejoramiento del sistema de seguridad estandarizado en norma ISO 27001, permitirán mejorar la calidad y oportunidad de los procesos que se generan dentro de la institución?

1.3 LINEA DE INVESTIGACION

El presente proyecto pertenece a la línea de investigación relacionada con el tema de seguridad en comunicaciones del Grupo de Investigación en Seguridad y Sistemas de Comunicaciones (GISSIC) de la Universidad Militar Nueva Granada, con lo cual se le dará un enfoque hacia la parte de diseños de redes de seguridad y la gestión de riesgos para

empresas que brindan diversos tipos de servicios y necesitan mantener un nivel de seguridad en sus instalaciones.

1.4 OBJETIVOS

1.4.1 Objetivo General

Diseñar un plan de mejoramiento para el sistema de seguridad físico y lógico de acuerdo con modelos de gestión de la infraestructura de redes, aplicable a una institución educativa con el fin de optimizar los procesos que se generan dentro de la Academia Nacional de Sistemas.

1.4.2 Objetivos Específicos

- Hacer un levantamiento de información referente al estado de los equipos y software utilizados en las dependencias de la institución.
- Generar un diagnóstico de los estándares y normas que se aplican en la actualidad para el servicio de seguridad dentro de la Academia Nacional de Sistemas.
- Realizar una propuesta de los equipos necesarios y plantear un presupuesto aproximado para su implementación en la institución.
- Realizar el diseño de red y las políticas de seguridad basados en el estándar ISO27001 que garanticen la funcionalidad y evite la vulnerabilidad de la red.
- Aplicación del estándar para integración de servicios que ofrece la institución basados en Cloud Computing **[1]**.
- Implementar el diseño físico correspondiente para la evaluación de los resultados y ejecución del piloto.

1.5 JUSTIFICACION

Los grandes avances tecnológicos están haciendo presencia dentro de nuestra sociedad, estos avances han revolucionado la manera en que el hombre se comunica, lo cual atrae novedosos retos que permiten el buen funcionamiento de los métodos utilizados para comunicarnos. Día a día nacen nuevos términos que hacen referencia al rendimiento y

buen funcionamiento de las redes, obligando a la innovación en nuevos campos como la disponibilidad, flexibilidad, seguridad entre otros.

En la actualidad uno de los recursos más valiosos que poseen las instituciones es la información, esta se encuentra fuertemente unida a la infraestructura, servicios y economía que estas manejan. El crecimiento del volumen de información confidencial, como claves de acceso, bases de datos e información valiosa que se comparte, exige que se tomen medidas con respecto a la forma en que ésta se transmite. Por estas y otras razones más, se presentó la necesidad de implementar sistemas de seguridad en las redes de datos, medidas de seguridad en la infraestructura, para que de esta forma se garantice que la información llega al destino deseado **[2]**, respetando los pilares de seguridad.

Económicamente se presenta rentabilidad debido a que el beneficio ofrecido por estos sistemas es inmenso y se ajusta a las necesidades de la institución. Los costos generados por perdidas de información, hurto dentro de la misma y perdida de equipos se evitarían y así se invertiría este capital en desarrollo y mejoramiento de los procesos dentro de la entidad.

1.6 ALCANCE

El presente proyecto busca mejorar el sistema de seguridad físico y lógico de la Academia Nacional de Sistemas, implementando un estándar para su futura certificación, la utilización e implantación de nuevos equipos, con el fin de generar beneficios en la calidad de los servicios ofrecidos por esta.

1.7 DESCRIPCION DE LA ORGANIZACIÓN

Este trabajo se desarrollará para la Academia Nacional de Sistemas, ubicada en el Departamento del Caquetá; ya que esta se encuentra en crecimiento y busca el mejoramiento continuo, mantenimiento e investigación en los aspectos de la implementación de nuevas tecnologías y sistemas de prevención y seguridad.

1.7.1 Misión

Formar personas íntegras, responsables y creativas, con sólidas aptitudes para el trabajo en el campo de los sistemas, la contabilidad, las finanzas y el idioma inglés. Asimismo, desarrollar en los educandos competencias pertinentes con el sector productivo y académico, a través de metodologías innovadoras y participativas, estableciendo cadena de formación con la educación media, técnica, tecnológica y profesional, contribuyendo así, con el desarrollo regional y nacional **[3].**

1.7.2 Visión

La Academia Nacional de Sistemas será el instituto de formación para el trabajo y desarrollo humano más importante del departamento del Caquetá. Al mismo tiempo, se compromete a implementar programas con innovación tecnológica, en aras de ser una institución que contribuya con la formación de personas no solamente competitivas, sino también con criterios de calidad y pertinencia laboral. Lo anterior, con el fin de formar individuos responsables, críticos y analíticos, que sean capaces de potenciar el desarrollo tecnológico y de responder, de manera idónea, a las necesidades específicas de la región y del país **[3].**

1.7.3 Naturaleza Institucional

La Academia Nacional de Sistemas es una institución educativa que nació en la ciudad de Florencia, el 26 de agosto de 1991, en virtud de la resolución 00439, como respuesta a una necesidad de los sectores productivos de la economía del Caquetá en áreas administrativas, teniendo como objetivo la formación y la capacitación de personal profesional, con programas presenciales de formación continua, complementación y actualización, dirigidos al área de servicios financieros, informática e inglés.

Los programas implementados toman como objeto de estudio la población estudiantil y productiva del departamento del Caquetá, y parte de un diagnóstico que estudia la situación real en lo referente a las necesidades informáticas, contables, administrativas e inglés en el campo laboral, del sector privado y oficial.

Por medio de los programas de educación continuada y permanente, la Academia busca una mayor integración con la comunidad que le permita aplicar los conocimientos al proceso de identificación y resolución de problemas cotidianos de mediano y largo plazo.

1.8 Estructura organizacional de la Academia Nacional de Sistemas

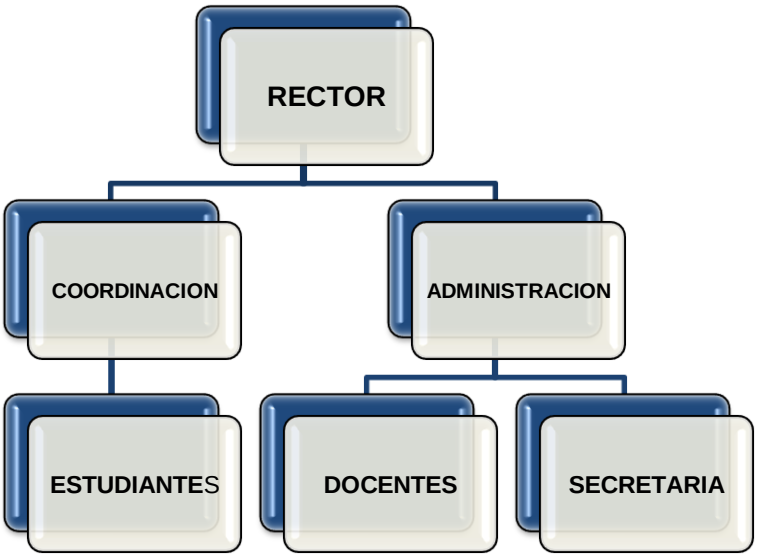


Figura 1. Organigrama General ACADEMIA NACIONAL DE SISTEMAS

2. MARCO TEORICO

2.1 ESTADO DEL ARTE

En la actualidad los sistemas y redes habitualmente están expuestos a diversos ataques electrónicos, éstos son tan frecuentes que se crea la necesidad de implementar requerimientos de seguridad que protejan los equipos y los datos almacenados en ellos. Las vulnerabilidades de los equipos se detectan por medio de herramientas del sistema a nivel de red, estas herramientas permiten la corrección de problemas y errores de configuración que ocasionan fallas en la seguridad de un sistema de información.

Haciendo un análisis de los sistemas actuales se detecta que los ataques a estos pueden ser externos a éste o provenientes del interior, como por ejemplo, usuarios autorizados o intrusos que se hacen pasar como usuarios autenticados por el sistema.

En la implementación de sistemas de seguridad, objeto de este trabajo de grado se tomaron como referencia proyectos desarrollados en otros países y ámbitos diferentes, cuyos resultados permitieron ser una guía para la elaboración del presente proyecto. A continuación se describen algunos de ellos.

En el año 2008, en la Universidad Politécnica de Cataluña, se llevó a cabo una propuesta de diseño de una red de seguridad que tenia por nombre “Sistema integral de seguridad y acceso a la red para un departamento de la UPC”, en la cual se lograron grandes beneficios en el área de rendimiento y calidad de los servicios requeridos por esta dependencia, además es bueno resaltar que esta implementación fue realizada sobre software libre lo que le dio una mayor flexibilidad al proyecto.

En Venezuela se diseñó e implementó un Sistema Integral de Respaldo y Recuperación (SIRR), para toda la plataforma tecnológica del Banplus Banco Comercial, C.A. en primer lugar se inició con el levantamiento de información, el análisis del ambiente a ser protegido, la selección del equipamiento de respaldo adecuado a las necesidades del cliente y finalmente el diseño y establecimiento en conjunto con el personal de IT de BANPLUS del esquema de respaldo y recuperación.

En Colombia, la Universidad de los Andes (Bogotá) diseñó un “Esquema de Seguridad en Redes de Datos” en donde se hacia el análisis de vulnerabilidades aplicados a la empresa

las cuales fueron objeto de estudio. Estas amenazas se evaluaron con el fin de identificar las variedades de daños que podían causar y las probabilidades de que siguieran ocurriendo. Se suministraron herramientas que soportan el acceso a Internet de forma segura, se capacitó a los usuarios sobre el alto grado de importancia que tiene la información.

Lo anterior se describe con el fin de dar seguridad a los procedimientos que se desean implementar en la Academia Nacional de Sistemas, para posteriormente facilitar el soporte y atención de incidentes relacionados con los sistemas de seguridad.

2.2 MARCO CONCEPTUAL

Los conceptos generales que se van a tener en cuenta para el desarrollo del proyecto son los que a continuación se describen:

2.2.1 Seguridad Lógica

La seguridad es la protección de la infraestructura digital, lo cual comprende, la información, los datos, el software y las bases de datos que se almacenan dentro de un equipo de cómputo. Esto se encuentra regulado por una serie de estándares, herramientas y leyes creadas, con el fin de disminuir los riesgos que puedan presentarse en la infraestructura digital de las empresas.

La Seguridad Lógica, también se puede definir como una "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita el acceso a las personas autorizadas para hacerlo." **[4]**

Entre los objetivos que enmarca la seguridad lógica se encuentran:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Certificar que se estén utilizados los datos, archivos y programas correctos.
4. Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.2.2 Control de Accesos (Seguridad Informática)

El control de acceso es un medio de gran ayuda cuando se trata de proteger el sistema operativo, las aplicaciones y la información de los equipos de la institución de la utilización o modificaciones no autorizadas; para mantener la integridad de la información, lo cual se logra restringiendo la cantidad de usuarios y procesos con acceso permitido, con el fin de proteger el sector lógico de algún tipo de acceso no autorizado.

Estos controles pueden ser implementados sobre el Sistema Operativo (SO), sobre los sistemas de aplicación, en las bases de datos, en paquetes específicos de seguridad o en cualquier otro elemento lógico de la entidad.

2.2.3 Perfil de Usuario

El acceso a los equipos también puede ser controlado a través del perfil y del cargo de cada uno los usuarios que requieren dicho acceso.

En la institución algunos de estos cargos son los siguientes: Administrador, asistentes de oficina, docentes y estudiantes.

- **Administrador:** En este cargo se encuentra el rector de la academia, el cual tiene acceso a todos los procesos de la institución sin dejar de lado sus funciones como verificador del estado de la red.

- **Asistentes de oficina:** Están directamente encargadas con el ingreso y registro de los estudiantes a las bases de datos de la academia, tienen privilegio acceso a toda la red de la academia.

- **Docentes:** Tienen asignado un computador especifico dentro de la academia y de acuerdo a la asignatura que dictan, tendrán instalados los programas necesarios para el desarrollo de las clases.
- **Estudiantes:** No Se les aplican las restricciones adecuadas para hacer su proceso académico más ameno.

Para este caso los derechos de acceso pueden agruparse y limitarse de acuerdo con el cargo de cada uno de los usuarios.

2.2.4 Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Por ejemplo, para la Academia Nacional de Sistemas donde se disponen de licencias para la utilización simultánea de un determinado producto de software para cinco personas, la limitación se hace en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

2.2.5 Niveles de Seguridad Informática

Para definir los niveles de seguridad, es necesario conocer el estándar de mayor uso internacionalmente que es el TCSEC Orange Book, el cual fue desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos **[4]**.

Los niveles de seguridad describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad hasta el máximo. Los niveles de seguridad a su vez, han sido la base de desarrollo de estándares europeos como por ejemplo ITSEC/ITSEM y también abarcando los internacionales como lo son ISO/IEC.

A continuación se muestra la clasificación en cuanto a niveles de seguridad informática y lógico, los cuales son:

- **Nivel D [4]**

Este nivel solo está hecho para sistemas que al haber sido evaluados, se encuentra que no cumplen con ninguna especificación de seguridad.

Cuando no hay seguridad para el hardware, el sistema operativo comienza a ser inestable y no presenta autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que incluye este nivel son MS-DOS y System 7.0 de Macintosh.

- **Nivel C1: Protección Discrecional [4]**

Es necesaria la identificación de los usuarios para que se permita el acceso a la información. Cada usuario tiene derecho al manejo de su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien toma el control total de accesos.

La gran mayoría de las tareas de administración del sistema sólo pueden ser realizadas por este "súper usuario" quien se ocupa de la seguridad del mismo. Con la actual descentralización de los sistemas de informáticos, no sería raro encontrar dos o tres personas encargadas de estas tareas en una organización. Esto podría ser un problema, ya que no habría manera de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios y grupos de objetos sobre los cuales podrán actuar usuarios o grupos de ellos.

- Identificación y Autentificación: Los usuarios deben identificarse antes de comenzar a ejecutar cualquier acción en el sistema.

- **Nivel C2: Protección de Acceso Controlado [4]**

Este subnivel se creó con el fin de dar solución a las debilidades presentadas en el nivel C1. Cuenta con características adicionales que mejoran el ambiente de accesos controlados. Se ve la necesidad de llevar una auditoria de accesos e intentos fallidos de acceso.

Tiene la capacidad de restringir el acceso a ciertos archivos, también restringe el uso de comandos que puedan mostrar elementos ocultos, así mismo, puede permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere auditoria del sistema. Esta auditoría se utiliza para llevar todos registros de las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y los usuarios.

Esta auditoría necesita de una autenticación adicional para verificar que la persona que ejecuta el comando es quien dice ser. Presente una gran desventaja, esta es que el nivel C2 reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Algunos de los usuarios de los sistemas que utilizan seguridad de nivel C2 tienen la autorización para realizar cualquier tarea de administración del sistema sin tener q ser administrador de este.

- **Nivel B1: Seguridad Etiquetada [4]**

Este subnivel, tiene la capacidad de soportar seguridad multinivel, como lo son la seguridad secreta y ultra secreta. En este nivel, se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato) le es asignada una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado) y con unas categorías (contabilidad, nóminas, ventas).

Cada usuario para poder acceder a un objeto debe tener un permiso expreso para hacerlo y viceversa.

- **Nivel B2: Protección Estructurada [4]**

Requiere que cada objeto de nivel superior tenga una etiqueta de este mismo nivel para demostrar que es padre de un objeto nivel inferior.

La Protección estructurada es la que empieza a referir el problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Así, un disco duro será etiquetado por almacenar archivos que pueden ser accedidos por distintos usuarios.

Este sistema es capaz de generar alertas a los usuarios si sus condiciones de accesibilidad y seguridad han sido modificadas; y el administrador es el que se encarga de la fijación los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

- **Nivel B3: Dominios de Seguridad [4]**

El nivel B3, es el encargado de reforzar los dominios con la instalación de hardware: por ejemplo, el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un motor de referencia, el cual recibe las peticiones de acceso de cada usuario y permite o deniega las peticiones según las políticas de acceso que hayan sido definidas.

Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

- **Nivel A: Protección Verificada [4]**

Este es el nivel de mayor seguridad, en el, se incluyen los procesos de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario dentro del sistema.

Para implementar a este nivel de seguridad, todos los componentes de los niveles inferiores deben ser incluidos. El diseño debe ser verificado de forma matemática y también se deben realizar los respectivos análisis de los canales encubiertos y de

distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

2.2.6 Seguridad Física

La seguridad física es uno de los componentes más olvidados cuando se trata de realizar el diseño de un sistema informático. La seguridad física se refiere a la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". La seguridad física abarca los diferentes controles y mecanismos de seguridad que se instalan dentro y alrededor del centro informático, así como los medios de acceso remoto al medio. **[5]**

Este tipo de seguridad se enfoca en el cubrimiento de las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre (robos, daños).
3. Disturbios, sabotajes internos y externos deliberados.

Se nombran algunos peligros que pueden ocurrir en un centro de procesamiento; todo esto con el fin de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos **[6].**

- Incendios
- Inundaciones
- Condiciones climatológicas
- Ergometría
- Robo

- Fraude
- Sabotaje

2.2.7 Sistema Integrado de Seguridad

Un Sistema Integrado de Seguridad es un conjunto de elementos necesarios que, relacionados entre sí, contribuyen a prevenir riesgos y asegurar el buen funcionamiento de las instalaciones e información, evitando y disminuyendo las probabilidades de falencias dentro de las instalaciones **[7]**.

Existen diferentes tipos de sistemas Integrados de Seguridad que disponen de sistemas de Detección de Incendios, Control de Accesos e Intrusión, Circuito Cerrado de Televisión (CCTV) y Seguridad de Red que satisfacen las necesidades de los clientes con tecnología avanzada. Asimismo, es de gran importancia que estos sistemas sean eficaces, flexibles y de fácil manejo reduciendo así los diferentes errores típicamente cometidos por el operador. Son útiles y presentan un alto rango de aplicaciones en diferentes entornos permitiendo variar desde la gestión sistemática de alarmas hasta el control de los elementos del sistema **[8]**.

2.2.8 Control de acceso para seguridad física

El control de acceso es un aspecto muy importante cuando se habla de seguridad, este no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

- Utilización de guardias
- Detectores de metales
- Utilización de sistemas biométricos
- Protección electrónica

Para lograr una seguridad integral se requiere evaluar permanentemente los riesgos que puede presentar la infraestructura ya que es la base para o comenzar a integrar la seguridad como la prioridad dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

2.2.9 Cámaras IP

Las cámaras IP (ver figura 3) tienen como característica principal que cuentan con un servidor web de video incorporado, lo que les permite poder transmitir su imagen o capturas a través de redes IP como redes LAN, WAN e INTERNET.

Las cámaras IP ofrecen un gran servicio, permiten que el usuario pueda ubicar la cámara en un lugar determinado y a su vez poder ver el vídeo que esta genera en tiempo real desde cualquier otra ubicación por medio de Internet.

Las cámaras IP contienen internamente un ordenador, de tamaño pequeño pero a su vez enfocado en ejecutar aplicaciones de red. Por esta razón es bueno tener en cuenta que a diferencia de las cámaras web, una capara IP no necesita estar conectada a un computador para poder funcionar.

Algunas de las grandes ventajas que presentan las cámaras IP son:

- Las cámaras IP brindan una mayor resolución con respecto a las cámaras de video tradicionales o de las también denominadas webcams.
- Las cámaras IP permiten al usuario observar en tiempo real lo que está sucediendo en un lugar determinado, aunque este se encuentre en otro lugar distinto.

- Las cámaras IP pueden ser vistas sólo por las personas autorizadas. También se puede ofrecer acceso libre y abierto si el vídeo en directo se desea incorporar al web site de una compañía para que todos los internautas tengan acceso.

- Las cámaras IP gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen.

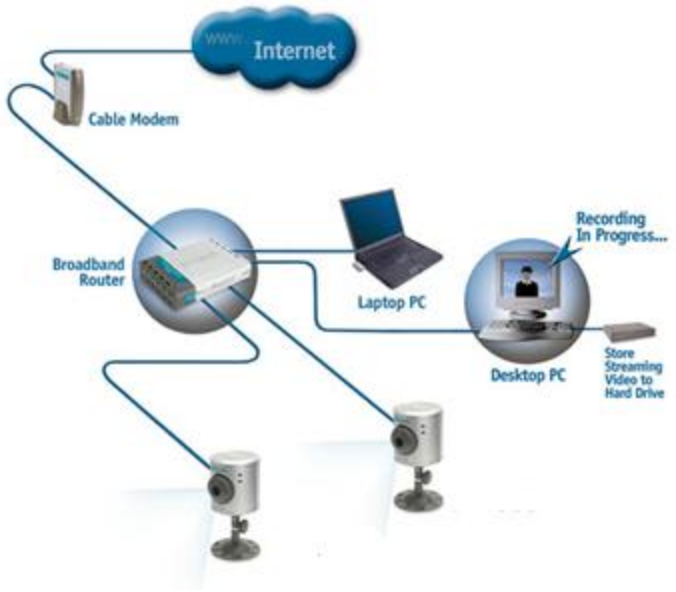


Figura 2. Diagrama Conexión Cámaras IP[1]

Características de las Cámaras IP

- Tienen una resolución lo suficiente para reconocer las acciones que se están desarrollando en un determinado lugar.

- Permiten ser controladas de manera remota, por medio de cables ó de manera inalámbrica, ya que son capaces de transmitir la señal a través de la red inalámbrica.

[1] *Tomado de http://mydlink.dlink.com/products*

- Cuentan con movimiento giratorio remoto en varias direcciones (tecnologías PAN/TILT), lo que permite enfocarla al lugar deseado de manera inmediata.

- Con respecto al audio y video que capturan, es transmitido en formatos comprimidos, diseñados para un flujo rápido en Internet (GSM-AMR/MPEG4 y AAC "Advanced Audio Coding").

- Como la transmisión es enfocada hacia Internet, es posible observar los eventos desde cualquier dispositivo que tenga una conexión y un explorador de Internet.

2.2.10 UPS (Uninterruptible Power Supply) [9]

Una UPS se define como una fuente de suministro eléctrico, la cual posee una batería, con el fin de ofrecer una continuidad en el sistema de energía al dispositivo que se encuentre conectado, en el caso que se presente una interrupción eléctrica. Las UPS también son conocidas como SAI (Sistema de alimentación ininterrumpida).

Las UPS se conectan a la alimentación de los computadores, permitiendo de esta manera usarlas varios minutos después de que se produzca un corte eléctrico. Algunas UPS ofrecen aplicaciones que se encargan de realizar algunos procesos automáticamente en los casos en los que el usuario no se encuentre presente y se corte la electricidad.

Tipos de UPS

Las UPS se pueden clasificar en dos tipos distintos los cuales se analizaran a continuación:

- SPS (standby power systems): Tiene como objetivo monitorear la entrada de energía, detectando cualquier tipo de problema que se pueda presentar en el suministro de energía para de este modo cambiar a la batería. Cabe resaltar que este cambio puede demorar algunos milisegundos.

- UPS on-line: Este tipo de UPS evita los milisegundos que se producen cuando hay un corte de energía, ya que genera una alimentación constante desde su batería y no de forma directa.

Componentes de las UPS

- Rectificador: como su nombre lo indica, está encargado de rectificar la corriente alterna de entrada, suministrando corriente continua para cargar la batería. Desde la batería se alimenta el inversor que nuevamente convierte la corriente en alterna. Cuando se descarga la batería, necesita de un tiempo estimado de 8 a 10 horas, para volver a cargarse.

- Batería: Es la encargada de proveer la energía en caso de interrupción de la corriente eléctrica. Su capacidad, es dependiente de la cantidad de tiempo que puede suministrar energía sin alimentación.

- Inversor: Es el que transforma la corriente continua en corriente alterna, con la cual se alimentan los dispositivos conectados a la UPS.

2.2.11 Plan de contingencia

Es un plan que va enfocado en la parte de prevención, predicción y reacción, de situaciones de emergencia que se puedan llegar a presentar en una empresa o entidad. Presenta a su vez una estructura estratégica y operativa que ayudara a controlar este tipo de situaciones de emergencia y a su vez a ayudar a minimizar las consecuencias negativas que esta pueda llegar a presentar.

Un plan de contingencias contiene tres grandes parámetros o subplanes.

1. El plan de respaldo: Abarca las medidas preventivas antes de que se presente y ejecute una amenaza.

2. El plan de emergencia: Contempla las medidas necesarias tomadas durante la ejecución de una amenaza, o inmediatamente después de presentada.

3. El plan de recuperación: Hace referencia a las medidas necesarias tomadas después de ejecutada y controlada la amenaza.

2.2.12 Plan de diseño ITIL (Information Technology Infrastructure Library)

Es un plan con el que se busca poder ayudar a la gran variedad de organizaciones en el medio a lograr un alto nivel de calidad y eficiencia en cuanto a las operaciones IT. Algunas de las ventajas que se obtienen al implementar un plan de diseño ITIL son **[10]**:

1. Permite mejorar la comunicación con los clientes y usuarios finales a través de los diversos puntos de contacto establecidos.
2. Se le da un mejor manejo en cuanto a la calidad y los costos de los servicios.
3. Con respecto a la entrega de servicios, esta se enfoca más hacia el cliente, mejorando de esta forma la calidad de los mismos y la relación entre el cliente y el departamento de IT.
4. Permite una mayor flexibilidad y adaptabilidad de los servicios.

2.2.13 Estándar ISO 27001

La ISO 27001 es un estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información.

El objetivo fundamental es proteger la información de su organización para que no caiga en manos incorrectas o se pierda para siempre **[11]**.

2.2.14 Ciclo PHVA (Circulo de Deming o circulo de Gabo)

Ciclo PHVA (ver figura 3 y 4)

- **Planificar** (Plan): establecer el SGSI.
- **Hacer** (Do): implementar y utilizar el SGSI.
- **Verificar** (Check): monitorizar y revisar el SGSI.
- **Actuar** (Act): mantener y mejorar el SGSI.

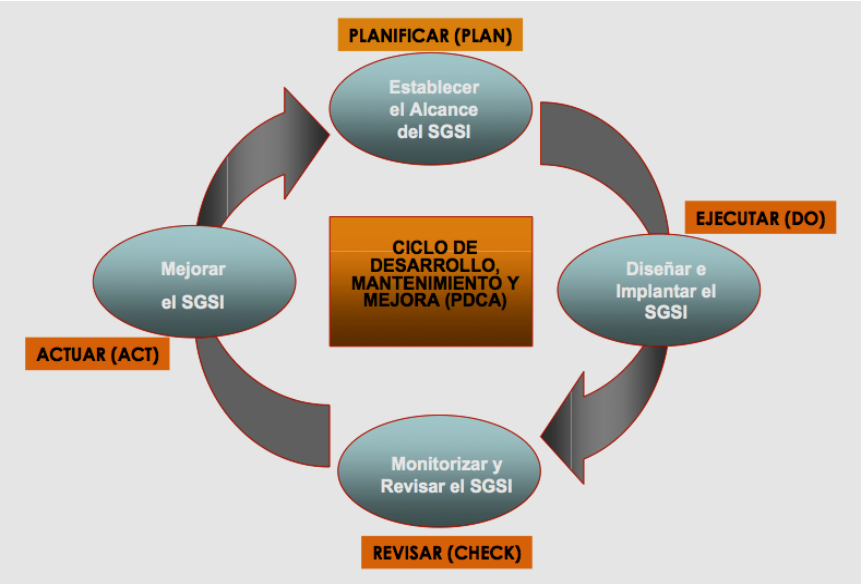


Figura 3. Esquema Ciclo PHVA[2]

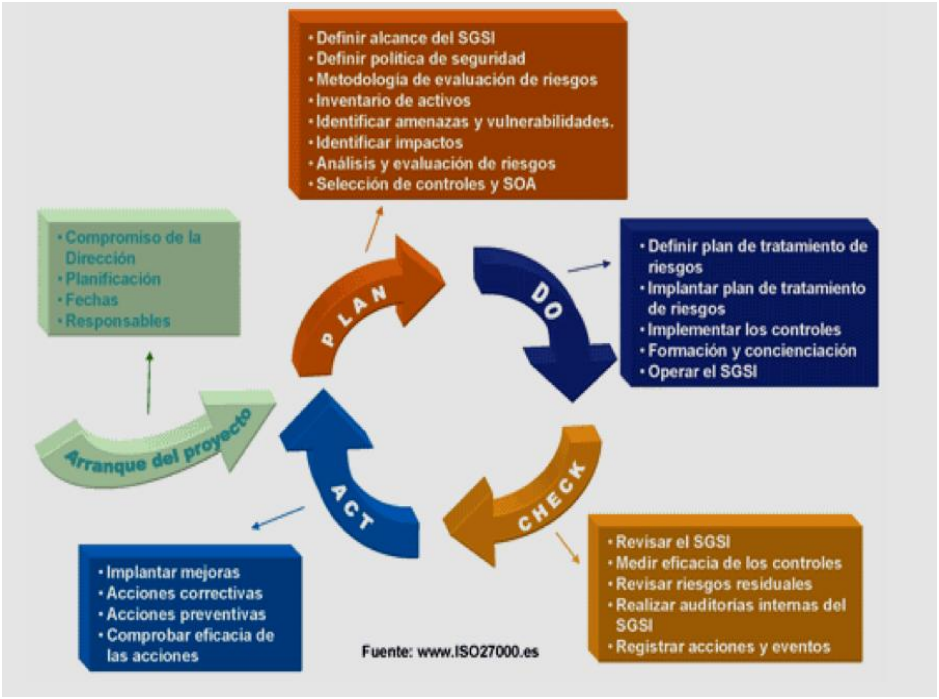


Figura 4. Definición Ciclo PHVA[3]

[2] *Tomado de http://www.iso27000.es/iso27000.html#section3e*

[3] *Tomado de http://www.iso27000.es/iso27000.html#section3e*

- **PLANIFICAR: Establecer el SGSI [11]**

  - Establecer el alcance del SGSI en términos de la organización, su ubicación, los activos y tecnologías.

  - Especificar una política de seguridad en donde:

    -Se incluyan los objetivos de seguridad de la información que se vayan a cumplir dentro de la organización;

    -Se alinee el contexto estratégico de gestión de riesgos de la organización en el cual va a mantener el SGSI

    -Sea aprobado por la dirección.

    -La característica principal de este tipo de metodología es que los resultados que se vayan obteniendo puedan ser comparables y repetibles.

  - Identificar los riesgos:

    -Identificar todos los activos que puedan ser cubiertos por el SGSI y a los responsables directos, es decir, a sus propietarios.

    -Identificar las posibles amenazas que se presenten en relación a los activos.

    -Identificar los impactos que se pueden presentar dentro de la confidencialidad, integridad y disponibilidad de los activos.

  - Analizar y evaluar los riesgos:

    -Evaluar el impacto que se produciría en la organización por causa de fallos de seguridad en donde se suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

    -Analizar la probabilidad de que ocurra un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.

-Determinar los niveles de riesgo.

-Según los criterios de aceptación de riesgo previamente establecidos, determinar si el riesgo es aceptable o necesita ser tratado.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

  -Implementar los controles adecuados.

  -Aceptar los riesgos, y seguir cumpliendo con las políticas y los criterios establecidos para la aceptación de los riesgos.

  -Evitar los riesgos, por ejemplo, terminando las actividades que lo originan;

  -Si no es posible evitarlo por completo, transferir el riesgo a terceros, como por ejemplo, a compañías aseguradoras o proveedores de outsourcing[4].

➢ **HACER: Implementar y utilizar el SGSI [11]**

- Crear un plan para el tratamiento de los riesgos el cual identifique las acciones, los recursos, las responsabilidades y las prioridades en la gestión de los riesgos de seguridad de la información.

- Implementar el plan de tratamiento de riesgos, el cual debe alcanzar los objetivos de control, donde se incluyan la asignación de recursos, responsabilidades y prioridades.

- Implantar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Establecer un sistema de métricas el cual permita la recolección de resultados que sean reproducibles y comparables con el objetivo de medir la eficiencia de los controles.

[4] La subcontratación es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

- Crear programas de capacitación relacionados con la seguridad de la información para todo el personal.

- Construir procedimientos y controles que lleven a cabo una rápida detección y respuesta a los incidentes de seguridad.

➢ **VERIFICAR: Monitorizar y revisar el SGSI [11]**

La empresa deberá llevar a cabo los procedimientos de monitorización y revisión para:

- Descubrir a tiempo los errores en los resultados generados por el procesamiento de la información.

- Determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se cumpliendo en relación a lo previsto.

- Mediante el uso de indicadores, detectar y prevenir eventos e incidentes de seguridad.

- Evaluar habitualmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI.

- Medir la efectividad de los controles para asegurar que se cumple con los requisitos de seguridad.

- Revisar regularmente las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que se hayan producido dentro de la organización.

- Ejecutar periódicamente auditorías internas del SGSI.

- Revisar que el alcance definido por el SGSI siga siendo el adecuado y que las mejoras en el proceso sean evidentes.

- Documentar las acciones y los eventos que puedan haber producido un impacto sobre la efectividad o el rendimiento del SGSI.

- **ACTUAR: Mantener y mejorar el SGSI [11]**

La organización deberá periódicamente:

- Actualizar el SGSI.
- Realizar las acciones adecuadas en relación a la clausula 8 de ISO 27001.[5]
- Difundir todas las acciones y mejoras al personal detalladamente y acordar, si es pertinente, la forma de proceder.
- Verificar que las mejoras introducidas alcanzan los objetivos previstos.

2.3 MARCO REFERENCIAL

En esta unidad se encuentran las teorías, referencias y especificaciones en las cuales se basa el presente proyecto con el fin de comprender de una manera más práctica el planteamiento del tema.

2.3.1 Políticas de Seguridad (PSI)

Las Políticas de Seguridad son un conjunto de exigencias definidas por las personas directamente responsables de un sistema, las cuales llegan a indicar en términos generales lo que está y no está permitido en el área de seguridad durante la marcha habitual del sistema **[12].**

Las políticas de seguridad se pueden ver reflejadas en una serie de protocolos, normas o reglamentos a seguir en la organización, en las cuales se pueden definir las medidas a adoptar para proteger la seguridad del sistema.

En términos generales cualquier política de seguridad debe comprender una serie de elementos claves de seguridad como lo son: Integridad, disponibilidad y privacidad.

[5] **8. Mejora del SGSI:** mejora continua, acciones correctivas y acciones preventivas.
8.1 Mejora continua
8.2 Acción correctiva
8.3 Acción preventiva

2.3.2 Vulnerabilidades del Sistema

Las vulnerabilidades del sistema hacen referencia a una serie de debilidades dentro de un sistema, permitiendo a un atacante vulnerar factores de alta importancia para una organización como lo son: la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones **[13].**

Las vulnerabilidades básicamente son el resultado de fallos que se pueden presentar en el diseño del sistema, sin dejar a un lado que también estas pueden ser generadas por las limitaciones tecnológicas, porque siendo consientes, no existe un sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales.

2.3.3 Gestión de la información

Se puede definir como un conjunto de procesos a través de los cuales se controla el ciclo de vida de la información, desde su obtención, hasta su disposición final. Incluye además una serie de operaciones tales como la extracción, manipulación, tratamiento, depuración, conservación y acceso de la información que es obtenida por una organización a través de diferentes fuentes, la cual gestiona el acceso y los derechos que tendrán los usuarios sobre dicha información **[14].**

La gestión de la información tiene como finalidad garantizar la integridad, disponibilidad y confidencialidad de la información.

3. INGENIERÍA DEL PROYECTO

El presente capítulo describe detalladamente los procedimientos y conceptos utilizados para dar solución a la necesidad presente en la organización, aplicando la solución ingenieril más adecuada de acuerdo a los estudios realizados al sistema, identificando sus fortalezas y debilidades, que contribuyen al desarrollo de un diseño que se acople fácilmente a los servicios y arquitectura existente. Para cumplir con los objetivos establecidos se definió una metodología determinada, así como las variables de ingeniería que contribuyen al desarrollo de la solución.

3.1 ESTUDIO DE LAS VARIABLES DE INGENIERÍA

Se identificaron las siguientes variables de ingeniería para la elaboración del presente proyecto teniendo en cuenta que este abarcará el análisis de la red.

3.1.1 Integridad

Hace referencia a la eficacia y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basado en lo anterior se puede decir que las herramientas de seguridad informática se deben encargar de que todos los procesos de actualización estén sincronizados para que de este modo se asegure de que todos los elementos del sistema puedan manipular los datos de una forma adecuada.

3.1.2 Disponibilidad

La disponibilidad se define como la continuidad que se le da al acceso con respecto a los elementos de información que se encuentren guardados y a su vez están siendo procesados dentro de un sistema informático.

Además se busca que se integre con toda la seguridad informática, fortaleciendo la permanencia del sistema informático, de tal manera que los usuarios podrán acceder a la información en cualquier momento, de acuerdo a los parámetros que sean establecidos por la organización.

3.1.3 Privacidad

Privacidad es el derecho de mantener de forma reservada o confidencial los datos almacenados en el ordenador y los que a su vez se intercambian por la red. En la actualidad, la privacidad se ve sistemáticamente violada por spywares, cookies, piratas informáticos y virus.

3.1.4 Confidencialidad

La confidencialidad es la privacidad de los elementos de información, almacenados y procesados en un sistema informático, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones, accesos, por parte de personas o programas no autorizados.

Esto es importante en la implementación de sistemas integrados de seguridad, en donde los ordenadores, datos y usuarios se encuentran en diferentes lugares, pero a su vez se encuentran interconectados tanto física como lógicamente.

3.1.5 Control

El control de la información, se enfoca en asegurar de manera puntual que solo las personas autorizadas podrán decidir cómo y cuándo los usuarios podrán tener acceso a dicha información. El control es una herramienta fundamental en una organización debido a que ayuda a los administradores de la información a tener una supervisión sobre los recursos, operaciones y procesos que se realizan internamente para de esta manera tener un control sobre los mismos.

3.2 SISTEMA ACTUAL

Las políticas de red que maneja la institución han venido decayendo debido al mal manejo e implementación de los equipos actuales (ver figura 5), esto se debe a la poca asistencia profesional que se da en estas ciudades. El sistema de seguridad y de red es manejado por un solo usuario, conectado únicamente a un Enrutador ADSL sin ninguna protección permitiendo así que el sistema sea fácilmente vulnerado.

El flujo permanente de tráfico de datos, de voz y video dentro de la red está saturando por completo el sistema, haciendo que este pierda la calidad del servicio ofrecido a los usuarios.

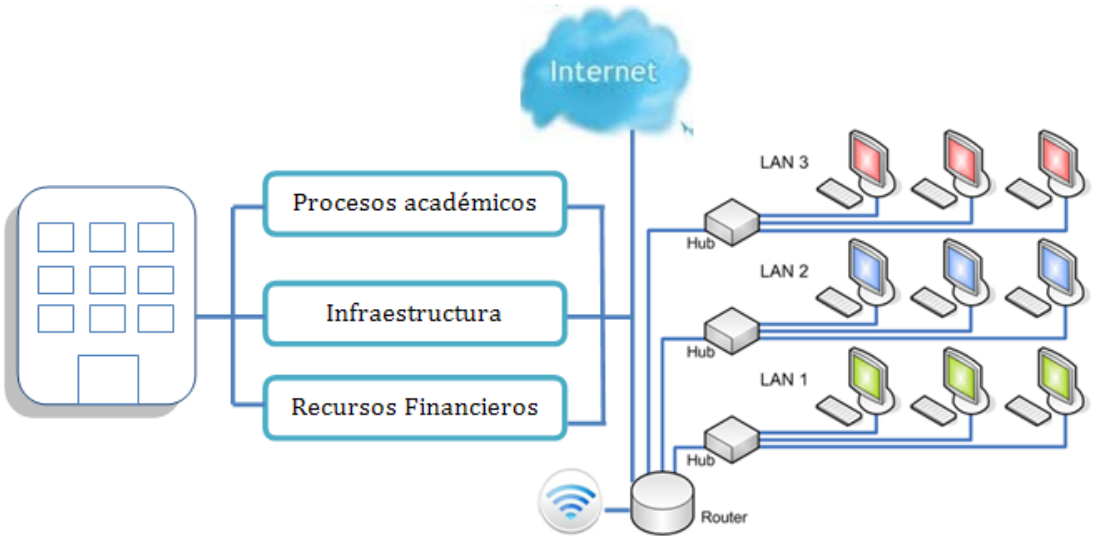


Figura 5. Estado Actual del sistema

Teniendo en cuenta los conceptos de seguridad lógica y física anteriormente mencionados, y basados en la implementación que se va a hacer en la institución, se realizó un análisis de acuerdo a las debilidades encontradas, las cuales son descritas a continuación:

- **Debilidad:** No se lleva ningún registro de revisión periódica ni control sobre el buen funcionamiento de los equipos (equipos de computo, de red y de vigilancia) y los permisos de acceso que tienen asignados los usuarios.

  Efectos: Es posible que, por error, negligencia, fraude o algún otro motivo, los equipos y las cuentas sean modificados, vulneradas y hasta dañadas permitiendo que usuarios no habilitados accedan a datos que no le están permitidos.

- **Debilidad:** No se tiene en cuenta ninguna restricción horaria en el momento de permitir acceso a un usuario a los equipos de la institución.

Efectos: Esto puede permitir que un usuario no autorizado intente ingresar al sistema en cualquier horario, condición que se ve agravada por el hecho que no todos los equipos tienen claves de acceso y pueden acceder a cualquier tipo de información de los usuarios.

- **Debilidad:** No se tiene en cuenta ninguna restricción con respecto al equipo desde donde se ubican los usuarios.

  Efectos: Al no controlar el dispositivo físico que usa cada usuario, puede ocurrir que alguna persona tenga acceso a un equipo que no le corresponde, permitiéndosele ver y modificar información para la que no tiene autorización.

- **Debilidad**: Las comunicaciones dentro de la institución se realizan utilizando ordenadores que no tienen ningún control especial con respecto a la conexión a Internet. Esta comunicación se realiza sin la supervisión del firewall.

  Efectos: una conexión a Internet sin resguardo es peligrosa, ya que aumenta los riesgos de intrusiones, virus, entre otros sucesos no deseables.

- **Debilidad:** Los equipos de la empresa disponen unidades lectoras de CD, aunque solo el 90% de los usuarios no las necesitan. Estos dispositivos están habilitados y no hay ningún control sobre ellos, permiten acceso automático de virus y tampoco se prohíbe el booteo desde estos dispositivos.

  Efectos: Debido a que cualquier usuario puede introducir un CD con virus o intentar bootear desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos.

- **Debilidad:** No hay inventarios de los equipos de hardware, ni documentación con respecto a los equipos de la red física.

  Efectos: Esta documentación facilita las actividades de los administradores del centro de cómputos, en el momento de realizar tareas de mantenimiento y para el desarrollo del plan de contingencias.

- **Debilidad:** No hay control de acceso físico a la institución, ya que ninguna de las cámaras del circuito cerrado de video lo apunta a su puerta de ingreso.

  Efectos: Al no haber un control de acceso especial a la institución, cualquier persona que tenga acceso al área y ante una distracción del personal, puede ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se encuentran.

3.3 SISTEMA PROPUESTO:

Para el sistema propuesto (ver figura 6) tendremos en cuenta diferentes aspectos básicos de diseño:

- Principio de la satisfacción y de la seguridad, lo que nos permite resaltar que la elección será la más efectiva haciendo el trabajo más satisfactorio y seguro para los usuarios del sistema (estudiantes, profesores, directivos, administrativos entre otros).
- Lograr la mejor utilización de los equipos disponibles.
- Adaptarse a gran variedad de servicios educativos (nuevos programas académicos).
- Adaptarse fácilmente a una demanda intermitente.
- Facilidad de control tanto del uso de las instalaciones, como de la realización de las diferentes actividades.
- Plantear un sistema flexible con el fin de permitir cambios a medida que se vayan requiriendo de acuerdo a la siguiente figura que esquematiza la mejora del sistema actual.

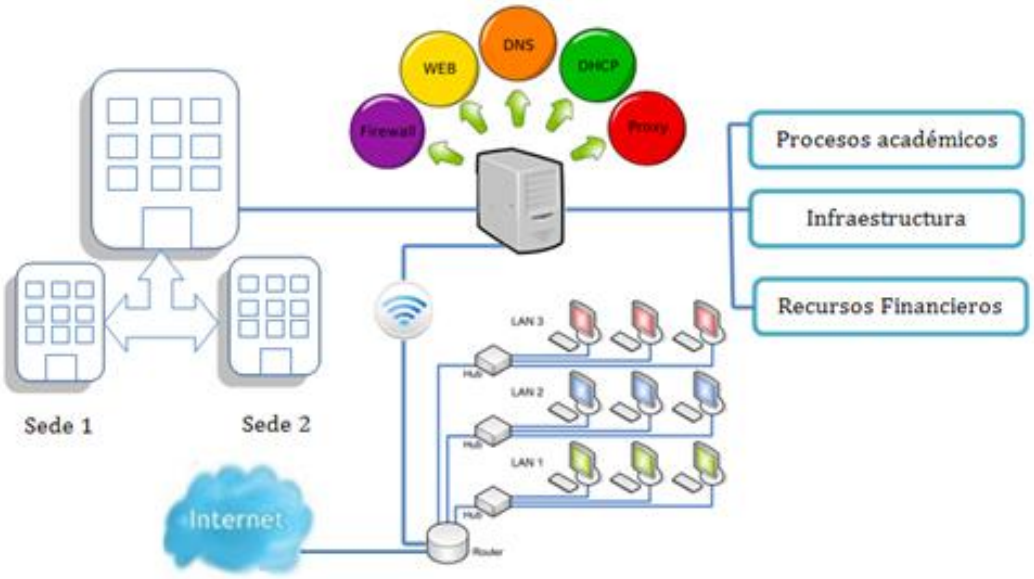


Figura 6. Sistema Propuesto

4. DESARROLLO DEL PROYECTO

El desarrollo del proyecto abarca una serie de fases definidas que comprenden actividades y procedimientos que aseguran el cumplimiento del objetivo final del proyecto (Ver Figura 7).

Algunas de las fases se hicieron simultáneamente, pues estaban interrelacionadas, mientras que las otras deben desarrollarse individualmente, todas las actividades se desarrollaron de acuerdo al cronograma actividades estipulado al inicio del proyecto.

Figura 7. Metodología del proyecto

Para el desarrollo del proyecto se ha tenido en cuenta el estándar para la seguridad de la información ISO/IEC 27001 **[15]** a fin de aplicarlas en todas las fases del trabajo. Este estándar define los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), para lo cual se ha tomado el ciclo de Deming[6] conocido como PHVA (Planificar, Hacer, Verificar, Actuar) el cual hace parte del estándar y que incluye los siguientes pasos:

1. Planificar (Plan)
2. Hacer (Do)

[6] El ciclo **PHVA**, también conocido como "Círculo de Deming o circulo de Gabo" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina *espiral de mejora continua*. Es muy utilizado por los SGC.

3. Verificar (Check)

4. Actuar (Act)

Otro aspecto importante a tener en cuenta dentro del estándar, es definir el cargo del responsable de la seguridad de la empresa que se ocupa de garantizar que dicha seguridad tenga el nivel adecuado de respaldo ejecutivo, que la directiva se comprende claramente en todos los niveles de la organización y que se articula a éstos. Hay que definir las necesidades de personal y asegurarse de que todos los miembros de la organización adquieran el compromiso y la capacitación necesarios para asumir la cultura de la seguridad. Muchas incursiones de seguridad se producen como consecuencia directa de una falta de formación o una deficiencia en el proceso de implantación.

4.1 PLANIFICAR (PLAN)

El desarrollo de la primera fase del proyecto se hará basado en el primer aspecto que del ciclo de Deming, teniendo en cuenta todas las recomendaciones descritas anteriormente.

4.1.1 FASE I. LEVANTAMIENTO DE INFORMACIÓN

Se debe hacer el levantamiento de información de 3 elementos principales dentro del escenario: Inventario de Hardware, Software y recursos Humanos.

Con el levantamiento de información de estos elementos se contabilizará el número de equipos con los que se cuenta, sus características principales (tipo de procesador, capacidad de discos de almacenamiento, memoria RAM) y el estado de los mismos con el fin de evaluar la actualización de las plataformas de software y el hardware.

Finalmente con la evaluación del personal, se recopilará información acerca de los conocimientos que poseen sobre sistemas de seguridad y de su utilización.

4.1.1.1 Recopilación de información y diagnóstico del estado actual del sistema

Actualmente la Academia Nacional de Sistemas no reconoce la importancia de la utilización de un estándar de seguridad de la información y seguridad física, es por esto que en la institución se instaló un circuito cerrado de televisión desprotegido, basados en

que la aplicación de este sistema prevendría cualquier tipo de anomalía física (pérdidas, robos) sin tener en cuenta que para la aplicación de este sistema se deben seguir unos pasos y establecer unos requerimientos antes de la implementación. Estudiando los criterios que tuvo el personal de administración de la empresa para la implementación del sistema de cámaras no se encontró ningún estudio de la planta física, de los puntos críticos donde se ubicarían las cámaras y mucho menos de cómo iba a ser manejado y administrado este sistema, por este motivo se determinó que el circuito cerrado de televisión es vulnerable y al alcance de cualquier administrativo de la institución, los cuales pueden tener acceso al servidor de cámaras, modificando y borrando lo que deseen.

Otro aspecto importante de la institución es la distribución de red. Esta presenta un bajo rendimiento y poca confiabilidad, lo cual fue determinado inicialmente por una serie de encuestas hechas a todo el personal académico e institucional de la empresa, en las cuales se indagó sobre aspectos generales pero a la vez muy importantes del funcionamiento y rendimiento de la red, tales como niveles de disponibilidad, tiempos de respuestas a las peticiones y desempeño de los equipos en cuanto a la navegación en internet (VER ANEXO 1).

A raíz de esto se logró determinar que en la academia nacional de sistemas no se tuvieron en cuenta detalles importantes al crear la distribución de red, todo esto se dio debido al crecimiento de la planta física y la rápida adquisición de nuevos equipos, para lo que no se tuvo en cuenta la implementación de servidores, sino la instalación de un SWITCH por aula conectado al mismo punto (ROUTER ADSL), lo que producirá fallas, bajo rendimiento y poca seguridad en la red de la institución, además de generar fácil acceso a cualquier punto de la empresa, ocasionando posibles modificaciones de la base de datos que se encuentra administrada por esta red.

Con base en estos detalles que no fueron tenidos en cuenta, se presenta la necesidad de hacer un rediseño ***(segundo paso del ciclo del Estándar ISO/IEC 27001)*** de la red y elaborar una propuesta basada en el presupuesto que maneja la institución para la compra y adquisición de nuevos equipos que serán de utilidad para brindar un mejor nivel de seguridad y un alto rendimiento de todos los equipos de la institución.

4.1.1.2 Inventario de hardware y software empleado en la actualidad

Con respecto al inventario de hardware, software y recursos humanos en las instalaciones de la Academia Nacional de Sistemas se encontró la siguiente información:

INVENTARIO ACADEMIA NACIONAL DE SISTEMAS				
EQUIPOS				
AULA 201				
Equipos	**Cantidad**	**Sistema operativo**	**Software**	**Hardware**
Equipo portátil Acer Aspire	8	Windows 7 Home Premiun	Microsoft Office 2007, Corel Draw x5, Netbeans, Adobe CS4	Memoria Ram 4 Gb, D.D 320 Gb, Procesador AMD Turion x2
Equipo portátil Toshiba LA	2	Windows 7 Home Premiun	Microsoft Office 2007, Corel Draw x5, Netbeans, Adobe CS4	Memoria Ram 4 Gb, D.D 500 Gb, Procesador intel Core i3

Tabla 1. Inventario de computadores Aula 201

AULA 204				
PC Escritorio Clon	8	Windows 7 Home Premiun	Microsoft Office 2007, Corel Draw x5, Netbeans, Eclipse, Java, MySQL	Memoria Ram 2 Gb, D.D 320 Gb, Procesador Intel Dual Core.
PC Escritorio Compaq	6	Windows XP SP 3	Microsoft Office 2007, Corel Draw x5, Netbeans, Eclipse, Java, MySQL	Memoria Ram 2 Gb, D.D 250 Gb, Procesador Intel Core 2 Duo.

Tabla 2. Inventario de computadores Aula 204

AULA 203				
PC Escritorio Janus	8	Windows 7 Home Premiun	Microsoft Office 2007, Corel Draw x5, Dreamweaver, Helisa, SIIGO.	Memoria Ram 3 Gb, D.D 320 Gb, Procesador Intel Dual Core.
PC Escritorio Clon	6	Windows XP SP 3	Microsoft Office 2007, Corel Draw x5, Dreamweaver, Helisa, SIIGO.	Memoria Ram 2 Gb, D.D 320 Gb, Procesador AMD Athlon X2.
PC Escritorio Compaq	2	Windows XP SP 3	Microsoft Office 2007, Corel Draw x5, Dreamweaver.	Memoria Ram 2 Gb, D.D 250 Gb, Procesador Intel Core 2 Duo.

Tabla 3. Inventario de computadores Aula 203

AULA 301				
PC Escritorio Janus	8	Windows 7 Home Premiun	Microsoft Office 2007, Corel Draw x5, Dreamweaver, Helisa, SIIGO.	Memoria Ram 3 Gb, D.D 320 Gb, Procesador Intel Dual Core.
PC Escritorio Clon	6	Windows XP SP 3	Microsoft Office 2007, Corel Draw x5, Dreamweaver, Helisa, SIIGO.	Memoria Ram 2 Gb, D.D 320 Gb, Procesador AMD Athlon X2.
PC Escritorio Compaq	1	Windows XP SP 3	Microsoft Office 2007, Corel Draw x5, Dreamweaver.	Memoria Ram 2 Gb, D.D 250 Gb, Procesador Intel Core 2 Duo.

Tabla 4. Inventario de computadores Aula 301

OFICINA				
PC Escritorio Clon	3	Windows 7 Home Premiun	Microsoft Office 2007, MySql, Dreamweaver, Flash.	Memoria Ram 4 Gb, D.D 500 Gb, Procesador Intel Core 2 Duo
Equipo portatil Toshiba	1	Windows 7 Home Premiun	Microsoft Office 2007.	Memoria Ram 4 Gb, D.D 500 Gb, Procesador intel Core i3

Tabla 5. Inventario de computadores Oficina Administración

EQUIPOS ADICIONALES	
Equipos	**Cantidad**
Router ADSL + wifi Hawei	1
Acces Point Dlink	1
Switch 18 Puertos 3com	2
Switch 18 Puertos Dlink	1
Camaras Vigilancia CCTV	6
Video Beam Epson	4

Tabla 6. Equipos adicionales Academia

PERSONAL	
Cargo	**Asignatura**
Rector	No Aplica
Administradora	No Aplica
Secretarias (2)	No Aplica
Docentes (6)	Sistemas
Docentes (4)	Ingles
Docentes (3)	Contabilidad

Tabla 7. Personal Docente y Administrativo

4.1.1.3 Estudio financiero del plan

La institución cuenta con una infraestructura física que comprende dos bloques (BLOQUE A, BLOQUE B) y cada uno tiene 3 plantas, es por esto que al realizar el inventario y de acuerdo a las necesidades de la empresa se determinó que la cantidad y calidad de los equipos no abarcaban la totalidad de la instalación, comprometiendo así la seguridad física y lógica de la empresa, la poca cantidad de equipos y el crecimiento de la institución están presentando grandes problemas para la seguridad de esta.

Para realizar la propuesta de la compra de nuevos equipos, en busca del beneficio para la Academia Nacional de Sistemas, se realizó una comparación de costos de los equipos entre las ciudades de Florencia y Bogotá; para la realización de este estudio se tuvieron en cuenta 4 aspectos básicos que fueron:

- Costo
- Calidad
- Garantía
- Transporte

De acuerdo a los datos obtenidos en el estudio se obtuvo que en la ciudad de Bogotá la compra y gestión de los equipos es más favorable que en la ciudad de Florencia, teniendo en cuenta los costos por envío de Bogotá hacia Florencia y la garantía de estos mismos.

A continuación se presenta la comparación de costos entre las dos ciudades:

EQUIPO	DESCRIPCION	VALOR BOGOTA	VALOR FLORENCIA	TOTAL (BOGOTA)
CAMARA IP D-LINK (x6) 	• Cámara IP marca D-Link 930L • Tecnología Wireless N para una conexión perfecta desde cualquier punto. • Sensor de 1,0 Lux para condiciones de poca luz. • Envío de alertas por correo electrónico por detección de movimiento • Micrófono integrado • Soporte de DNS dinámico para acceder fácilmente a la cámara desde cualquier punto de internet	$220.000	$250.000	$ 1.320.000
ACCESS POINT D-LINK (x2)	•Access Point inalámbrico potenciado de alto rendimiento • Soporta control de acceso 802.1x •Antena desmontable, conector RSMA •Cinco diferentes modos	$150.000	$180.000	$300.000

	de operación. • DHCP Server • Administración Web y Windows			
UPS (x3) 	Tiene un alcance para 3 ordenadores, con duración de 1 hora para cada uno	$950.000	$1.120.000	$1.900.000
SERVIDOR SAMSUNG	Procesador Intel Core i5, 4 Gb Memoria Ram DDR3, 2 Discos duros 1TB cada uno, Tarjeta de Red, Tarjeta gráfica NVIDIA 1 Gb dedicada, SO Ubuntu.	$1.500.000	$1.735.000	$1.500.000

MONITOR 22” (X2)	Monitor LCD 22” Samsung	$280.000	$330.000	$280.000

Tabla 8. Comparación de precios de los equipos sugeridos

NOTA: Los precios anteriormente descritos incluyen IVA, pero no incluyen los gastos de transporte desde la ciudad de Bogotá hacia Florencia, debido a que el precio por transporte no influye mucho ya que la Academia Nacional De Sistemas tiene convenio con la empresa transportadora Taxis Verdes.

De acuerdo con el inventario realizado de los equipos con los que cuenta actualmente la Academia Nacional de Sistemas y al estudio de costos, se propone la adquisición de diferentes y nuevos equipos que ayudaran al mejoramiento y confiabilidad de los procesos realizados dentro de la institución, estos equipos son:

EQUIPO	CANTIDAD	VALOR
Cámara IP	6	$220.000 c/u
UPS	3	$950.000 c/u
SERVIDOR	2	$1.500.000 c/u
Monitor LCD 22”	2	$280.000 c/u
Access Point	2	$150.000 c/u

Tabla 9. Equipos propuestos para el montaje del diseño

4.1.2 FASE II. DIAGNÓSTICO DE ESTÁNDARES Y NORMAS

Se evaluarán los estándares y normas utilizados en la actualidad para el servicio de seguridad dentro de la Academia Nacional de Sistemas.

Al realizar esta evaluación se determinarán cuales de estos son necesarios para la ejecución del proyecto y qué normas nuevas se deberán utilizar dentro de los parámetros del sistema.

4.1.2.1 Desarrollo

Para verificar y evaluar los estándares y normas implementados en la Academia Nacional de Sistemas se entrevistó al actual rector con el fin de verificar que tipo de estudios se habían realizado dentro de la institución para implementar el sistema de seguridad que actualmente posee y se obtuvo que:

- La Academia Nacional de Sistemas nunca realizó un estudio para implementar el circuito cerrado de televisión.
- La institución conoce acerca de los servicios que pueden prestar los servidores para la seguridad lógica pero no han adaptado ninguno de estos servicios debido a falta de información.
- Con el rápido crecimiento de la institución, la distribución de la red nunca fue diseñada antes de ser implementada, solo se utilizaron conocimientos empíricos de los administrativos sin tener en cuenta alguna norma o estándar que ayudará a la distribución de la red.

Palabras del rector Carlos Julio Beltrán:

“La Academia Nacional de Sistemas nunca realizó un estudio de estándares y normas apropiados para el desarrollo de los sistemas de seguridad físicos y lógicos que actualmente se manejan, solo confiamos en el conocimiento del personal administrativo.”

Con base en lo anterior se plantea que el estándar adecuado para la institución es el ISO/IEC 27001.

- **Comparación estándares de seguridad**

En la actualidad las empresas han presentado muchas necesidades por las cuales se hace necesaria la implementación de estándares de seguridad, algunas de ellas son:

- Establecer una serie de normas para prácticas favorables para la gestión de la seguridad.
- Establecer las especificaciones para la adopción de un Sistema de Gestión de la Seguridad de la Información.
- Establecer un estándar de facto a nivel global, que se implemente en las entidades que administran la seguridad de la información.
- Establecer un conjunto de normas que se apliquen en cualquier entorno y sector, y que utilicen tecnologías de la información para lograr los objetivos propuestos.
- Mejorar los niveles de competitividad, optimizando la seguridad y el funcionamiento de la empresa.
- Promover servicios para que la empresa se incorpore más fácil y eficientemente a la sociedad de la información.

En la siguiente tabla se realizó la comparación de los estándares actuales que hacen referencia a la parte de gestión y seguridad (Tabla 10):

ESTANDAR	¿QUE ES?	ALCANCE	CERTIFICACION
ISO/IEC 17799	Es un estándar orientado a la Seguridad de la Información, y está reconocido internacionalmente. Define la información como un activo que posee valor para la organización.	Este estándar aporta una serie de recomendaciones para realizar la gestión de la seguridad de la información. Está dirigida a todos los responsables de iniciar, instaurar o velar por la seguridad de una organización.	La norma es una guía de buenas prácticas, pero a su vez no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado para este documento

ISO/IEC 27001	Es una norma internacional que sirve para Implantar controles y procedimientos para asegurar la gestión de la seguridad de la información (SGSI).	Esta norma se enfocada en los aspectos técnicos, organizacionales y legales. Se hace referencia a los activos de la organización que son susceptibles de implementar gestión, medidas y procedimientos, con el fin de minimizar el riesgo derivado de su falta de integridad, confidencialidad y disponibilidad.	Es un proceso en el cual una entidad de certificación externa, independiente y acreditada, audita el sistema determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia emite el correspondiente certificado.
SAS 70 (Statement on Auditing Standards No. 70)	Es un estándar de auditoría, el cual es reconocido a nivel internacional y además desarrollado por el AICPA (American Institute of Certified Public Accountants).	Está orientada en el control interno de la organización, que incluye procesos internos referentes a clientes, operaciones, recursos humanos, operaciones, entre otras. La SAS70 está diseñada con el fin de proveer información a las organizaciones beneficiarias y a sus auditores, acerca del control interno de la de los servicios de la organización.	No se certifica el sistema de Gestión. El auditor lo que hace es dar una nota sobre el alcance de la norma en un informe que se entrega a terceros, lo que se conoce como el "stakeholder", pero no existe certificado reconocido al exterior, no hay esquema de certificación español.

Tabla 10. Equipos propuestos para el montaje del diseño

- **¿POR QUÉ ISO/IEC 27001?**

ISO/IEC 27000 son una serie de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), los cuales proporcionan un enfoque de gestión de riesgos y promueve la mejora continua de los procesos para cualquier tipo de organización, ya sea pública o privada, grande o pequeña. **[16]**

El estándar ISO/IEC 27001 dice: "la información es el activo más importante y es vital para el éxito y la permanencia en el mercado de cualquier organización. La seguridad de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización". **[16]**

La norma ISO/IEC 27001 es la única norma internacional que es auditable y además define los requisitos necesarios para un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma fue creada para garantizar la adecuada selección de controles de seguridad, esto ayuda a prevenir riesgos en los activos de información y genera confianza a en cualquiera de los sectores interesados ya sean clientes o administrativos de las organizaciones. La norma se enfoca en diferentes procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

A continuación se presentan las clausulas de funcionamiento de la norma ISO/IEC 27001

- Introducción: generalidades e introducción al método PHVA.
- Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- Normas para consulta: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.

- Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- Auditorías internas del SGSI: cómo realizar las auditorías internas de control y cumplimiento.
- Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.

➢ **¿QUÉ BENEFICIOS PRESENTA ISO/IEC 27001?**

- Presenta una metodología de gestión de la seguridad clara y estructurada.
- Reduce el riesgo de pérdidas, robos o corrupción de la información.
- Servicio de acceso a la información a través medidas de seguridad para los clientes.
- Revisión y control de los riesgos permanentemente.
- Confidencialidad comercial entre clientes y socios estratégicos para la garantía de calidad.
- Presta servicio de auditorías externas que ayudan a detectar las falencias del sistema y las áreas a mejorar.
- Capacidad de integración con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Posicionamiento de la organización a nivel internacional.
- Generación de confianza y creación de reglas claras para las personas de la organización.
- Reducción de costos y mejoramiento de los procesos y servicios de la organización.

- Ampliación de la seguridad en base a la gestión de procesos economizando la compra sistemática de productos y tecnologías.

4.1.2.2 SGSI (Sistema de Gestión de la Seguridad de la Información)

El SGSI (Sistema de Gestión de la Seguridad de la Información) realiza la gestión por medio de un proceso sistemático, documentado y conocido por toda la organización. Se puede considerar por su similitud con la norma ISO 9000, como el sistema de calidad para la seguridad de la información.

El Objetivo de SGSI (Sistema de Gestión de la Seguridad de la Información) no se trata de garantizar la seguridad, por el contrario es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de tal forma que estén documentados, sistematizados, estructurados de manera continua, repetible, eficiente y que sean adaptables a cualquier tipo de cambios que se presenten en la organización.

El tipo de información que protege un SGSI (Sistema de Gestión de la Seguridad de la Información) independientemente del soporte en donde se encuentren, son los e-mail, informes, páginas web, imágenes, documentos, hojas de cálculo, presentaciones, contratos, registros de clientes, información confidencial y cualquier otro tipo de activo lógico que posea la organización.**[17]**

Para la implementación y gestión de un Sistema de Gestión de la Seguridad de la Información (SGSI) con base en ISO/IEC 27001, se maneja el ciclo continuo conocido como PHVA, que generalmente es empleado en los sistemas de gestión de la calidad.

4.1.2.3 Gestión del Riesgo y ciclo de vida PHVA

Por medio de la gestión del riesgo se reconocen, evalúan y corrigen a niveles razonables y considerables en el costo de todos los riesgos en seguridad que podrían afectar a la información.

PDCA son las siglas en inglés del conocido como: Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

En la primera sección PLANIFICAR se hace la evaluación de todos los tipos de amenazas, riesgos e impactos. En la sección HACER, se escogen e implementan los controles que van a reducir el riesgo a niveles aceptables, en VERIFICAR y ACTUAR se cierra y se reinicia el ciclo de vida con la recolección de evidencias y readaptación de los controles según los nuevos niveles obtenidos y requeridos.

Es un proceso cíclico sin fin que permite la mejor adaptación de la seguridad al cambio continuo que se produce en la empresa y su entorno.

4.2 HACER (DO)

Después de haber escogido los elementos necesarios para el mejoramiento de los sistemas de seguridad físicos y lógicos de la Academia Nacional de Sistemas, se procede a realizar el diseño y la implementación de los nuevos sistemas de seguridad.

4.2.1 FASE III. REALIZACIÓN DEL DISEÑO

Basados en la arquitectura de red actual de la Academia Nacional de sistemas, en la problemática presentada por el desempeño de esta y aplicando el análisis del proyecto, se presentó el diseñó de los nuevos servicios a implementar para la óptima solución a los inconvenientes presentados dentro de la institución.

En esta fase de diseño se presentan los beneficios y la manera en cómo se van a implementar los servicios red, dado que, con la implantación de estos, dará una mejora significativa a la problemática actual generando un beneficio tanto para a los administrativos como para los estudiantes, quienes se están viendo afectados por estos problemas.

La finalidad de la implementación de estos servicios de red es permitir que los usuarios de la institución puedan hacer un mejor uso de los equipos y efectuar controles de accesos a la red, mejorando de este modo el rendimiento global de la institución.

Existen un sinnúmero de ventajas y beneficios para las redes cuando se hace la aplicación de estos servicios, tales como:

- Facilidad de comunicación.

- Mejora de la competitividad.
- Reducción del presupuesto para proceso de datos.
- Mejoras en la administración de los programas.
- Mejoras en la integridad de los datos.
- Mejores tiempos de respuesta.
- Flexibilidad en el proceso de datos.
- Mejor seguridad.
- Mejorar el estado de configuración del software de los equipos de la Institución.

➢ **REQUERIMIENTOS**

La Academia Nacional de Sistemas requiere la mejora inmediata del circuito cerrado de televisión, el cual, actualmente se encuentra desprotegido, para la realización de esta mejora se van a tener en cuenta los puntos estratégicos de la institución para su implementación, otro aspecto importante a mejorar es la distribución de red, esta, será redistribuida basados en la aplicación de niveles de disponibilidad, tiempos de respuestas a peticiones dentro de la red, lo cual mejoraría de manera notoria el desempeño de los procesos realizados dentro de la institución.

Basados en estos requerimientos se realizará la adecuada implementación de servicios de red, estos mejorarán la seguridad física y lógica de la institución, dando así, solución a muchos de los problemas actuales de la Academia Nacional de Sistemas.

Como primer paso para la implementación se hace necesario la adquisición de dos (2) equipos para desempeñar el papel de servidores, con base en esto, se indagó acerca del tipo de Sistema Operativo (SO) que debería instalarse en cada uno de estos, teniendo en cuenta las variables de ingeniería y así, escoger el sistema que ayude al mejor desempeño de las funciones.

A continuación se muestra el diseño de red con los servicios que se piensas implementar (ver figura 8):

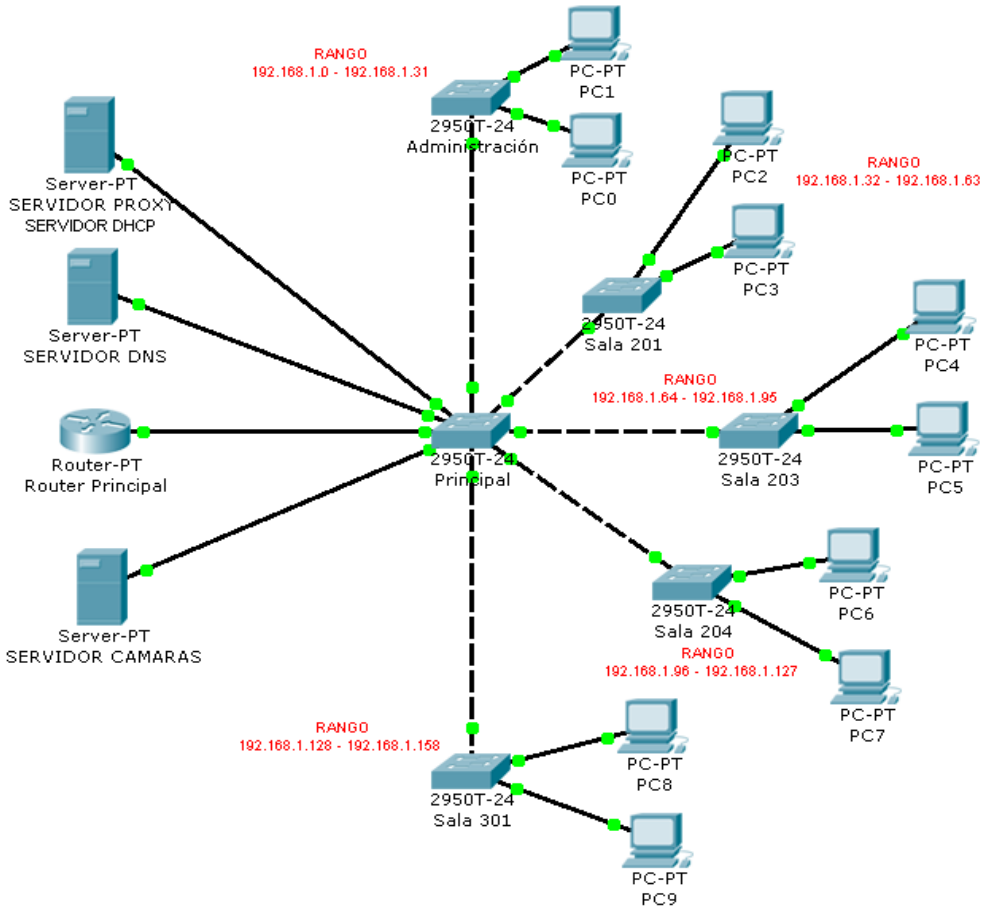


Figura 8. Simulación del Diseño Propuesto

4.2.1.1 Servicios

En la actualidad se han creado un gran variedad de servicios que presentan mejoras al ser implementados dentro de la red, para el caso concreto y en vista de los problemas descritos anteriormente que presenta la red de la Academia Nacional de Sistemas los servidores escogidos fueron:

- SERVIDOR DHCP
- SERVIDOR PROXY
- SERVIDOR DNS

- SERVIDOR DE CAMARAS

- **Servidor DHCP (Dynamic Host Configuration Protocol) [18]**

El servicio DHCP usa el concepto de "alquiler" o "préstamo" de dirección IP, cuyo significado es que una dirección IP determinada será válida para un ordenador durante un cierto período de tiempo. La duración del préstamo puede variar dependiendo de cuánto tiempo suele conectarse a Internet el usuario de una ubicación determinada. Es especialmente útil en educación y en otros entornos en los que los usuarios cambian con frecuencia.

Sin el servicio DHCP, la dirección IP de cada ordenador debe ser ingresada manualmente, y si los ordenadores cambian de sitio, hay que introducir nuevamente una dirección IP. El servidor DHCP permite al administrador de la red supervisar y distribuir las direcciones IP de forma automática cada vez que un ordenador se conecta en un lugar diferente de la red.

- **Servidor PROXY [19]**

Un servidor proxy es un servicio que hace de intermediario entre el sistema del usuario e Internet. Puede utilizarse para el registro del uso de Internet y también para restringir el acceso a páginas Web. El servidor de seguridad del servidor proxy bloquea algunas páginas Web por diversas razones.

Funcionan como firewall y como filtro de contenidos.

Un servidor proxy, sirve como mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet para crear un filtro en el acceso a ciertas páginas web consideradas ofensivas o dañinas para la red y los usuarios.

Mejoran el rendimiento.

Los servicios Proxy almacenan en la caché las páginas web a las que acceden los sistemas de la red durante un lapso tiempo. Cuando otro equipo solicita la misma página web, el servidor proxy utiliza la información guardada en la caché en lugar de recuperarla

del proveedor de contenidos. De esta manera, se hace más eficaz el acceso a las páginas Web.

Los servidores proxy son utilizados dentro de organizaciones en sus redes. Normalmente, las personas que se conectan a Internet desde casa no usan un servidor proxy.

- **Servidor DNS (Domain Name System) [20]**

Este servicio se utiliza para proveer a las computadoras un nombre de domino equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando éste está bien configurado.

Para un administrador o un usuario de la red, es más fácil recordar un nombre de dominio fijo que una dirección IP cambiante, y para el caso en común cuando una entidad tiene el servicio DNS, es decir, su propio nombre de dominio, se puede localizar más fácil dentro de la red.

La función del servidor DNS es permitir acceder a un dominio en internet entre los millones existentes. Básicamente su función es atender a las peticiones hechas por los distintos programas que acceden a internet y resolver la dirección IP asociada al dominio consultado.

4.2.1.2 Diseño de servidores

Ante la necesidad de mejorar el rendimiento, la seguridad y desempeño de la red y en busca de una solución veraz y de fácil uso, se hace un comparativo entre los dos sistemas operativos a escoger para la implementación de los servidores por medio de una encuesta (Ver Anexo B) hecha a los administrativos y docentes de la institución.

Así que se decidió, con base en los resultados de las encuestas y teniendo en cuenta que se van a adquirir dos (2) equipos, que los servicios se implementarán de la siguiente manera:

SERVICIO	LINUX	WINDOWS
DHCP	X	
PROXY	X	
DNS		X
CAMARAS		X

Tabla 11. Selección de Sistema Operativo

Los servicios se distribuirán en los equipos como se ve en la tabla anterior (ver tabla 11) dependiendo de las características de hardware de estos.

SERVICIOS EN LINUX

Para la instalación de los servicios en el Sistema Operativo Linux, se utilizará una herramienta ampliamente conocida y de fácil manejo llamada WEBMIN.

- **WEBMIN [21]**

Esta aplicación es una interfaz web creada en Perl [7] para administrar uno o más servidores, es una herramienta que permite configurar los permisos para usuarios y grupos mediante una estructura por módulos que facilita la administración de las herramientas como Apache, DNS, SAMBA, DHCP, PROXY, además de tener una interfaz gráfica de fácil manejo.

Webmin está disponible para las distribuciones GNU/Linux más comunes y Unix, con diversos paquetes para su instalación, una vez instalado su uso es tan sencillo como introducir la dirección web por el puerto asignado a la aplicación, el usuario y contraseña.

[7] Perl: Es un lenguaje de programación multipropósito y multiplataforma, diseñado por Larry Wall en 1987. Está basado en un estilo de bloques como los del lenguaje C o AWK

4.2.1.3 Servidor DHCP

La Academia Nacional de Sistemas cuenta con cinco salas informáticas equipadas cada una entre 10 y 22 computadores, además cuenta con una sección de administración donde se incluyen los equipos de administrativos y docentes, es por esto, que se hace necesario evaluar y realizar una nueva distribución del direccionamiento IP para cada una de las salas, estas direcciones van a ser repartidas por medio del servidor DHCP.

A continuación se muestra la distribución de direcciones IP para cada una de las salas (Tabla 7):

Subred	Dirección de Red	Inicio de Host	Fin de Host	Broadcast
Administración	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
Aula 201	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
Aula 203	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
Aula 204	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
Aula 301	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
Aula 301B	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
6	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
7	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

Tabla 12. Distribución de Direcciones IP por salas

Esta distribución (ver tabla 12), se hace con el fin de evitar que las direcciones IP aparezcan duplicadas y así mismo verificar en qué lugar se encuentran las fallas de manera más fácil, ya que cada sala tiene asignada una subred.

Como sistema de seguridad para el direccionamiento, se piensa en una alternativa que puede mejorar la distribución de las direcciones que consiste en tomar cada una de la direcciones MAC[8] de los equipos y así mismo definir una dirección por medio del servidor DHCP para cada MAC, esta medida evitaría que dos o más equipos tuvieran la misma dirección IP y permitiría saber el lugar donde se presentan fallas de una manera más eficaz, ya que cada aula contará con una subred específica.

[8] MAC (Media Access Control) se conoce como un identificador de 48 bits que consta de 6 bloques hexadecimales, que corresponde de forma única a una tarjeta de red.

En ese orden de ideas, se obtuvieron las direcciones MAC de cada uno de los equipos de las salas informáticas y la sala de administración, mediante el comando por consola IPCONFIG[9] y se organizaron de la siguiente manera:

ADMINISTRACION	
REFERENCIA	**MAC**
PC1 - Servidor Linux	00:30:67:D0:CE:EE
PC2 - Servidor Windows	00:30:67:D0:C4:7D
PC3 - Servidor Cámaras	00:25:22:75:51:5B
PC4 - Secretaria1	00:26:18:B2:44:2B
PC5 - Secretaria2	00:1C:C0:6F:0E:A7
PC6 - Oficina	00:1D:92:01:25:8ª
PC7 - Dirección	00:08:54:9D:B0:E9

Tabla 13. Direcciones MAC equipos de administración

En la tabla 13 se muestran las direcciones MAC de los equipos de la administración de la Academia Nacional de Sistemas.

La sala de informática 201 cuenta con catorce (14) equipos portátiles, estos poseen una configuración de hardware diferente, para este caso, estos equipos tienen dos tarjetas de red, una alámbrica y otra inalámbrica, es decir, cada equipo cuenta con dos direcciones MAC, las cuales fueron obtenidas y se muestran a continuación (Ver Tabla 14).

Se utilizó la letra W (wireless) para definir las tarjetas inalámbricas y la letra C (cableada) para las tarjetas alámbricas.

[9] IPCONFIG: por medio de este comando se puede ver la información relativa a los parámetros de la configuración IP actual

SALA 201		
REFERENCIA	**CABLEADA**	**INALAMBRICA**
PC1	60:EB:69:0D:38:FA	68:A3:C4:31:6D:32
PC2	00:26:22:6B:F6:09	00:17:C4:B5:E8:D9
PC3	00:26:22:64:05:BF	00:17:C4:B5:56:7E
PC4	00:26:22:65:32:FA	00:17:C4:B5:55:1F
PC5	00:26:22:69:42:57	00:17:C4:B5:3D:F2
PC6	00:26:22:64:05:C9	00:17:C4:B5:3D:D2
PC7	00:26:22:64:04:55	00:17:C4:B5:54:8A
PC8	00:26:22:89:40:8B	00:17:C4:B5:56:77
PC9	00:26:22:63:FF:43	00:17:C4:B5:40:3F
PC10	00:26:22:6B:F5:F8	00:17:C4:B5:E7:FB
PC11	00:26:6C:D0:D9:B9	E0:CA:94:32:06:C3
PC12	00:26:6C:D0:CB:1C	E0:CA:94:31:D4:74
PC13	00:26:6C:E3:80:87	E0:CA:94:7E:4E:9D
PC14	00:26:6C:E3:65:03	E0:C4:94:83:81:97

Tabla 14. Direcciones MAC equipos Sala 201

El aula 203 es la más grande de la institución, cuenta con veintidós (22) computadores de escritorio, con solo una tarjeta de red cada uno, en la tabla 15 se muestra la referencia y la dirección MAC de cada equipo.

SALA 203			
REFERENCIA	**MAC**	**REFERENCIA**	**MAC**
PC1	00:21:85:35:95:2A	PC12	00:E0:4C:69:13:43
PC2	00:19:66:D7:49:82	PC13	00:25:22:54:68:35
PC3	00:25:22:73:E7:C7	PC14	00:19:66:DF:10:1F
PC4	00:25:22:73:C5:A7	PC15	00:19:66:11:79:FE
PC5	00:1D:92:E1:0F:D7	PC16	00:1C:C0:6F:0E:6C
PC6	00:19:66:88:39:98	PC17	00:1C:C0:6F:OE:80
PC7	40:61:86:7A:39:D0	PC18	00:13:8F:1B:5E:1A
PC8	00:21:85:1E:40:AC	PC19	6C:62:6D:F5:3F:50
PC9	8C:89:A5:35:44:B2	PC20	00:19:21:13:0F:F5
PC10	00:19.66:F0:62:9B	PC21	20:6A:8A:3B:B0:CA
PC11	00:19:21:6F:CF:29	PC22	00:26:22:64:06:FA

Tabla 15. Direcciones MAC equipos Sala 203

La sala de informática 204 está equipada con trece (13) equipos, en la siguiente tabla (Tabla 16) se puede observar cada una de las direcciones MAC de las tarjetas de red de los equipos:

SALA 204	
REFERENCIA	**CABLEADA**
PC1	00:24:8C:AA:E3:84
PC2	00:0B:6A:42:FD:FD
PC3	D0:27:88:9D:7C:90
PC4	00:1C:C0:6F:0E:48
PC5	00:25:22:B8:09:49
PC6	00:1C:C0:6F:0E:22
PC7	6C:62:6D:F5:3F:44
PC8	00:13:8F:BE:07:2C
PC9	00:19:21:13:11:B6
PC10	00:19:D1:3F:F8:38
PC11	00:13:8F:85:A7:37
PC12	00:19:D1:43:5E:E1
PC13	00:13:8F:63:66:7C

Tabla 16. Direcciones MAC equipos Sala 204

Para culminar el levantamiento de todas las direcciones MAC, se obtienen las direcciones de la sala de informática 301, ubicada en el tercer piso y cuenta con quince (15) computadores, en la siguiente tabla (Tabla 17) se publican las direcciones MAC de esta sala.

SALA 301	
REFERENCIA	**CABLEADA**
PC1	00:19:D1:3B:1A:76
PC2	00:25:22:94:73:20
PC3	00:24:8C:AA:1C:F3
PC4	00:1D:92:94:02:4B
PC5	00:24:8C:AA:41:E0
PC6	00:1C:C0:6F:0E:A5
PC7	00:19:D1:3B:14:A1
PC9	00:19:D1:43:5E:9E
PC10	00:25:22:94:74:AA
PC11	6C:62:6D:F5:3F:48
PC12	00:13:8F:63:65:C1
PC13	00:19:66:88:39:A8
PC14	00:19:DB:E5:67:51
PC15	00:13:8F:6E:AA:CC

Tabla 17. Direcciones MAC equipos Sala 301

Teniendo las direcciones MAC y la distribución de direcciones IP, se procederá, en la fase de implementación a la asignación de cada IP a una MAC específica.

4.2.1.4 Servidor PROXY

El diseño del servidor PROXY se hace en LINUX basados en la aplicación Squid, esta hace el papel de un servidor Intermediario de alto desempeño, es un servicio confiable, robusto y versátil.

Este servicio se va a implementar de tipo transparente, es decir, los usuarios no van a conocer la existencia de este y no se podrá modificar desde los equipos de las salas sino desde el servidor.

Con la implementación de este servicio se busca restringir el acceso a páginas y contenidos que perturban, fomentan la distracción y reducen el ancho de banda de la red con el fin de mejorar el desempeño tanto de las clases como de la red.

Este servidor permite restringir el acceso a páginas que contengan ciertas palabras claves que se restringirán desde la configuración del mismo.

A continuación se muestran algunas de las páginas y palabras claves que se restringirán al momento de implementar el servidor PROXY. (Tabla 18)

CONTENIDO	PROPUESTA DE PÁGINAS Y CONTENIDOS A RESTRINGIR
Pornográfico	Youporn, Sexo, pornografía, videos porno, xxx, sex, porn.
Juegos	Mundijuegos, juegosjuegos, minijuegos, juegos, jugargratis.
Servidores de Descarga	Softonic, taringa, uptodown, descargas, portal programas, downloads, free download.
Redes Sociales	Facebook, twitter, skype, messenger, badoo, Hi5.

Tabla 18. Contenidos a restringir con el servidor Proxy

4.2.1.5 Servidor DNS

Para el diseño del servidor DNS y la asignación de dominios, se van a tener en cuenta los cuatro últimos dígitos de la dirección MAC de cada equipo, el número de la sala a la que pertenece y en caso de ser un computador portátil se tendrá en cuenta la marca del equipo.

El hecho de escoger los cuatro últimos dígitos, se hace con el fin de establecer cada equipo dentro del aula y al momento de presentarse alguna falla, se podrá indicar de manera más sencilla el lugar del problema.

En las siguientes tablas se presentan la distribución de dominios para cada una de las divisiones de red anteriormente descritas.

A continuación se podrá observar (Ver Tabla 19) como fueron asignados los dominios de todos los equipos que comprende la administración de acuerdo a la función que cumplen:

ADMINISTRACION	
REFERENCIA	**NOMBRE PC**
PC1 - Servidor Linux	SERVIDORLIN
PC2 - Servidor Windows	SERVIDORWIN
PC3 - Servidor Cámaras	PC515B
PC4 - Secretaria1	PC442B
PC5 - Secretaria2	PC0EA7
PC6 – Oficina	PC258A
PC7 – Dirección	PCB0E9

Tabla 19. Dominios Sala de Administración

Para la sala 201, los dominios de los equipos se asignaron teniendo en cuenta que son portátiles por lo cual sus nombres están relacionados de acuerdo a la marca como se observa a continuación (Ver Tabla 20):

SALA 201	
REFERENCIA	**NOMBRE PC**
PC1	Toshiba6D32-201-W
PC2	AcerE8D9-201-W
PC3	Acer567E-201-W
PC4	Acer551F-201-W
PC5	Acer3DF2-201-W
PC6	Acer3DD2-201-W
PC7	Acer548A-201-W
PC8	Acer5677-201-W
PC9	Acer403F-201-W
PC10	AcerE7FB-201-W
PC11	Toshiba06C3-201-W
PC12	ToshibaD474-201-W
PC13	Toshiba4E9D-201-W
PC14	Toshiba8197-201-W

Tabla 20. Dominios Sala 201

En la sala 203, como se menciono anteriormente solo hay computadores de escritorio por lo cual se organizaron de acuerdo a una referencia y de este modo se procedió a asignarle un domino a cada ordenador (Ver Tabla 21):

SALA 203			
REFERENCIA	**NOMBRE PC**	**REFERENCIA**	**NOMBRE PC**
PC1	PC952A-203	PC12	PC1343-203
PC2	PC4982-203	PC13	PC6835-203
PC3	PCE7C7-203	PC14	PC101F-203
PC4	PCC5A7-203	PC15	PC79FE-203
PC5	PCOFD7-203	PC16	PC0E6C-203
PC6	PC3998-203	PC17	PCOE80-203
PC7	PC39D0-203	PC18	PC5E1A-203
PC8	PC40AC-203	PC19	PC3F50-203
PC9	PC44B2-203	PC20	PCOFF5-203
PC10	PC629B-203	PC21	PCB0CA-203
PC11	PCCF29-203	PC22	PC06FA-203

Tabla 21. Dominios Sala 203

En la siguiente tabla (Ver tabla 22) se puede observar el orden y los dominios que fueron asignados para la sala 204:

SALA 204	
REFERENCIA	**NOMBRE PC**
PC1	PC3E84-204
PC2	PCFDFD-204
PC3	PC7C90-204
PC4	PC0E48-204
PC5	PC0949-204
PC6	PC0E22-204
PC7	PC3F44-204
PC8	PC072C-204
PC9	PC11B6-204
PC10	PCF838-204
PC11	PCA737-204
PC12	PC5EE1-204
PC13	PC667C-204

Tabla 22. Dominios Sala 204

Para la sala 301 al igual que en las anteriores salas se referenciaron los computadores y se les asigno su respectivo dominio como se puede observar a continuación (Ver tabla 23):

SALA 301	
REFERENCIA	**NOMBRE PC**
PC1	PC1A76-301
PC2	PC7320-301
PC3	PC1CF3-301
PC4	PC024B-301
PC5	PC41E0-301
PC6	PC0EA5-301
PC7	PC14A1-301
PC9	PC5E9E-301
PC10	PC5E9E-301
PC11	PC3F48-301
PC12	PC65C1-301
PC13	PC39A8-301
PC14	PC6751-301
PC15	PCAACC-301

Tabla 23. Dominios Sala 301

4.2.1.6 Servidor de Cámaras

El servidor de cámaras se diseña con base en la infraestructura física de la Academia Nacional de Sistemas, la ubicación de las cámaras se hace teniendo como referencia las salas informáticas, los pasillos y sitios estratégicos como la oficina de secretaría y la oficina de administración, estos lugares deben tener una permanente vigilancia y control por parte del encargado de la administración del circuito cerrado de televisión.

Este servicio se instalará sobre el sistema operativo Windows, teniendo en cuenta que las cámaras se conectarán a una tarjeta PCI EXPRESS, esta, trae un software de instalación y administración compatible con cualquier versión de Windows, haciendo así, el monitoreo y la grabación de videos una tarea más práctica y efectiva.

4.3 FASE IV. IMPLEMENTACIÓN DEL PILOTO.

Posterior al diseño de la distribución de los servicios, se procede a realizar la implementación de estos como se había mencionado anteriormente (**Unidad 4.2.1**), con el fin de comprobar la eficacia del diseña y así mismo mejorar el desempeño de los procesos que se realizan en la Academia Nacional de Sistemas.

Se procedió con la instalación del sistema operativo en cada uno de los equipos según la Tabla 11 seleccionado para servidores, de este modo, se hicieron las configuraciones correspondientes de software a cada equipo para la instalación, manejo, administración y revisión de los servicios.

Después de la instalación del sistema operativo en cada equipo servidor, se empieza con la configuración de los servicios, el servicio DHCP y DNS se configuran con la distribución de direcciones IP y dominios mencionados en la fase de diseño (**Unidades 4.2.1.3 y 4.2.1.5**) y se implementa de la siguiente manera (Ver Figura 9):

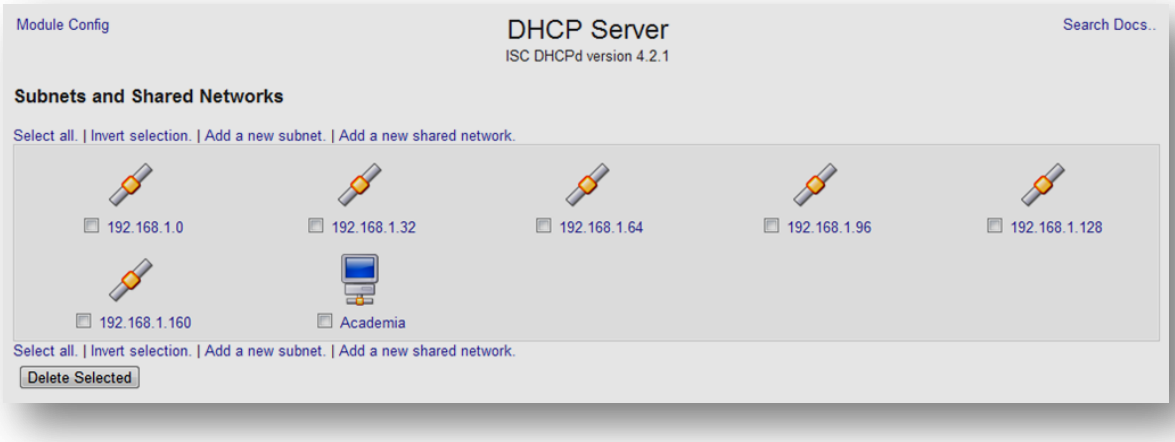


Figura 9. Distribución de Direcciones IP en WEBMIN[10]

Luego de esto la se procedió a hacer la distribución de direcciones y dominios en cada una de las salas, A continuación, se observan las direcciones y los dominios que fueron asignados para la administración (Tabla 24).

10 Imagen Tomada de Webmin, servidor Linux ANS

ADMINISTRACION			
DHCP-DNS			
REFERENCIA	MAC	IP	NOMBRE PC
PC1 - Servidor Linux	00:30:67:D0:CE:EE	192.168.1.2	SERVIDORLIN
PC2 - Servidor Windows	00:30:67:D0:C4:7D	192.168.1.3	SERVIDORWIN
PC3 - Servidor Cámaras	00:25:22:75:51:5B	192.168.1.4	PC515B
PC4 - Secretaria 1	00:26:18:B2:44:2B	192.168.1.6	PC442B
PC5 - Secretaria 2	00:1C:C0:6F:0E:A7	192.168.1.7	PC0EA7
PC6 – Oficina	00:1D:92:01:25:8A	192.168.1.8	PC258A
PC7 – Dirección	00:08:54:9D:B0:E9	192.168.1.9	PCB0E9

Tabla 24. Implementación servidor DHCP y DNS, sala de Administración.

Las direcciones IP y los dominios de la sala 204 (Ver Tabla 25) se implementan de la siguiente manera:

SALA 201			
DHCP-DNS			
REFERENCIA	MAC	IP RED INALAMBRICA	NOMBRE PC
PC1	68:A3:C4:31:6D:32	192.168.1.33	Toshiba6D32-201-W
PC2	00:17:C4:B5:E8:D9	192.168.1.34	AcerE8D9-201-W
PC3	00:17:C4:B5:56:7E	192.168.1.35	Acer567E-201-W
PC4	00:17:C4:B5:55:1F	192.168.1.36	Acer551F-201-W
PC5	00:17:C4:B5:3D:F2	192.168.1.37	Acer3DF2-201-W
PC6	00:17:C4:B5:3D:D2	192.168.1.38	Acer3DD2-201-W
PC7	00:17:C4:B5:54:8A	192.168.1.39	Acer548A-201-W
PC8	00:17:C4:B5:56:77	192.168.1.40	Acer5677-201-W
PC9	00:17:C4:B5:40:3F	192.168.1.41	Acer403F-201-W
PC10	00:17:C4:B5:E7:FB	192.168.1.42	AcerE7FB-201-W
PC11	E0:CA:94:32:06:C3	192.168.1.43	Toshiba06C3-201-W
PC12	E0:CA:94:31:D4:74	192.168.1.44	ToshibaD474-201-W
PC13	E0:CA:94:7E:4E:9D	192.168.1.45	Toshiba4E9D-201-W
PC14	E0:C4:94:83:81:97	192.168.1.46	Toshiba8197-201-W

Tabla 25. Implementación servidor DHCP y DNS, sala 201.

Luego de asignar los dominios y direcciones IP en la sala 201 se procede a hacer la distribución de estos en la sala 203 y 204 teniendo en cuenta los parámetros establecidos en la fase diseño (**Unidades 4.2.1.3 y 4.2.1.5**). La asignación queda de la siguiente manera (Ver Tablas 26 y 27):

SALA 203			
DHCP-DNS			
REFERENCIA	**MAC**	**IP**	**NOMBRE PC**
PC1	00:21:85:35:95:2ª	192.168.1.65	PC952A-203
PC2	00:19:66:D7:49:82	192.168.1.66	PC4982-203
PC3	00:25:22:73:E7:C7	192.168.1.67	PCE7C7-203
PC4	00:25:22:73:C5:A7	192.168.1.68	PCC5A7-203
PC5	00:1D:92:E1:0F:D7	192.168.1.69	PCOFD7-203
PC6	00:19:66:88:39:98	192.168.1.70	PC3998-203
PC7	40:61:86:7A:39:D0	192.168.1.71	PC39D0-203
PC8	00:21:85:1E:40:AC	192.168.1.72	PC40AC-203
PC9	8C:89:A5:35:44:B2	192.168.1.73	PC44B2-203
PC10	00:19.66:F0:62:9B	192.168.1.74	PC629B-203
PC11	00:19:21:6F:CF:29	192.168.1.75	PCCF29-203
PC12	00:E0:4C:69:13:43	192.168.1.76	PC1343-203
PC13	00:25:22:54:68:35	192.168.1.77	PC6835-203
PC14	00:19:66:DF:10:1F	192.168.1.78	PC101F-203
PC15	00:19:66:11:79:FE	192.168.1.79	PC79FE-203
PC16	00:1C:C0:6F:0E:6C	192.168.1.80	PC0E6C-203
PC17	00:1C:C0:6F:OE:80	192.168.1.81	PCOE80-203
PC18	00:13:8F:1B:5E:1A	192.168.1.82	PC5E1A-203
PC19	6C:62:6D:F5:3F:50	192.168.1.83	PC3F50-203
PC20	00:19:21:13:0F:F5	192.168.1.84	PCOFF5-203
PC21	20:6A:8A:3B:B0:CA	192.168.1.85	PCB0CA-203
PC22	00:26:22:64:06:FA	192.168.1.86	PC06FA-203

Tabla 26. Implementación servidor DHCP y DNS, sala 203.

SALA 204			
DHCP-DNS			
REFERENCIA	CABLEADA	IP	NOMBRE PC
PC1	00:24:8C:AA:E3:84	192.168.1.97	PC3E84-204
PC2	00:0B:6A:42:FD:FD	192.168.1.98	PCFDFD-204
PC3	D0:27:88:9D:7C:90	192.168.1.99	PC7C90-204
PC4	00:1C:C0:6F:0E:48	192.168.1.100	PC0E48-204
PC5	00:25:22:B8:09:49	192.168.1.101	PC0949-204
PC6	00:1C:C0:6F:0E:22	192.168.1.102	PC0E22-204
PC7	6C:62:6D:F5:3F:44	192.168.1.103	PC3F44-204
PC8	00:13:8F:BE:07:2C	192.168.1.104	PC072C-204
PC9	00:19:21:13:11:B6	192.168.1.105	PC11B6-204
PC10	00:19:D1:3F:F8:38	192.168.1.106	PCF838-204
PC11	00:13:8F:85:A7:37	192.168.1.107	PCA737-204
PC12	00:19:D1:43:5E:E1	192.168.1.108	PC5EE1-204
PC13	00:13:8F:63:66:7C	192.168.1.110	PC667C-204

Tabla 27. Implementación servidor DHCP y DNS, sala 204.

Dando fin a las distribuciones del primer y segundo piso de la academia, se comienza a hacer la asignación de las direcciones IP y dominios en la sala del tercer piso 301(Ver tabla 28).

SALA 301			
DHCP-DNS			
REFERENCIA	CABLEADA	CABLEADA	NOMBRE PC
PC1	00:19:D1:3B:1A:76	00:19:D1:3B:1A:76	PC1A76-301
PC2	00:25:22:94:73:20	00:25:22:94:73:20	PC7320-301
PC3	00:24:8C:AA:1C:F3	00:24:8C:AA:1C:F3	PC1CF3-301
PC4	00:1D:92:94:02:4B	00:1D:92:94:02:4B	PC024B-301
PC5	00:24:8C:AA:41:E0	00:24:8C:AA:41:E0	PC41E0-301
PC6	00:1C:C0:6F:0E:A5	00:1C:C0:6F:0E:A5	PC0EA5-301
PC7	00:19:D1:3B:14:A1	00:19:D1:3B:14:A1	PC14A1-301
PC9	00:19:D1:43:5E:9E	00:19:D1:43:5E:9E	PC5E9E-301
PC10	00:25:22:94:74:AA	00:25:22:94:74:AA	PC74AA-301
PC11	6C:62:6D:F5:3F:48	6C:62:6D:F5:3F:48	PC3F48-301
PC12	00:13:8F:63:65:C1	00:13:8F:63:65:C1	PC65C1-301
PC13	00:19:66:88:39:A8	00:19:66:88:39:A8	PC39A8-301
PC14	00:19:DB:E5:67:51	00:19:DB:E5:67:51	PC6751-301
PC15	00:13:8F:6E:AA:CC	00:13:8F:6E:AA:CC	PCAACC-301

Tabla 28. Implementación servidor DHCP y DNS, sala 301.

La implementación del servidor proxy se hace en base a la tabla de los contenidos a restringir con el servidor PROXY (Ver Tabla 18), estos contenidos se ingresan dentro de la aplicación webmin, restringiendo así, no solo las búsquedas por páginas sino las búsquedas por palabras, es decir, si el usuario ingresa en algún buscador o en la barra de direcciones alguna palabra que se encuentre restringida dentro de la lista de control de accesos, inmediatamente esta petición será denegada por parte del servidor proxy.

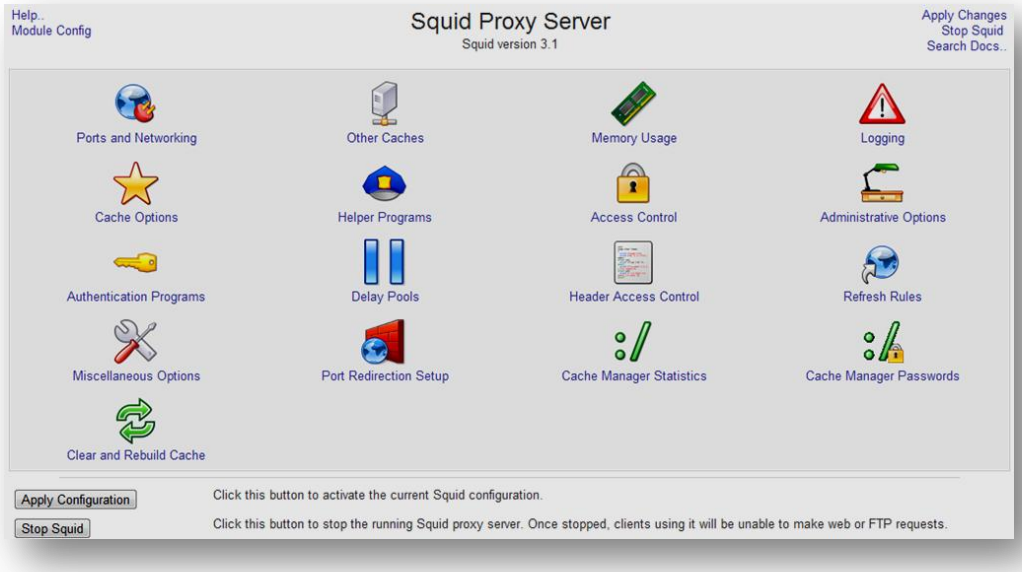


Figura 10. Configuración del Servidor Proxy en Webmin

4.4 VERIFICAR (CHECK)

El desarrollo de la fase de documentación se basa en la revisión y verificación de las actividades realizadas y así mismo de los dispositivos, con el fin de garantizar la seguridad de la información y de las instalaciones de la institución.

4.4.1 FASE V. DOCUMENTACION

Para continuar con el desarrollo del proyecto, se hacen la pruebas correspondientes para verificar que la implementación haya quedado perfecta en cada uno de los equipos, estas

pruebas se realizan por medio del software símbolo del sistema[11] para los computadores que cuentan con sistema operativo Windows.

Una de las pruebas ejecutadas en la sala 201 se basó en la revisión del domino y la IP asignados al equipo Acer3DD2-201-W (Ver Tabla 25), esta prueba se hizo iniciando el software símbolo del sistema desde el laptop, después se digitó el comando PING[12] hacia el dominio mencionadoy los resultados se muestran en la figura 11 :

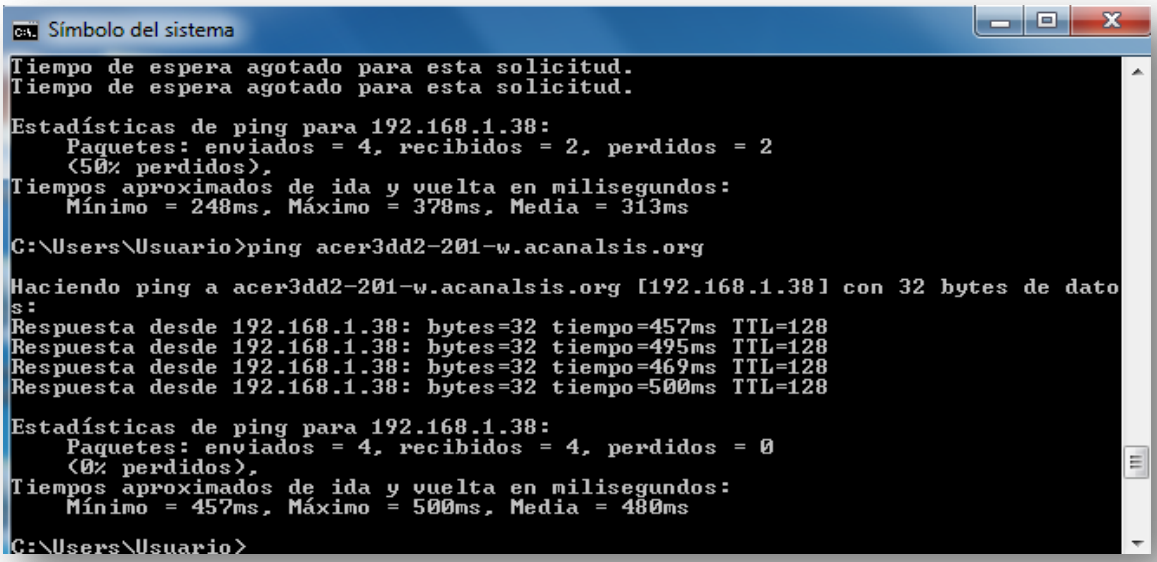


Figura 11. Prueba Ping sala 201.

La prueba PING, se hace con el fin de verificar que los paquetes enviados sean transmitidos de manera correcta entre los equipos, haciendo la prueba no hacia la IP como normalmente se hace, sino hacia el dominio asignado para observar que el servidor DNS y DHCP estén funcionando correctamente como se muestran en la figura anterior (Ver Figura 11).

---

[11] Símbolo del sistema: es la terminal de comandos para controlar el computador, antes se llamaba MS-DOS.

[12] PING: Es una utilidad que sirve para comprobar el estado de la conexión con uno o varios equipos remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco para determinar si un sistema IP específico es accesible en una red

Siguiendo con las pruebas de verificación, se hace la siguiente en el aula 204, esta prueba se realiza desde el PC7 de esta aula, se inicia el símbolo del sistema y se ejecuta el comando IPCONFIG /ALL para comprobar que la información que muestra el software coincida con la de la tabla 27.

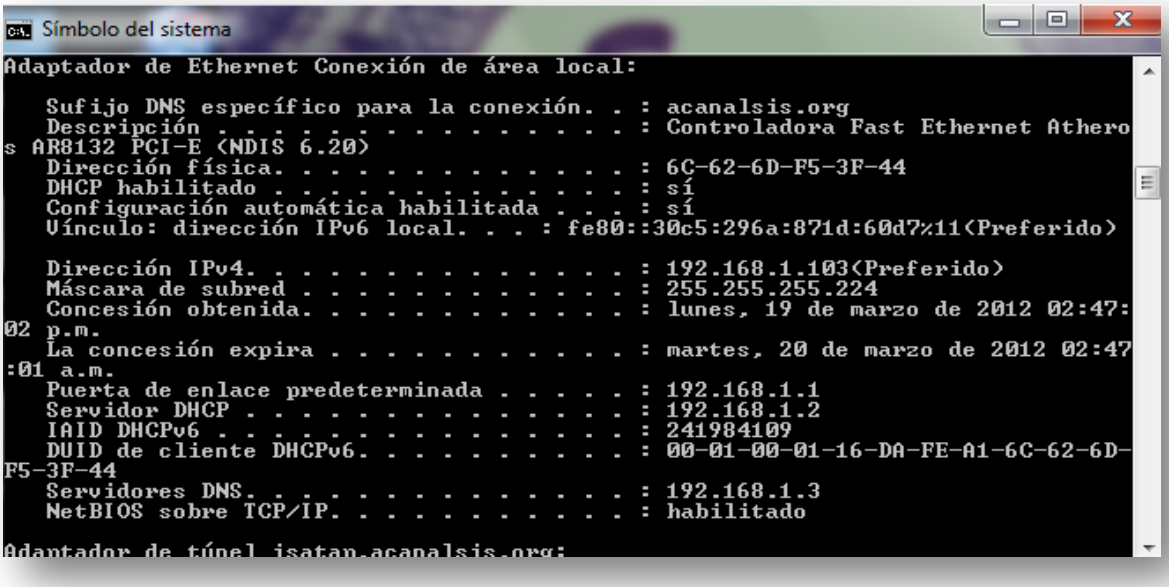


Figura 12. Prueba IPconfig/ all sala 204.

El servidor proxy se distribuyó y se aplicó en cada una de las subredes, restringiendo y bloqueando el acceso a los contenidos y paginas descritas en la Tabla 18.

Estas pruebas se realizaron en cada uno de los equipos de la Academia Nacional de sistemas, comprobando y verificando que la configuración de cada uno de los servidores estuviera funcionando perfectamente.

Para verificar el funcionamiento de este servicio se hacen las pruebas correspondientes, intentando ingresar a alguna de las páginas restringidas, dando como resultado lo siguiente (Figura 13):

Figura 13. Prueba Servidor PROXY

Por último se pone en funcionamiento (Monitoreo y grabación) el servidor de cámaras, este estará encargado de la grabación permanente y en tiempo real de todos los movimientos que se realicen dentro de la institución, a continuación se muestra la captura de imagen (Figura 14) de cómo quedaron instaladas las cámaras.

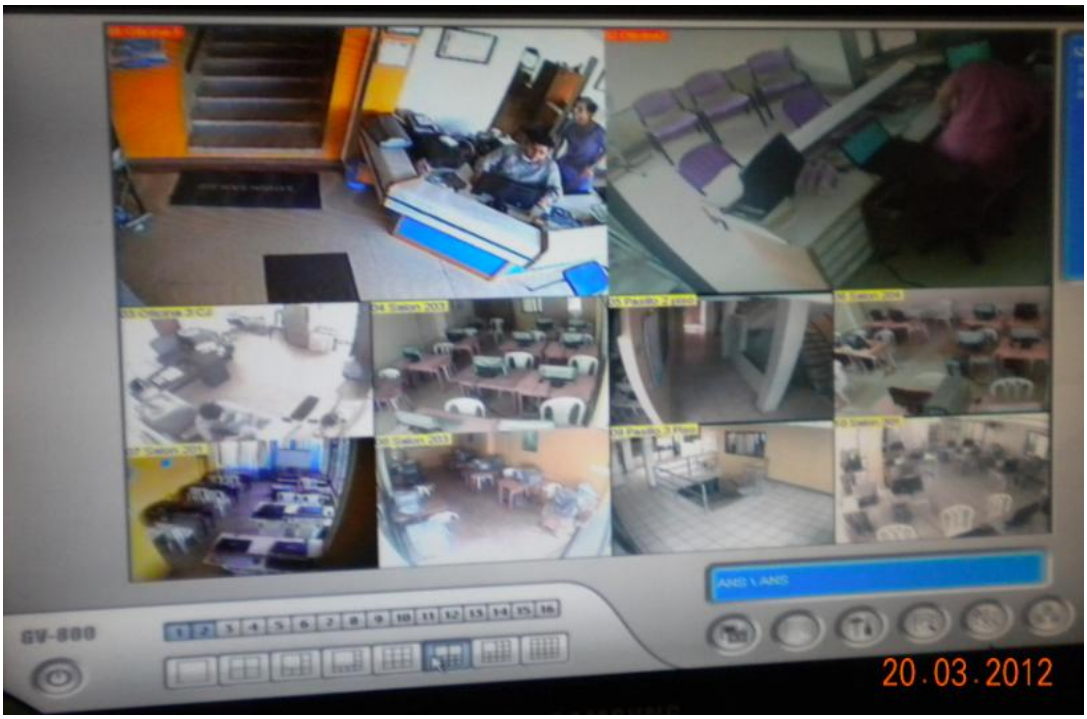


Figura 14. Prueba Servidor Cámaras

Una vez aprobada la implementación, se llevó a cabo la revisión por parte del Director de la institución Carlos Julio Beltrán quién se mostró conforme y satisfecho con el desarrollo del proyecto dentro de su institución (ver carta satisfacción).

En conclusión, el proyecto si entregó resultados, que dejan abierta la posibilidad de mejorar aún más el sistema actual y así mismo, ampliar el número de servicios implementados.

4.5 ACTUAR (ACT)

La finalización del proyecto se realizará basada en el cuarto y último aspecto del ciclo de Deming, teniendo en cuenta todas las recomendaciones descritas anteriormente (**unidad 2.2.14)**.

4.5.1 RECOMENDACIONES

En esta unidad se encuentra el análisis de la experiencia y de los resultados obtenidos durante la implementación de este presente proyecto, estos análisis se dividen en 3 partes distintas pero que a su vez se relaciona.

- Se deben programar revisiones con ciclos máximos de 4 meses(es decir cada dos periodos académicos de la institución), documentando previamente los siguientes aspectos:
    - ✓ El estado de los equipos.
    - ✓ Los datos de los usuarios dentro de los equipos.
    - ✓ Los privilegios del usuario.
- Se deberán discriminar los horarios en que puede ser utilizado de manera libre el sistema informático de la empresa, de manera que:
    - ✓ Las aulas de clase cuenten con un sistema de registro de estudiantes que digiten un código para acceder a los equipos sin poder vulnerar ninguno de sus datos.

- Sería conveniente que las unidades lectoras de CD/DVD se deshabilitaran desde el BIOS de cada máquina. Sí en algún momento llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo, habilitar el dispositivo necesario y una vez utilizado, deshabilitarlo nuevamente.

4.5.2 PLAN DE MANTENIMIENTO

La Academia Nacional de Sistemas, para mantener sus servicios y procesos al día debe realizar un plan de manteamiento preventivo de los equipos, instalaciones y servicios, en donde se incluya:

Hardware: dispositivos instalados en cada máquina, número de serie, y demás datos sobre procesadores, tarjetas, teclados, terminales, computadoras personales, impresoras, unidades de disco, cableado de la red, servidores de terminal, routers.

Software en los equipos: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos o principales archivos que contienen los equipos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, y dueño designado de la información.

Puede ser útil disponer de un responsable a cargo de la actualización de los sistemas, que controle periódicamente los dispositivos y la información almacenada. Se sugiere, además desarrollar procesos para rotular, manipular y dar de baja una computadora, sus periféricos y medios de almacenamiento removibles y no removibles.

5. CONCLUSIONES

- Un plan para el mejoramiento de los sistemas de seguridad necesita de la colaboración activa por parte de la comunidad administrativa y docente de la institución, debido a que estos, deben mantener un control con respecto al funcionamiento de los procesos implementados.

- Con la implementación del plan de mejoramiento la Academia Nacional de Sistemas está aplicando políticas de seguridad acordes a sus necesidades, debido a que esta institución se encuentra realizando las mejoras pertinentes en sus instalaciones en busca de estar a la vanguardia en lo que corresponde a la gestión y manejo de las políticas de seguridad de la información y lo respectivo a la seguridad física de las instalaciones, con el fin de garantizar el perfecto funcionamiento de los procesos que se realizan dentro de la institución.

- Basados en los resultados obtenidos en el piloto del plan de mejoramiento de los sistemas de seguridad, se puede determinar que la Academia Nacional de Sistemas obtuvo una gran mejora en los servicios de navegación de Internet y seguridad física, tales como:

    - ✓ Mejor desempeño de la red al momento en los que el tráfico que circula por esta es demasiado pesado, es decir, cuando se descarga algún documento, video o imagen desde internet.

    - ✓ Mejoras en la seguridad al momento de navegar, debido a que los usuarios no tendrán acceso a contenidos que reduzcan el ancho de banda de la red ni páginas de descargas de software innecesarios.

    - ✓ Mejoras en el sistema de seguridad físico, gracias a el software instalado en el servidor del circuito cerrado de televisión que permite el monitoreo constante y la grabación de todos los movimientos realizados en las salas de informática, aulas de clase y pasillos de la institución.

6. BIBLIOGRAFIA

[1] Integración De Servicios. (2010). Definición de Cloud Computing. http://www.oracle.com/webapps/dialogue/ns/dlgwelcome.jsp?p_ext=Y&p_dlg_id=9340796&sc=7054580&Act=18&sckw=WWMK10058758MPP018.GCM.9333

[2] Donald Graji, Mohnish Pabrai, Uday Pahrai (1990). Methodology for Network Security Design. Novcmber 1990 - IEEE Communications Magazine 0 163-6804/90/0011-0052 $0 1.OO @1990 IEEE

[3] Academia Nacional De Sistemas. (2011). *Misión y Visión* http://www.ans.edu.co/seccion.php?seccion=nosotros&ids=5&secc=0-5-

[4] SEGU-INFO Seguridad de la Información. (2009). Seguridad Lógica. http://www.segu-info.com.ar/logica/seguridadlogica.htm

[5] *HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.* http://www.kriptopolis.org

[6] SEGU-INFO Seguridad de la Información. (2009). Seguridad Física. http://www.segu-info.com.ar/fisica/seguridadfisica.htm

[7] Yongli Zhu, Baoyi Wang, Shaomin Zhang, (2005), The Analysis and Design of Network and Information Security of Electric Power System, 2005 IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific Dalian, China, 0-7803-9114-4/05/$20.00 ©2005 IEEE.

[8] Xia Qing, (2010), Network Security Management Platform System Design and Implementation, 2010 2nd International Conference on Computer Engineering and Technology, 978-1-4244-6349-7/10/$26.00 ¸c 2010 IEEE

[9] Diccionario de informática. (2011). Definición de UPS. http://www.alegsa.com.ar/Dic/ups.php. [Citado el 18 de Noviembre de 2011]

[10] Soporte Remoto de México. (2008) ¿Qué es ITIL? Ventajas y desventajas. http://www.soporteremoto.com.mx/help_desk/articulo04.html [Citado el 18 de Noviembre de 2011]

[11] Portal ISO 27001. (2005). Sistema de gestión de la seguridad de la información. http://www.iso27000.es/sgsi.html [Citado el 18 de Noviembre de 2011]

[12] HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2). Capítulo 16-Página 259.

[13] Diccionario Informático. (2011). Definición de Vulnerabilidad. http://www.alegsa.com.ar/Dic/vulnerabilidad.php [Citado el 22 de Noviembre de 2011]

[14] Gestión de la Información. (2006) ¿Qué es la gestión de la información? http://informationmanagement.wordpress.com/category/gestion/gestion-de-la-informacion/ [Citado el 22 de Noviembre de 2011]

[15] Principales Estándares para la seguridad de la información IT, alcances y consideraciones esenciales de los Estándares, EOS, Flor Nancy Díaz Piraquive.

[16] Portal de ISO 27001. (2005). ISO 27001. http://www.iso27000.es/iso27000.html [Citado el 18 de Enero de 2012]

[17] Sistema integral de seguridad y acceso a la red para un departamento de la UPC, Albert Marques. PFC - Ingeniería en Electrónica etsetb. UPC 2008.

[18] Documentos Apple. (2011) ¿Qué es DHCP y qué necesito saber? http://docs.info.apple.com/article.html?artnum=58507-es [Citado el 29 de Marzo de 2012]

[19] Ayuda y procedimientos Windows (2012) ¿Qué es un servidor proxy? http://windows.microsoft.com/es-ES/windows-vista/What-is-a-proxy-server [Citado el 2 de Abril de 2012]

[20] Somos Linux y Asterisk en Colombia (2012). Definición servidor DNS. http://www.netsecuritysolutionsltda.com/spanish/index2.php?option=com_content&do_pdf=1&id=39 [Citado el 10 de Abril de 2012]

[21] Linux Zone (2012). Webmin, una herramienta para administrar servidores. http://www.linuxzone.es/2012/02/28/webmin-administra-tu-servidor-y-mas-cosas-con-esta-interfaz-web/ [Citado el 10 de Abril de 2012]

ANEXOS

ANEXO A: ENCUESTA Nº1

UNIVERSIDAD MILITAR NUEVA GRANADA

DISEÑO DE UN PLAN DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD FÍSICO Y LÓGICO DE ACUERDO CON MODELOS DE GESTIÓN DE LA INFRAESTRUCTURA DE REDES APLICABLE A UNA INSTITUCION EDUCATIVA

EVALUACION DE RENDIMIENTO DE LA RED EN LA ACADEMIA NACIONAL DE SISTEMAS

Nombre: _____ **Fecha:** _____

En la presente encuesta usted va a encontrar preguntas específicas sobre el comportamiento y desempeño de la infraestructura de red dentro de la ACADEMIA NACIONAL DE SISTEMAS.

A continuación usted deberá responder las preguntas marcando con una X su percepción sobre el funcionamiento de la red:

Califique de 1 a 5 (siendo 5 la calificación más alta y 1 la más baja)

1. Le es fácil poder ingresar a cualquier tipo de página en internet.
   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____
2. Cómo considera la velocidad de subida de archivos a internet en la red de la academia (adjuntar documentos al correo o al subirlos a un servidor en la web):
   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____
3. Cómo es el nivel de desempeño de la red en los momentos en los que se descarga algún documento, video o imagen desde internet.
   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____
4. Cuando utiliza internet para ver un video, como considera la velocidad en que este carga:
   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____

5. Como categoriza el nivel de rendimiento de la red cableada:

   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____

6. Como considera el nivel de servicio y disponibilidad de la red inalámbrica dentro de las instalaciones

   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____

7. Las instalaciones son las indicadas para el correcto desarrollo y habilidades de su conocimiento.

   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____

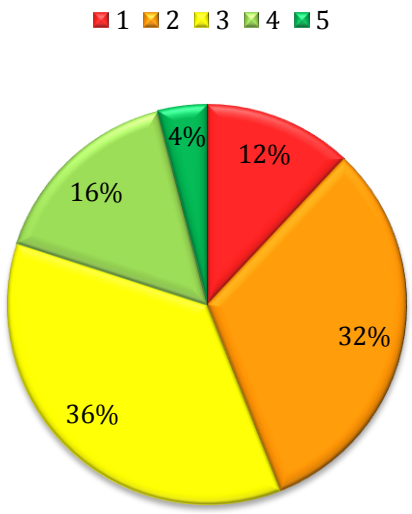
8. Las cámaras de vigilancia existentes en la academia tienen la ubicación adecuada para garantizar la seguridad interna:

   - 1 _____
   - 2 _____
   - 3 _____
   - 4 _____
   - 5 _____

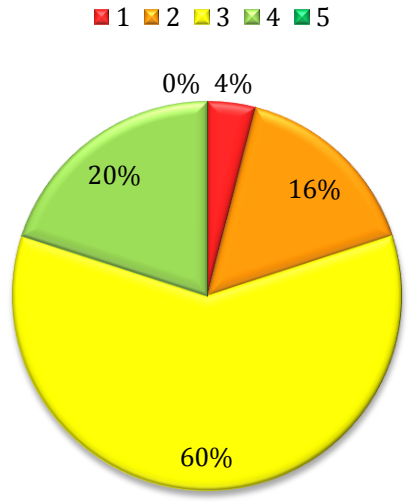
TABULACION ENCUESTA Nº1

Califique de 1 a 5 (siendo 5 la calificación más alta y 1 la más baja)

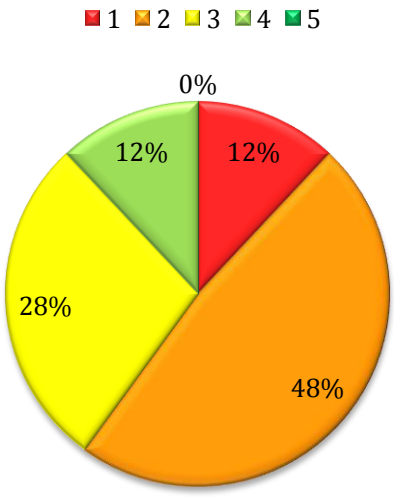
1. ¿Le es fácil ingresar a cualquier tipo de pagina en internet?



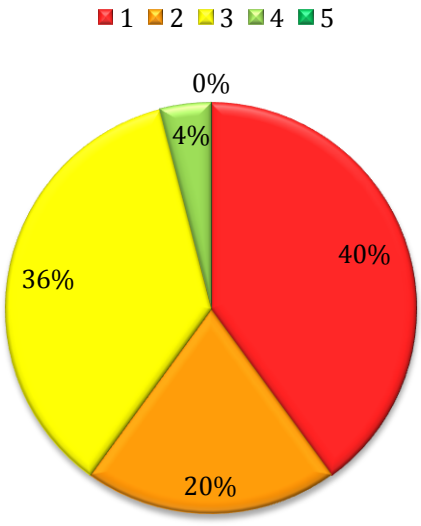
2. ¿Cómo considera la velocidad de subida de archivos a internet en la red de la academia?



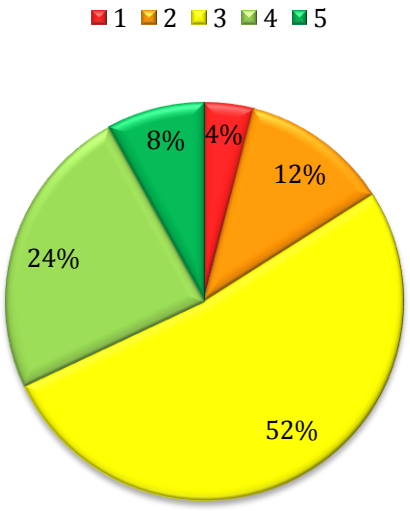
3. ¿Cómo es el nivel de desempeño de la red en los momentos en los que descarga algun documento, video o imagen?



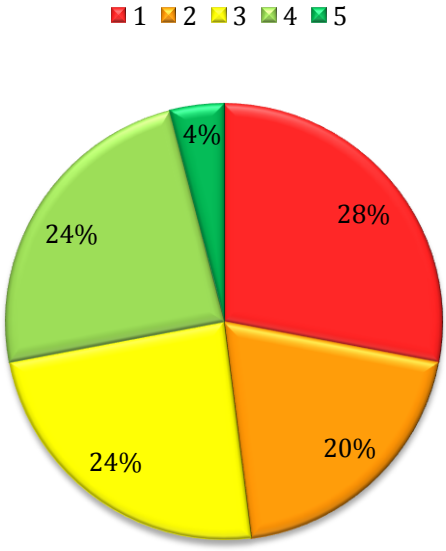
4. ¿Cuando utiliza internet para ver un video como considera la velocidad en que este carga?

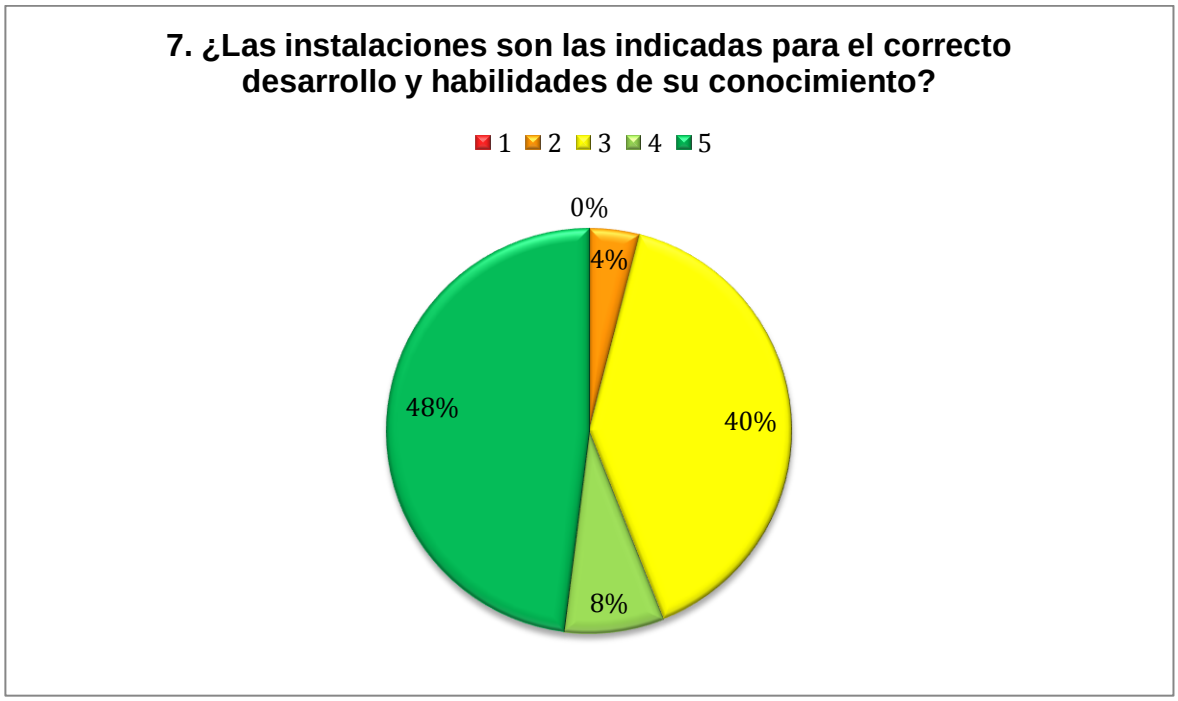


5. ¿Cómo categoriza el nivel de rendimiento de la red cableada?



6. ¿Cómo considera el nivel de servicio y disponibilidad de la red inalámbrica dentro de las instalaciones?




7. ¿Las instalaciones son las indicadas para el correcto desarrollo y habilidades de su conocimiento?
1
2
3
4
5
0%
4%
40%
8%
48%

ANEXO B: FORMATO CALIFICACION SISTEMA OPERATIVO

FORMATO DE CALIFICACION DE SISTEMA OPERATIVO "CARACTERISTICAS DE LOS SISTEMAS OPERATIVOS"

Nombre: _____ **Fecha:** _____

Califique de 1 a 5, cada sistema operativo de acuerdo a las características y a su experiencia en ellos. (Siendo 1 el índice más bajo y 5 el más alto.)

Tenga en cuenta las siguientes variables:

- **Facilidad de uso**: Comprende los aspectos de instalación, configuración y uso del software.
- **Rendimiento:** Como se desempeña el software.
- **Escalabilidad:** Hasta qué punto el software se escala en un entorno amplio
- **Comunidad**: Que tan frecuente se actualiza el SO tanto en versiones como en repositorios.

ESCRIBA EN CADA UNO DE LOS ESPACIOS LA CALIFICACIÓN QUE USTED CONSIDERA PARA CADA UNO DE LOS SISTEMAS OPERATIVOS DEPENDIENDO DE LAS VARIABLES ANTERIORMENTE MENCIONADAS.

VARIABLE	WINDOWS	LINUX
Facilidad de uso		
Rendimiento		
Escalabilidad		
Comunidad		